idm.
information & data manager
APRIL-MAY 2023

Bendigo and Adelaide Bank CIO Andrew Cresp

Why Unstructured Data Visibility Matters

Privacy by Design: What You Need to Know

Top five ChatGPT uses in the workplace

Why does security awareness fail?

AIIM 2023 State of the Intelligent Information Management Industry

$A4M Cloud Migration at Transport for NSW

Transport for NSW, the agency responsible for the state's transport network, is underway with a major shift in its information management strategy, in a $A4 million migration to Micro Focus Content Manager Cloud.

The cloud-based ECM platform will provide TfNSW with a centralised repository for all its digital content, including documents, images, videos, and audio files. This will make it easier for staff to access and collaborate on content, regardless of their location or device. TfNSW has entered into a three-year SaaS contract with Micro Focus that expires in 2025.

One of the agency's major projects is the Sydney Metro, a new rapid transit system that will provide faster and more frequent trains between Sydney's booming western suburbs and the city's central business district. The project is expected to be completed in 2024 and will significantly reduce travel times for commuters. TfNSW is also investing in the development of autonomous vehicles, with trials underway in several locations across the state.

The new SaaS offering provides TfNSW with a secure cloud-based content management solution that accelerates digital transformation while addressing data sovereignty concerns.

Micro Focus, now owned by OpenText, has expanded its Content Management product line to provide Content Manager Select Subscription licensing and Content Manager Cloud Software as a Service.

The global market for cloud ECM solutions is expected to reach $US55.68 billion by 2025, growing at a CAGR of 15.7% during the forecast period of 2020-2025.

TfNSW joins other local cloud deployments of Content Manager by Micro Focus at the ACT Government, CSIRO, NSW Crown Solicitor's Office and Brisbane City Council.

Mark J. Barrenechea, Open Text Vice Chairman, CEO & CT, recently stated that "We're going to offer the OpenText private cloud capabilities to all Micro Focus customers to accelerate innovation."

"FY 2023 will be a year of cloud acceleration and onboarding Micro Focus. We're on a clear path to a $US2 billion cloud revenue business.

"Process and information sprawl is increasing, as business information and automation spans supply chains, service management, assets, payment, financial systems, email, service and support," said Barrenechea.

FOI Commissioner Resigns

Australia's Freedom of Information Commissioner has quit less than 12 months into his five-year appointment, with Leo Hardiman announcing his resignation on LinkedIn.

Frustration over the difficulties in overhauling the FOI system to enable timely response to FOI requests were cited as his reason behind abandoning the role.

"The Commonwealth FOI system is a small but important adjunct to the doctrine of responsible government inherent in our Westminster system of government. It provides one check on the integrity and apolitical nature of the Australian Public Service. Essential to the proper functioning of the FOI system in that context is the provision of timely access to information in accordance with legally robust access decisions, including Information Commissioner (IC) review decisions."

A 2023 Budget estimates hearing was told there were thousands of outstanding FOI reviews, many going back at least five years, and more than 200 dating back to 2019.

During the February 13 hearing, Australian Information Commissioner Angelene Falk said her office was currently trying to clear a backlog of 2,010 matters. Hardiman said that under his leadership some changes had been made to the way in which Commonwealth's core FOI regulatory functions are processed, but these were not enough.

"Further changes are, however, necessary in my view to ensure that the timeliness of [Information Commissioner] IC reviews and, consequently, access to government-held information, is increased. The making of those changes is not within the powers conferred on me as FOI Commissioner.

"I have come to the view that I will not be able, in the absence of those changes, to increase timeliness of IC reviews and access in a way which best promotes the objects of the FOI Act. I have accordingly decided the most appropriate course is to resign my appointment.

FOI requests responded to outside the statutory 30-day period have increased from 11.5 per cent in 2011-12 to 22.5 per cent in 2021-22.

idm
information & data manager

Publisher/Editor: Bill Dawes
Email: bill@idm.net.au

Web Development & Maintenance: Cordelta

Advertising Phone: 02 90432943
Email: idm@idm.net.au

Published by Transmit Media Pty Ltd
PO Box 392, Paddington NSW 2021, Australia

Class action looms for Latitude breach

Law firms Gordon Legal and Hayden Stephens and Associates have announced they are investigating a potential legal action against Latitude Financial, for the massive data breach that includes personal data for customers stretching back to 2005.

Latitude confirmed that the stolen data includes 7.9 million driver's license numbers; 53,000 passport numbers; and 6.1 million customer records which include personal information (name, address, telephone, date of birth).

The breach has affected millions of past and present customers of Latitude Financial and is one of the biggest in Australian history. More information about the breach is still being uncovered, but it is estimated that the private data of up to 8 million past and current customers has been stolen.

Latitude Financial has revealed ithe breach also included much more than individual drivers' licences and passports. It included personal financial data and employment history provided on loan applications.

A letter from Latitude Financial Services CEO Bob Belan advises that "In addition to our previous notification to you, our further analysis has determined that you have had additional information stolen. This information was provided by you at the time you made an enquiry or applied for a personal loan from Latitude.

"This information includes: General financial information that was used to assess your personal loan application which, where applicable, includes details about your employment, income, expenses, assets and liabilities."

Gordon Legal partner James Naughton said the firm was investigating how a breach of this size could occur, including the effectiveness of Latitude's security measures.

"Latitude customers deserve to understand their legal rights and the steps that have been taken to protect their personal data," he said.

The Office of the Australian Information Commissioner (OAIC) has announced is making "preliminary inquiries."

The fact that customer data from 18 years ago was included in the breach will no doubt come under scrutiny.

In an earlier statement to the Australian Stock Exchange, Latitude stated that the breach extends to previous applicants and customers who may have closed their account as it "is required to retain account records for at least 7 years after an account is closed. This is to comply with Anti-Money Laundering and counter-terrorism financing laws."

Under the Australian Privacy Principles (APPs), guidelines used by the Office of the Australian Information Commissioner (OAIC), Principle 11.2. states that "entities must also take reasonable steps to destroy or de-identify the personal information they hold once it is no longer needed for any purpose for which it may be used or disclosed under the APPs".

The company says the breach extends to previous applicants and customers who may have closed their account as it "is required to retain account records for at least 7 years after an account is closed. This is to comply with Anti-Money Laundering and counter-terrorism financing laws."

The Latitude breach is now one of the biggest in Australian history. It follows a string of other breaches, including attacks on Medibank and Optus. Other law firms are also investigating potential class actions over these breaches.

The "sophisticated, well-organised and malicious cyber-attack" on one of Australia's largest non-bank lenders effects current customers and also those who have applied for finance in both Australia and New Zealand. The company operates finance companies Genoapay and Gem Visa in New Zealand.

Latitude, which provides consumer finance services to retailers Harvey Norman, JB Hi-Fi, The Good Guys, Apple and David Jones, says it is contacting those who have been impacted and the Australian Cyber Security Centre and Australian Federal Police have been advised of the breach, which the AFP is now investigating.

The Australian Department of Foreign Affairs and Trade has advised that Latitude Financial customers concerned about the recent data breach do not need to replace their passports, although those who had their NSW driver licence details exposed in the breach may need to replace their card.

The Department of Internal Affairs (DIA) revealed more than 1300 New Zealanders have had their passport details stolen, although it also states there is no need for passports to be replaced.

The NSW Government has advised that there is no need for residents of that state to replace their drivers licence unless Latitude Financial has informed them that both licence number and the card number were compromised.

This is because in NSW, increased identity protections came into effect on 1 September 2022, to help guard against unauthorised use of a drivers licence for ID purposes.

Since that date, both numbers on your driver licence, the licence number and the card number, are required to pass a Document Verification Service (DVS) check.

When you replace your licence, your drivers licence number will remain the same but your card number will change. This will protect you from unauthorised DVS checks using the old card's information.

Anyone who has renewed or replaced their NSW drivers licence card recently and has not provided those credentials to Latitude Financial since replacement may not need to have their card replaced again.

The breach was initially uncovered when Latitude noticed unusual activity on its systems that originated from "a major vendor" it uses.

The vendor has not been identified, although the company stated it "uses service providers to deliver certain services, including to verify identity. "

"The attacker was able to obtain Latitude employee login credentials before the incident was isolated," the company stated.

"The attacker appears to have used the employee login credentials to steal personal information that was held by two other service providers."

How the Privacy Act Review Report could impact and how to prepare

By Samuel Wall

In February 2023, the 2022 Privacy Act Review Report was released by the Attorney-General's Department. The Report proposes many sensible reforms in line with the current cultural shift towards greater privacy regulation. Organisations should start getting ready now.

These reforms have been a long time in the making and are well overdue. Many of the proposed changes resemble recommendations made in previous reports from the Australian Law Reform Commission, the Australian Competition and Consumer Commission, and national and state parliamentary committees over the last 20 years.

But this time seems different: we're in the midst of a cultural shift towards actually caring about privacy.

Donald Trump's election as US President in 2015 marked a turning point, after which the general public became more sceptical of technology and democratic legislatures started to think seriously about risks to their citizens' security online. The reality of those risks was brought home clearly in Australia in 2022 following various high profile data breaches. Privacy risks and data hacks are now common conversation topics around the Australian dinner table. Community expectations are higher now - we expect all companies should be taking our data seriously and are indignant when we find that is not the case.

These reforms also come at a time when the fields of cybersecurity and privacy are overlapping more than ever before. The most popular international standard for information security – ISO 27000 – has changed its title from 'information technology – security techniques' to 'information security, cybersecurity and privacy protection'. But it doesn't matter what we call it. The point is we expect our data to be secure when we interact online.

The reforms are mostly good ideas

Many of these reforms should be helpful in encouraging organisations to raise their privacy game. For example, the small business exception is proposed to be removed. Most Australians would be shocked to find out that over 95% of businesses aren't covered by the Privacy Act because their annual turnover is less than three million dollars. The removal of the small business exception will be particularly helpful for expanding the coverage of the Privacy Act.

Second, and importantly, the definition of 'personal information' will be broadened, to be brought more in line with the community understanding of this term in a world where most individuals are subjected to near-constant data collection and analysis. The current definition requires 'personal information' to be 'about a' reasonably identifiable person. The proposed new definition uses the words 'relates to' instead, which broadens it to information such as technical and inferred information. In addition, the OAIC will provide more specific guidance, including examples, about what is deemed 'personal information' and when an individual is 'reasonably identifiable'. The proposed change widens the application of the Act, as is appropriate, and makes that application much clearer.

A third welcome change is a proposed state and territory working group on privacy. We may well ask why such an institution does not yet formally exist. This group will hopefully work on projects such as aligning the slight differences in definitions of privacy across jurisdictions in Australia to make it easier, clearer and quicker for organisations to comply with multiple frameworks.

But there are areas for improvement

There are, of course, some areas where we would like to see more ambitious reforms. Here are three examples:

A number of proposals bring Australia's regulation closer towards the General Data Protection Regulation (GDPR), including the proposal to separate out processors and controllers of personal information. However, the decision to continue the exemption for employee records places Australia out of step with the European Union and may affect our ability to be recognised as an 'adequate' jurisdiction to which European Union data can be shared without any further safeguards.

It would be better to require data holders to ask users to 'opt in' to targeted advertising by default, rather than the current practice in which users must often 'opt out'. We know consumers tend to prioritise convenience over safety online (and choice architecture frameworks are designed to push them to do so). It's disappointing that this protection is weaker than it could be.

A lot of thought has been put into enforcement through the OAIC, but not yet a lot of money. Special funding was required to enable the OAIC to respond to those high-profile 2022 data breach incidents. While peer funding models are being contemplated, the amount of money the federal government dedicates towards both awareness and enforcement will ultimately determine how effective these reforms are.

And there is still a long way to go

While the Government seems keen to move quickly, we should not expect legislation to be enacted anytime soon. Organisations have until 31 March 2023 to respond to the Report, after which draft legislation and final legislation will need to be debated. Additional awareness campaigns and consultations will need to be carried out before changes such as removing the small business exception could happen. The Government is taking advantage of the current momentum and interest around privacy issues – now it needs to sustain the pace until it actually delivers.

The reality is that businesses should expect many of the proposals to be accepted into law or regulation in some form. Organisations should be taking (and documenting) steps to minimise their data footprints, understand and secure the data they hold, and develop comprehensive, actionable breach response plans. Businesses can start preparing by developing an accurate understanding of their data footprint now; both as a matter of best practice and to be ready for the changes as they come.

Samuel Wall is Senior Consultant for Privacy and Cyber Security, Sekuro

AIIM 2023 State of the Intelligent Information Management Industry

The Association for Intelligent Information Management (AIIM) has released the results of a comprehensive global industry survey undertaken in January February 2023 and focused on the intersection of people, processes, and information.

"The information management landscape is constantly changing, as are the terms used to describe it," notes AIIM at the outset of its report.

"For example, the discipline that started as archiving via microfilm has since transformed through terms such as document management, enterprise content management, and, more recently, content services platforms.

"To determine the current en vogue way of describing this area of practice, we asked our respondents which terms they use to describe their role and work."

Technology is proving to be a double-edged sword for many.

Information management comes out firmly at the top of the list (69%); however, slightly more legacy terms such as records management (62%) and document management (51%) follow closely behind.

"The distribution of terms used is not surprising, given the wide range of activities the information management community performs. However, what is strikingly obvious is that despite the best efforts of analysts and vendors, the term "content services" is still not resonating with the marketplace."

One of the key findings of the survey was that Digital transformation (DT) appears to have stalled. "Yes, over 65% of organizations have achieved significant successes with DT, but that still leaves at least a third who have not. The difference between digitizing most of an enterprise and finishing the job is vast — if just one process still involves paper and manual handling it acts like the metaphorical thorn in the side of your department."

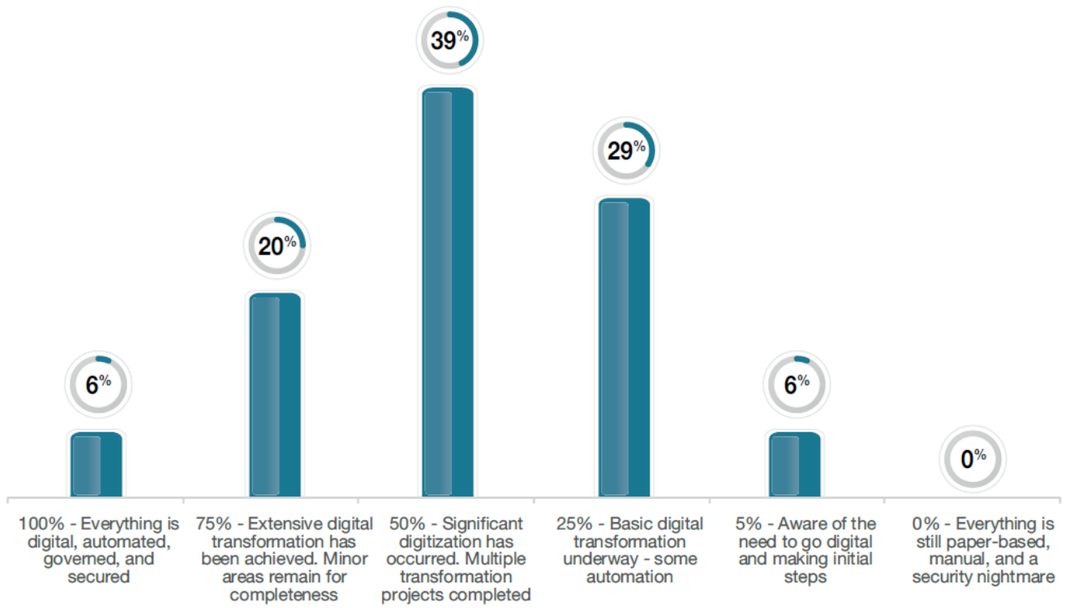
One of the metrics to emerge from the survey that caused concern was the continued increase in the number of information systems that organisations use, up to an average of nearly 5 in 2023.

"The rise of IM systems appears to be both fuelling the information chaos within organizations and trying to solve the problem," the report concludes.14 to 4.95 over the last ten years.

The average number of content systems in organizations has risen from 3.14 to 4.95 over the last ten years. The most significant growth area is for those with 7-10 systems - accounting for just 3.6% of organizations in 2013 but 14% in 2023.

"Technology is proving to be a double-edged sword for many. A huge majority (78%) feel that technology usage is driving the vast volume, velocity, and variety of information that is flooding their organizations. However, just over half (55%) also believe technology is winning the war against information chaos."

While almost two-thirds (65%) of organizations have achieved significant digital transformation, up from 46% in 2018, the challenges blocking further digital transformation remain consistent - lack of money, focus, and rigid culture.



If we consider Digital Transformation to be the process of streamlining a company's core operations and customer value propositions using technology, how complete is the digital transformation within your organization?

Which of the following is your BIGGEST obstacle to your efforts towards digital transformation?

The survey also uncovered a seeming contradictory approach to information governance. While compliance was identified is the top information management-related goal at organizational, departmental, and individual levels, this did not seem to be reflected in enterprise architecture.

Most content systems (74%) are not connected to other lines of business (LOB) systems, meaning only 26% of document, content, and records management systems integrate with other core applications.

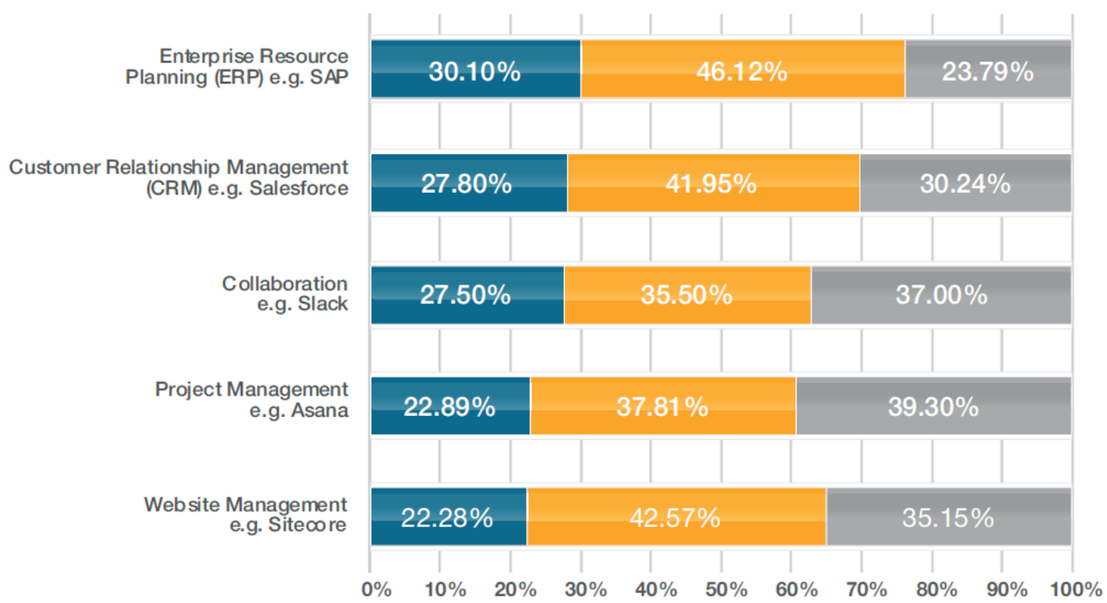
"Organizations' rating of their effectiveness in information management-related areas is not particularly positive. Except for long-term preservation (aka archiving), the digitizing, automation, and integration of processes, and legacy system modernization, none of the IM areas we asked about rated better than average by more than 50% of our audience.

"Around 1/3 of respondents rated their organizations below average in core information management areas, such as managing information through its lifecycle and applying governance and compliance.

"Interestingly, legacy modernization and migration rank above average for the majority, yet cloud migration has a split decision.

"This could suggest that the modernization of systems is either to newer on-premises solutions or to cloud-enabled versions of existing solutions that users do not perceive to be true "migrations."

To download a full copy of the survey results, visit https://www.aiim.org/resources



Which other applications do you use to store and/or access content— and how do they integrate to other information management systems?

ISO 31700 and Privacy by Design: What You Need to Know

by Greg Clark, Micro Focus

Recently, ISO 31700 was adopted as a Privacy by Design (PbD) standard. The concept of PbD was first developed by Ann Cavoukian, the former Information and Privacy Commissioner of Ontario, Canada, in 2009 and has become a central piece of global privacy regulations, including the GDPR, California Privacy Rights Act (CPRA) and Lei Geral de Protecao de Dados (LGPD) from Brazil.

Privacy by design (PbD) is a concept that places privacy requirements in the design, development, and deployment of products, services and systems. Core elements contain guiding principles for collecting, using, retaining, and disclosing personal information and implementing appropriate security measures to protect that information.

The idea is to embed privacy practices into how data is shared and in systems of engagement from the outset rather than trying to bolt on privacy protections after the fact. It is no small task, as much of the information and application sprawl is historical. However, conceptually it's a step in the right direction to preserve personal information and privacy.

PbD and some of the new ISO standard blends well with existing standards and frameworks for data discovery and classification, data minimization (ISO 27701), data access governance (NIST 800) and data protection (including NIST 800-38G and SP 800-57) capabilities that preserve privacy and support the safe and ethical use of data. ISO 31700 also emphasizes the benefits of policy-based retention and disposition of information to support PbD.

Privacy-enabling Technologies and ISO 31700

Privacy-enhancing technology (PET) refers to technologies designed to improve privacy and support standards like ISO 31700 by reducing the amount of personal data collected and shared. These technologies include PII detection, de-identification, anonymisation, and data minimisation techniques.

In addition, PET aims to reduce the risk of personal data being used or misused in ways that could harm the user if not handled ethically.

Within PET, there is a subset of capabilities designed to protect the privacy of individuals and organisations when they share, collect, or personally process data called privacy-preserving technology. These are used in various contexts, including consumer privacy, data analytics, and lifecycle management. They aim to ensure personal data remains protected and cannot be accessed or used by unauthorised parties.

Privacy-enhancing technology that can advance PdD and ISO 31700:

- Encryption: preserves data from unauthorized use/ access or seeing the data in clear text.
- Masking/Anonymisation: preserves data by removing personally identifiable information (PII) from data sets, making it difficult to trace the data back to specific individuals.
- Tokenisation: preserves data by replacing sensitive data with a unique, reversible token that can be used to represent the data but cannot be used to reveal the data itself without the presence of the token.
- Pseudonymisation: preserves data by replacing PII with a pseudonym, or fake name, that cannot be traced back to the individual.
- Data minimisation: preserves data by collecting and storing only the minimum amount necessary to achieve a specific purpose, reducing the risk of data misuse or abuse.
- Data access monitoring and controls: preserve privacy by ensuring unauthorised parties cannot access or use personal data.
- ISO 31700 contains several core principles for organizations align with to help ensure PbD. Many of these principles, processes and practices are enhanced with privacy enabling technologies. With specific callouts for lifecycle management being added, its evident privacy practices are maturing and aligning more with holistic information management across the entire enterprise.

One of the fundamental challenges of information security today is the fact you cannot secure what you don't know or if you don't know where it exists. Learn why Data Discovery is being increasingly recognised as a critical component of information security. Download NOW

Voltage by OpenText Advantages

- **Voltage File Analysis Suite (FAS):** Data discovery is vital for understanding your data's value and risk exposure. In addition, data classification helps identify and tag business critical, sensitive information (including PII, proprietary data, and intellectual property), which assists data minimization, privacy compliance and data protection efforts. Additionally, Voltage FAS SmartScan intelligent sampling is ideally suited for privacy impact assessments across large data estates and can help organisations be more prescriptive in how they approach their PIAs and operationalize privacy and compliance programs.
- **OpenText Content Cloud:** Content Cloud integrates with the systems that produce and consume information, extending enterprise-grade content management deeper into the organisation and facilitating seamless access, distribution and use of structured and unstructured data. Content Cloud's lifecycle management capabilities help support PbD by managing access to and retention of sensitive business and consumer information critical to privacy and records compliance.
- **Security standards and Privacy framework support**: ISO 31700 aligns with established security and privacy practices around ISO 27001/27701 and NIST. Voltage File Analysis Suite can help assess risk at scale and support data minimization in line with NIST and ISO 27701. In addition, Voltage SecureData developed the NIST standard for format-preserving encryption, which drives data protection techniques across our portfolio, ensuring information is shared securely and ethically within the business.

ISO 31700 has additional requirements highlighting privacy controls and data protection as core tools to protect the corporate brand and reputation. Data discovery, data protection, and lifecycle management help establish practices that build data trust, ensuring enterprise information is kept, protected, managed and maintained based on PbD practices and standards.

A core element to establishing data trust is privacy-enhancing technologies. Learn how the Voltage Data Privacy and Protection platform helps organizations put these practices in action across the entire eco-system of structured and unstructured data. Download NOW

California Privacy Rights Act (CPRA)

The CPRA emphasizes Privacy by Design practices and guides organizations toward embedding privacy into the design of their processes and IT systems. CPRA implicitly asks a user to opt-in to the sharing/ selling of personal information and has specific privacy-enhancing principles for data minimisation and data protection as best practices. See how Voltage Powers CPRA.

GDPR and UK GDPR

GDPR Article 25, sets up 'Data protection by design as a default,' and states that organizations must take 'appropriate technical and organizational measures to uphold data security and privacy rights. Article 25 specifically calls out privacy-enabling technologies like data minimisation and data protection techniques like encryption, tokenisation, and masking that preserve privacy. The UK GPDR includes the same measure as well. See how Voltage Powers GDPR.

Greg Clark is WW Director, SaaS Product Management and Portfolio Strategy - OpenText Cyber Security.

Speeding up NDIS claims processing with intelligent automation

As the National Disability Insurance Scheme (NDIS) continues to grow and mature, transforming the lives of more than half a million Australians, intelligent automation is shaping up as an important tool in easing the growing administrative burden. The NDIS assists Australians living with a disability to identify the support they need to achieve goals in many aspects of their lives.

This can include independence, education, employment, health and wellbeing, and involvement in their community. It provides them with greater choice and control over how and when they receive that support, while ensuring they receive the support they need over their lifetime.

Within the next three years, the NDIS is expected to provide more than $A40 billion in payments per year to over 650,000 Australians living with a disability. In line with this, the popularity of NDIS plan management also continues to grow.

Around 57 per cent of NDIS recipients choose to receive help from a plan manager in order to better understand their entitlements and manage their funds.

My Plan Manager Group, which comprises Assist Plan Managers, National Disability Support Partners and My Plan Manager, is the sector's largest plan management company, and has grown more than 50 per cent in the past year to collectively support more than 50,000 clients.

Founded in 2014, My Plan Manager Group helps clients make the most of their NDIS funding and now processes claims for more than 11 per cent of the plan management sector. Today, the My Plan Manager brand alone processes thousands of invoices on behalf of its clients every day and the task has been growing rapidly. Over the last 12 months, the volume of invoices has increased by almost 50 per cent.

To sustain this pace of growth, the business identified an opportunity to increase its level of technological and systems automation and data intelligence, says My Plan Manager's chief technology officer, Richard Hilliard.

Much of the business' process for NDIS claims and payment was still reliant on My Plan Manager's original, custom-built platform, which was nearing the end of its useful life. In order to sustain growth, a step change was required to remove process limitations, support system stability and mitigate risks, he says.

"The business was rapidly expanding and our existing systems were highly manual, resulting in rework and also limiting our ability to scale," Hilliard says. Against a backdrop of increased regulation and compliance, public scrutiny and customer expectations, My Plan Manager embarked on a whole-of-business effort to upgrade its technology, enhance processes and significantly improve its risk and quality guardrails.

As part of this focus, rapidMATION – an Australian-based intelligent automation consulting services company – worked with My Plan Manager to implement the new Automated Claims Experience (ACE) platform.

ACE allowed My Plan Manager to automate its accounts payable process using a combination of robotic process automation (RPA), optical character recognition (OCR) and the ability to automate key decisions via a rules engine. The end solution included a combination of UiPath, ABBYY and Salesforce's technology offerings.

RPA lets organisations automate and optimise repetitive tasks and processes, which can be broken down into rules. As with industrial robots, RPA began by handling the basic heavy lifting but, as the technology has increased in sophistication, it has progressed to managing more intricate and complex tasks.

Modern RPA does this by using complex algorithms and machine learning to continually improve, while reducing the need for manual human intervention.

Rather than employees needing to check rules and budgets manually, the ACE solution automates many processes. This frees employees to focus on tasks which require a human touch – such as exceptions – and other work that adds value for clients. "The results are clear," Hilliard says.

"We've seen increased productivity as many manual tasks have been eliminated and turnaround times improved.

"At the same time, the system is significantly more resilient to potential fraud exposure and has reduced client vulnerability."

As a result, My Plan Manager has been able to significantly reduce the amount of human intervention required when processing claims. Where it previously only saw up to 25 per cent of claims being fully automated, it now regularly sees up to 60 per cent of claims processed without employee intervention.

Rather than simply have a bot to replicate human processes step by step, Hilliard says embracing RPA has also provided an opportunity to optimise and enhance processes that unlock further business value.

"Intelligent automation isn't just about rubber- stamping things; the ability to embed intelligence into our platform has been key in getting the results that we see today," he says.

"That means our clients get better outcomes and better service from providers, and that those providers get paid accurately and on time – all of which contributes to the NDIS delivering value to everyone."

iCognition Celebrates 20 Year Information Management Journey

Two decades since consultancy iCognition opened its doors, founders Joe Mammoliti and Nigel Carruthers-Taylor reflect on the unique new challenges in information management today, and those that remain the same.

iCognition was founded in in 2003 in Canberra, the epicentre of Australian federal government, and now provides consulting and implementation services to government and enterprise customers across the nation. The firm was founded in recognition of the information revolution that was sweeping the world and making heads spin, with the vast amount of information being created, circulated, and churned through corporate networks.

iCognition was born with a mission to help its clients manage an ever-increasing quantity of information and find and retain nuggets of information gold.

"The amount of information bombarding organisations in 2003 was recognised to be increasing exponentially, particularly electronic documents and emails, and social media was on the horizon. We realised that simply throwing technology at the problem wouldn't solve anything – somebody needed to come up with a concept on how to manage that information using people, processes and technology," reflects Joe Mammoliti, iCognition's CEO.

An Enterprise Content Management (ECM) system called TRIM, developed in Canberra by Tower Software and keenly adopted by Australian federal government, was an easy choice to form the foundation of iCognition's practice.This was extended and enhanced with iCognition's own IP to develop an enterprise-wide Records and Information Management (RIM) solution offering a single source of truth.

Through the many changes in name and ownership of TRIM, now OpenText Content Manager, iCognition has stayed focussed on helping clients achieve compliance with governance and security frameworks.

iCognition quickly became a key partner for large government departments, councils, universities and not-for-profit organisations. Fast-forward 20 years and the market is experiencing a rapid increase in security, privacy, compliance and regulation requirements.

"Not only did the information explosion happen, but we're now hit daily with significant information security risks – while in the past these risks focused on database information, now all content is a target for hackers," says Nigel Carruthers-Taylor, iCognition Executive Director.

COVID ushered in more complexity as the pandemic forced organisations to pivot quickly to online collaboration and information sharing, despite increasing concerns about privacy and compliance. Unfortunately, many organisations found their information fragmented, leading to most RIM strategies being turned on their heads. Suddenly, information was everywhere, and records were mostly uncontrolled.

"That's why the days of monolithic, enterprise-wide ECM (Enterprise Content Management) systems are over. In this new landscape, ECM systems need to adapt to become part of a more extensive content platform," says Carruthers-Taylor.

Organisations are now turning to Content Services Platforms (CSPs) to create a holistic RIM environment to govern and manage enterprise-wide content ensuring security, privacy, and compliance under a single framework. CSPs enable users to manage content across multiple information repositories and protect sensitive information while allowing the business application to become a source of truth orchestrated with other systems.

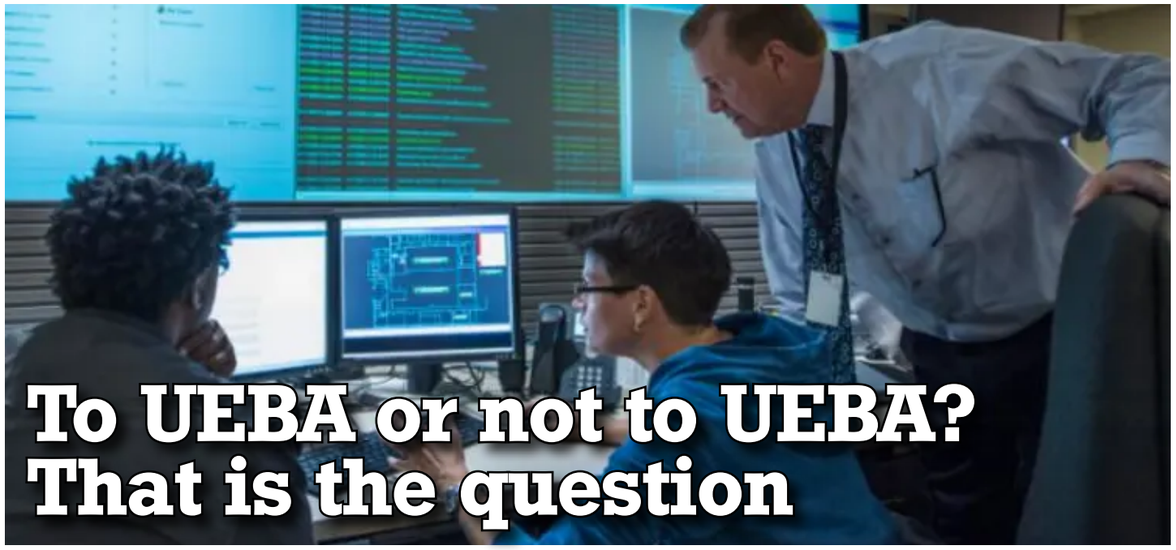
"With CSPs, business systems such as HR, case management, and finance can all become trusted sources of truth, managed under a single framework for compliance and records management purposes, while also increasing productivity and service delivery around content-related tasks."

So where does this leave the next generation of content and information management? Scheduled for release in May, iCognition is developing a new RIM solution that offers an efficient and secure records management environment where users won't have to worry about where content is sourced or how it is managed.

"After 20 years, we've seen it all when it comes to information management systems and processes. Honing this knowledge, our next-generation solution ensures users don't have to jump from system to system to work with content from across the enterprise," said Mammoliti.

"The content is delivered contextually to meet the information needs of the user at the specific point within their work task, while still abiding by the organisation's framework of policies, processes, and governance."

To learn more, contact iCognition at https://icognition.com.au/contact/



To UEBA or not to UEBA? That is the question

By Chris Ray

Over recent years, user and entity behaviour analysis (UEBA) has evolved as a new set of tools in the chief information security officer (CISO)'s armoury. So, where has it come from and how can today's solutions help?

To answer this, we first need to consider the overall shape of the cybersecurity landscape. The core areas that we are looking to protect are the applications we develop, deploy and use; the infrastructure (on-premises or cloud) on which we run these applications; and the identity domain - users, services, and other entities that interact with both applications and infrastructure.

The first two areas have challenges of their own: security concerns today range from protecting against compromised servers, to the relatively new area of development security operations (DevSecOps) which is aimed at securing new code and infrastructure, both of which are deploying at rapid speeds.

However, the third, identity domain has the most impact on security, because of its unpredictable nature. User behaviour is dynamic by nature; internet of things (IoT) devices, service accounts, and other entities are perhaps less susceptible to change, but are complex and can interact in unplanned ways.

A catalyst was undoubtedly the COVID-19 pandemic, which has driven a substantial shift in work environments and technology, and while this shift enabled effective remote work, it has created increased complexity which is ripe for exploitation. Given how bad actors are constantly looking for areas of weakness, it is unsurprising that this space has gained so much attention.

We have seen a two-pronged effect on attacker behaviours, illustrated in cybersecurity analysis such as the Verizon Data Breach Investigations Report and the 2022 CrowdStrike Overwatch Threat Hunting Report. First a reduction in attacks on endpoints, likely the result of more effective endpoint security solutions coming to bear on the landscape combined with the dispersion of endpoints increasing the perceived cost for an attacker to target them.

The second has been an intensified focus on identities as a means to execute attacks. Unlike endpoints, with robust and mature security measures that can be deployed quickly, identities across users, systems and other entities have been left relatively neglected - until recently, that is.

New battles in the cybersecurity war are now fought over the identities that belong to staff and technologies inside organisations. Attackers know that identities have trust built into them, and if they can compromise an identity, they will be able to abuse that trust to achieve their goals.

UEBA's direct ancestor, user behaviour analysis (UBA) was designed to analyse the actions of users in an organisation and classify normal versus abnormal behaviours. From this analysis, UBA solutions look for deviations from baseline activity, and can detect malicious or risky behaviours.

So far so good. But as the full scope of what's connected to the network has expanded in both entity type and distribution, the need to analyse entities other than users has moved front and centre. In response, security vendors have added entity analysis to UBA, creating UEBA.

While the overall strategy and technique – hunting for abnormal behaviours – remains the same, the scope of analysis has expanded to include things like daemons, processes, infrastructure, and cloud roles. Combining the data and insights from multiple entity types provides a more comprehensive view of an environment, adds much-needed context to security events, and drives the incident response process.

A common use case is detecting a compromised administrator account attempting lateral movements. While security information and event management (SIEM) solutions and other security monitoring tools can detect this behaviour with enough telemetry, UEBA solutions can detect it with far less data gathering and analytics.

Whereas SIEM relies on a set of rules that can be matched to a specific behaviour to identify malicious intent, UEBA actively looks for anomalies (essentially defining the rules in real time). This is important, because a single unusual event can be significant but very difficult to detect without the right tools – think of it like spotting the needle in the haystack.

As such, UEBA offers far more than just monitoring users and other entities for malicious actions. Instead, it collects and processes data to highlight anomalous behaviour through application of artificial intelligence (AI), statistical analysis, and other methods. While anomalous behaviour isn't by itself an indication of malicious intent, it can inform security staff to review the circumstances that led to the creation of the UEBA alert.

Organisations today are investing more heavily in UEBA solutions. Every organisation, regardless of size or industry vertical, has identities, which is why UEBA solutions have universal appeal. However, the nature of different solutions needs to be considered relative to both the scale of the problem being addressed (the identity threat surface, as it were) and the practices enacted by security teams.

For example, while most solutions offer the ability to identify anomalous behaviour, some are taking this a step further, to include automated investigation actions prior to the alert generation. These automated steps gather additional telemetry to enrich the primary events and provide critical context. We fully explain areas such as these in our Key Criteria report on the subject, available to subscribers.

As we have reviewed vendors delivering solutions in this area (for the accompanying Radar report), we have also seen how quickly the solutions market is evolving, much like other solutions in the security space. Vendors know that identity is the new battleground and have been building better ways to detect identity abuse and other anomalous behaviours.

If there was a unified approach to solving this challenge, there would likely be only a few solutions in the marketplace. But there isn't a single, best approach, and for that reason, several leading solutions may be applicable, depending on what you already have in place in your organisation.

To identify which UEBA offerings are worth considering, a great starting point is for organisations to review their existing security solutions and determine whether they serve their purpose. If organizations determine a new SIEM solution is needed to achieve its security objectives, then the best approach may be to consider a consolidated SIEM-plus-UEBA platform.

Several vendors offer UEBA solutions built on top of their SIEM solutions: once the SIEM solution is deployed and data is being ingested, UEBA becomes almost as straightforward as flicking a switch. However, if an existing SIEM is already operating effectively but doesn't have an associated UEBA, strong consideration should be given to a subset of vendors which offer powerful analytics solutions that can be easily layered on top of existing security solutions. Finally, surveying the technology infrastructure in its entirety can help to narrow down the scope of solution selection as well. Consideration of your incumbent security technologies should always occur when looking at additional capabilities, so you can take into account data integration capabilities, or the ability to manage multiple data feeds on the same dashboard.

Overall, UEBA is rapidly becoming a key element of the cybersecurity environment. By adopting an integrated approach rather than seeing it as a stand-alone tool, you will be setting yourself up best for the future.

Chris Ray is a GigaOm Security Analyst. This article appeared first on GigaOm.

Why does security awareness fail?

By Andrew Walls, Gartner Inc.

A small avalanche of data from various sources (including Gartner) confirms what many of us in the cybersecurity world have believed for years: security awareness doesn't work. I suspect that this will not come as a surprise to anyone who works in security as it is routine for employees to prioritise pretty much anything else over security when a conflict arises.

What is going on here? Why has the steady drumbeat of training and phishing simulations not produced effective cyberjudgement in our employees?

A few issues are obvious to me, some of which might make security people a bit uncomfortable.

1 Cybersecurity professionals are not expert in training design, development, training product selection or implementation. Fundamentally, making the security team responsible for selecting, developing, administering and measuring a training program pushes them into a state of incompetence. Most people in cybersecurity got there by being really good with computers, not by being good with people. The design and administration of effective training is a specialist discipline. Assuming that such expertise is not needed to get good results from training investments is both arrogant and foolhardy.

2 Despite decades of pushing 'alignment with the business,' the security team remains alienated and separate from the rest of the enterprise and, the truth is, we like it that way. There are myriad historical reasons for this alienation, but the foundation is that security seeks to limit the flexibility of the enterprise while the enterprise wants to be infinitely agile and responsive to the market. Security assures the predictable operation of systems and processes. Unbridled innovation makes for unpredictable outcomes.

This foundational tension leads to frustrations on both sides and, at times, clear condescension, and paternalistic behaviour from all parties. This pops up in our language. Why do we call 'them' users? Why do we say people are the weakest link in the security chain? The end result is that we do not have a deep commitment to enabling employees to become competent at security because we do not think they are capable of doing so. As a result, employees consistently rise to our level of expectations and engage in high-risk behaviour. No amount of training will overcome this kind of social alienation.

3 Policies and regulations have mostly defined the frequency of training interventions (e.g.: annual) and not achievement of measurable competence in trainees. We would never tolerate this in a standard or policy for security technology. Any policy that said, 'you must have a firewall' and lacked a focus on the functional outcomes expected of a well-managed firewall would be rejected.

This sort of policy or regulatory statement implicitly devalues training as a solution to poor security behaviour. If behaviour is important, policy should target measurement and improvement/maintenance of behaviour without specification of how behaviour change and maintenance is achieved. If your internal policy states that everyone must be trained a certain number of times in a year, it is perpetuating the problem.

4 If security is so important to the enterprise, why isn't it built into every manager's and employee's performance metrics? Few managers look for opportunities to take responsibility for the security behaviour of their teams, work processes and infrastructure. They know that this is a difficult area of endeavour and would prefer that that responsibility is allocated somewhere else.

The CISO and their team are a convenient repository for these responsibilities even though management of employee and management behaviour is nominally the responsibility of team managers in the business. Somehow the security team is expected to manage the day-to-day behaviour of all employees with or without the support of the management team over those employees. This leads inevitably to conflicts and employees generally do what they are rewarded to do by their manager. Security issues are left for the security team to clean up.

Employees are not fools. They recognise that business performance is more important to their personal success than performance against seemingly arbitrary and mostly irrelevant security metrics. As a result, they pay little attention to security awareness training and make little attempt to internalise the messages contained in the training, particularly if those messages conflict with or inhibit their ability to meet their personal performance targets.

Many people recognise these issues with security awareness and are exploring ways to step past these cultural and social challenges to create a truly security-conscious enterprise. Much of this work focuses on creating and maintaining an effective security culture throughout the enterprise. This is a great idea and could be transformative for enterprises; however, culture change is not a plaster you can slap on top of a dysfunctional relationship between the security team and the enterprise.

The four issues mentioned in this article need to be addressed and resolved in order to drive and sustain culture change. This means that the security team itself must change in attitude and behaviour and the executive management team of the enterprise needs to be an active supporter and champion of this change.

Privacy in the hybrid work era

The rise in remote and hybrid working has caused distress, as 77% of Australians are more worried about their personal data now that organisations operate distributed work models. On top of this, 49% of Australians said they'd no longer use or buy from a company they were previously loyal to if it failed to protect or leaked their personal data. IDM asked George Harb, Vice President, ANZ at OpenText, what organisations should be doing to protect data and establish cyber resilience.

IDM: What do you think of the key challenges that organisations face when coming to securing their enterprise information?.

GH: I think organisations have three key issues today. The first one is knowing their data; there has been so much collected over so long and there are so many platforms or applications that have been decommissioned and are still sitting there. People change, processes change, go to markets change. But that data is still there. Knowing what you have, and where it is, is critical. Then controlling your data. Who's got access to it? Where does it reside? What are the control mechanisms that you have in place in terms of reviewing, accessing, retrieving, etc.

The next one is remediating and maintaining your data. So, what information should be redacted? What information should be made available? What information should be deleted and removed because it's no longer useful. These are the three key challenges and organisations need to understand and how to manage those challenges to stay on top of that issue in regards to customer data privacy.

IDM: Over the COVID period, many organisations rushed to move to Office 365 to enable remote working and the ability for knowledge workers to access data about their clients or citizens remotely. How is that impacting in terms of securing information management systems?

GH: Consumers are worried about their information being hacked. When you add on top of that there is awareness that people are working from home. People are working from coffee shops. Accessing public Internet Wi-Fi platforms. It adds to their concern. And so, as an organisation, if you're thinking about your consumers and their concerns, that transfers over to how you control information.

"Knowing what you have, and where it is, is critical." - OpenText Vice President, ANZ, George Harb

When it's now being accessed from hundreds or possibly thousands of different locations versus what it previously used to be. Ultimately it comes down to the controls you put in place. And I go back to the control your data theme. It's around who's accessing, how they're accessing, understanding whether there's information that a person shouldn't be accessing, but they are, and being able to flag that. That to me is the concern that consumers have which transfers to organisational concerns.

The people that are responsible include your chief risk officers and IT officers; they're concern is how do I control that data? How do I control access? What's being retrieved? What's being downloaded? What's being uploaded and being able to track it. That's essentially one of the challenges that organisations have , how do you keep track of all of this. Can you stop it? Well, when you have a remote working workforce, it's difficult to stop, but you've got to be able to track it. You've got to be able to understand where and what is being used and I think that to me is the kind of question that needs to be answered.

IDM: Australia is trying to adapt its privacy regime to follow more European style privacy laws. Do you think Australia Enterprise and government is ready for that change?

GH: Technology can enable it. So, when you look at GDPR in Europe, organisations are having to adapt to it and that comes down to essentially knowing where your data is so that when the citizen comes along and says, I want you to remove my data, you know where it is and you can remove it. That's being enabled by technology.

So, organisations are going to be able to understand what those policies are, when they're being presented to the industry to adapt to. But quickly being able to determine whether they have the technology in place to enable that, and I think you'll find that a lot of organisations in Australia have got customers in Europe, and they need to adhere to GDPR, and have already gone down that path and understand it and put in place. But what the Australian rules will look like and how they need to be adhered to and implemented is something we are yet to understand. But technology is available today that can enable it.

IDM: What do you see as the top priorities for organisations coping with data privacy issues operating today?

GH: I think there's four. The first one is updating your retention rules. So, make sure you're not adding more data that you don't need to add. So, stop the binge, in essence. Then you need to clean your data up, understand what you've got, understand what data you have and then clean it out. Then the next step is to review these subject rights. So, who can access, what they can access, when they can access and where they can move it to, or to whom.

Review your rights/rules and make sure they support the new rules that we're all having to abide by. And then finally, internally, the business needs to update the privacy policy and educate the staff around that. I think it's important to make sure the mechanisms are in place, the documents, the training, the certification, so that people understand what they mean. Because when they come out, if your staff doesn't understand them, they can't respond.

IDM: Small businesses with an annual turnover of less than $A3 million could soon have to comply with the Privacy Act. Do you think this will up new markets for ECM and data discovery, which have traditionally been enterprise or large government?

GH: It will, but it comes with complexity. And with complexity comes cost. So, while these rules are being pushed down towards the smaller to medium enterprises, it's going to come down to cost and whether they have the ability or capability to implement these types of solutions. Because it's not a case of plug and play.

When you look at how organisations need to adapt, they need to understand their business and need to ensure their business rules and the way they work fits into that model. So, there isn't going to be one size fits all. It could be a 70 or 80% fit, but there's going to be certain ways that small organisations will work that has to be customised. And with that, either the business needs to adapt to what the technology and the rules allow it to do. Or they're going to need to go through some customisation, which comes with a cost. So possibly yes. Easily adaptable or easily implemented? Still a question mark.

IDM: OpenText offers solutions in a range of different areas, and one of these is privacy management. Do you see that as a separate product category to content management or document management solutions?

GH: Absolutely. Because within the document, there are going to be certain things that are privacy related or specific. And you need technology to be able to pick those up. How do you know what information you have that needs to adhere to privacy law? How do you know what information you have that could get you into trouble if it were hacked? And that's where those privacy solutions come into play. So yes, as a separate stream, absolutely.

IDM: What role do you see emerging technologies such as AI and machine learning playing in improving enterprise information management and security and how is OpenText incorporating those technologies into its solutions?

GH: We have our own Magellan AI platform, which we continue to incorporate in the solutions that we offer. This is a tool that enables us to detect and act on potential risks hidden from sensitive or inappropriate data, which is important today as there is a vast amount of information stored in business systems.

With our AI capability, we are able to sift through this information—even those in the form of unstructured data—and identify any risks. ChatGPT presents an opportunity and also a risk. Because you don't know what information you're introducing into your business and how valid the IP around that information. Are you setting yourself up with an unknown set of data and information that you're then presenting as your own? Companies need to put in place policies that address the use of these AI tools because we don't know yet how powerful or how risky they are in incorporating them into the way that you work.

Obviously, within the business, when you're using AI to leverage your own information, it's a massive value because you're able to provide customers with tools for them to self serve. Which is always something that organisations are looking at to help customers help themselves.

So that's fine, but once you bring that other element in and bring the wider information that's available out there, that presents risks. And I don't think organisations fully appreciate or have concluded how they're going to use that in the way they work. There's a lot of trials going on but I don't think it's fully appreciated, yet.

Why Unstructured Data Visibility Matters

By Krishna Subramanian

Most enterprises are flying blind with their unstructured data. They don't know what they have, who is using it, why it's growing so fast, or how to be more efficient in managing it.

IT leaders need insight into their unstructured data. Without it, they are hindered in their ability to cut significant costs on data storage. As it is, most enterprises are spending more than 30% of their IT budget on data storage, backups, and disaster recovery, according to a 2022 survey on unstructured-data management.

Beyond high spending—which can get higher if you don't optimise cloud-storage placement—there is also the question of monetising data. Unstructured data too often holds significant untapped business value. Most organisations use but a small percentage of the data they produce and store. A recent Accenture study revealed that 68% of companies don't realise tangible and measurable value from their data.

Since unstructured data comprises the lion's share of all data in the world, you need to know what data you have, who needs access to it, how much of it is active, where it is stored, and its value to the organisation. You need visibility.

Attaining this visibility isn't easy, of course; in our complex world of hybrid clouds, unstructured data is strewn across corporate and colocation data centres, edge systems, and various cloud services. Moving data into a central repository would be an expensive and likely impossible proposition because of the distributed nature of data and data creation in the modern world.

Since unstructured data (including images, video, and documents) can reach billions of files of various types and sizes, organisations need a systematic approach to analysing and classifying it. Creating searchable data index of all the organisation's data across silos—from on premises to edge to cloud—is an important first step to getting visibility.

Getting Started with Fundamentals

You can address data-visibility issues in your organisation by developing a plan and process to assess and track your unstructured data. There are several fundamentals about your data that you'll want to start tracking, including:

- Volume of data in storage
- Growth rate of data over time
- Age of data
- Access patterns, such as time of last access
- Location of data
- File types and file sizes
- Top data owners and types of data they are storing
- Costs of data storage, backup, and disaster recovery today and in the future

Here's why these data points are important:

Data-usage metrics: Without the ability to see which files/shares/directories are being used regularly and which haven't been touched for a year or more, it's hard to do anything other than keep all your data on your expensive, high-performing storage. If, however, you can see how much of your data is rarely accessed (or "cold"), then you can manage it at a much lower cost by migrating or tiering it to cheaper storage, such as cloud object storage (AWS S3 or Azure Blob, for instance). Additionally, in organisations with chargeback models in place, department managers need to know data-growth metrics and who the top data owners are so that those individuals are included in data-management conversations.

Sensitive data: Organisations sometimes need to delete data altogether for legal reasons—for instance, ex-employee data or ex-customer financial data. The ability to easily search customer and individual names connected to files delivers a huge advantage here. Granular search capabilities (such as by file extension or metadata) let the user locate intellectual property or financial data that might have been copied or moved to a location without appropriate security protections or access rules applied.

Financial metrics: As part of a data-operations (DataOps) and financial-operations (FinOps) strategy, IT leaders should understand the costs of storing data on current technologies and be able to project costs for moving to a different storage platform. From there, they can determine if it would be cost-effective to, say,

- Move less-active data to the cloud
- Move on-premises data to network-attached storage (NAS)
- Delete some portion of data archives

When armed with knowledge on their data assets, IT teams can set policies to transparently tier data to the most cost-effective storage based on data sets' use cases and priorities. With this empowerment, IT leaders can slash storage and data-management costs while accommodating rapid data growth.

Data Refinement

Once you get started on an unstructured-data assessment through indexing and analytics, consider further refinement. When you tag data with additional context, such as demographics, descriptive details (for instance, "image of eyes"), or project names, you open search parameters to help users and to make better data-management decisions.

(Look for an unstructured-data-management solution that supports automated tagging by policy and can retain tags for data wherever it moves.)

Moreover, systematically classified, well-managed, easily searchable data is vital for fuelling the latest generation of affordable, powerful artificial-intelligence (AI) and machine-learning (ML) applications.

New AI/ML tools can jump-start an organisation's innovation cycles, deliver noticeable productivity gains, and/or optimise anomaly detection to dramatically reduce security/compliance risks.

As data becomes ever more central to business decisions, product development, and customer strategy, knowledge about that data is increasingly valuable to people across the organisation. The CIO needs to understand high-level implications of cloud storage and data growth.

Researchers want to know what data is available for future projects. Legal and security teams need to ensure data is protected and discoverable if needed for auditing or investigations.

Yet visibility alone isn't enough. To get ROI from unstructured-data management, this data knowledge must be integrated into workflow processes. It should be simple to move from insight to action—migrating, tiering, copying, and deleting data, along with ongoing data-lifecycle management—to meet user, application, and departmental needs.

Krishna Subramanian is Co-founder, President and COO, Komprise. This article initially appeared HERE

Digital by Design – Human when it Matters

Bendigo and Adelaide Bank is underway on a quest to innovate the digital workplace and deliver against customer and staff expectations and regulatory obligations. Bendigo and Adelaide Bank CIO Andrew Cresp outlined the journey so far in a discussion with Microsoft's Director of Financial Services Rebecca Engel and Chief Technology Evangelist from EncompaaS Cassandra Bisset.

By Michelle Phillips, Head of Customer Success, EncompaaS.

When Andrew Cresp joined the bank three-years ago he commenced a program to simplify and modernise the technology landscape for the organization. Interestingly one of the better use cases was their document management capability. This discussion navigates the consolidation of thirteen document management systems to one, working with leadership to prioritise projects, novel approaches for supporting staff when moving to the cloud and developing strategies to deliver against the intent of regulatory requirements for greater flexibility and scale.

1. Consolidating systems allows you to focus.

Bendigo and Adelaide Bank has completed a journey to consolidate a diverse array of document management systems into SharePoint, with the EncompaaS platform providing discovery and automated classification. The multiple systems were the result of an extensive and quick set of acquisitions that had seen the organisation grow to over 7000 employees.

"We had 13 different document management solutions connected to various monolithic applications, we have now consolidated onto SharePoint using EncompaaS for its records management capability. Those 13 were in different states of application and infrastructure health so by moving from many to one you actually get to put some focus on it and manage it a lot better. That's pretty important knowing our customer expectations play out either through our regulators or directly, it is ever changing especially regarding privacy" said Cresp

2. Understanding organisational culture and project interdependencies helps you prioritise

Bendigo and Adelaide Bank has approximately 1000 subject matter experts (SMEs) and as Cresp explains that can be a double edge sword. Cresp recalls having conversations where he has stated there will be a focus on one project, "this is our number one thing and you know the entire organization sort of straightens up behind that. But there is a real danger in doing that too because with 1000 people we can get a lot of stuff done and there is risk in being myopic". Particularly when there are multiple competing projects and outcomes to be delivered.

Bendigo and Adelaide Bank is known for its very strong cultural identity of feeding back into the prosperity of others, its customers and the community. This community focused culture is pervasive throughout the Bank and Cresp understanding the importance of this incorporated it into projects and change initiatives he put forward to ensure they resonated with staff and leaders.

One such example is Cresp sharing his top ten projects with his team and asking them where they can add value. "For me it's always about giving our engineers and technology leaders as much context as possible, to say these are the business outcomes we're looking for."

Cresp recognises there is also the need to understand the sequencing required and interdependencies between projects, technologies, business units and outcomes but to also manage these elements collaboratively. This is something the bank is getting better at and was estimated to have taken approximately 2 years to get "fitter at working between these interdependencies across the organisation".

3. Find innovative ways to support staff in changing ways of working.

Cresp reflects that the Bank was behind the cloud race 2.5 years ago and needed to do an uplift in training for the organisation, not just for the technology part but for the organisation more broadly. "Covid in one way was a great democratisation and virtualisation of learning. There was a whole heap of events that we were able to attend virtually that we could not have afforded to send staff to the US for. We got access to some great thought leadership virtually", said Cresp.

The bank found the learning uplift was greatly accelerated through that period and via the virtual platforms that had been whole heartedly embraced by the world.

The move to digital ways of working saw a number of valuable initiatives kicked off to share critical knowledge, lessons learned and to provide responsive support for project teams; Cloud Fridays and the Bendigo Pub are two examples. Engineers started having Cloud Friday sessions where they would talk about the two mistakes they had made and what they had learnt, the goal was to admit they were all learning, share their experiences and learn from each other.

The other initiative was driven by an aggressive migration project moving 30 apps in 30 days to get out of a particular data centre. To meet this deadline the engineer's needed answers to their questions immediately and so the "Bendigo Pub" was born. A virtual room where someone from the Banks team of senior engineers would be available to help and answer questions. The Pub was open from 8am – 6pm and facilitated drop-ins at any time.

(Continued Over)

Andrew Cresp, CIO, Bendigo and Adelaide Bank

(From Previous Page)

4. Identify early wins – they may not be what you expect.

After analysing their enterprise architecture to find any duplication, the bank decided document management would be a good place to start and provide an early win. This may be seen as an unlikely candidate for most organisations and something you would not expect from a bank where front-end customer experience is paramount. However according to Cresp, concentrating on the back office has paid a front-end dividend.

“Lending, and home lending in particular, is going to be people’s biggest decision in their lives and do they want to do it digitally through self-serve or do they want some help through it? My experience in core banking transformations is to say most people want some help.”

“There will be digital parts to it which are generally loan application capture, tracking the application and document uploads, but there’s lots of aspects like checking property value and credit history that must be done by back-office staff. Therefore, the systems and capabilities that you have there will differentiate you from a customer perspective in how quickly you can process an application.”

A use case that is driving the adoption of AI & Machine Learning (ML) is the Bank’s desire to improve the quality of metadata captured with Loan Application submissions and removing the reliance on Lending Managers and staff to classify these documents.

Cresp poses the question; ”will people understand the value chain in a complex 52 step loan origination journey? Experience says yes, no or maybe and this simply isn’t good enough”.

Metadata is essential for supporting the process and the long-term management of the loan. Poor-quality metadata makes it harder for staff to find all associated documentation – particularly 5 to 7 years after it was originally submitted and by staff that were not involved in the loan origination process.

Auto classification is a key focus of the EncompaaS implementation, with AI and ML to be used to identify and classify documents as they are created. This will remove the need for Bendigo and Adelaide Bank team members to manually classify documents, which will make the process faster, more accurate and improve overall compliance.

“EncompaaS can auto classify a certificate of insurance and put it in SharePoint so it can be found rather than having to go through a process of annoying people and asking them to go through it” said Cresp.

5. Understand regulatory intent to keep ahead of the wave of obligations

Bisset opened the next part of the discussion on regulatory compliance with a different perspective; “with regulatory oversight you don’t always want to be stuck on someone else’s agenda. You want to get to the spirit of the regulation, leverage what can give advantage and not just tick the compliance obligation box. Maybe this is something you both want to comment on?”

Over the past 7-8 years the financial services industry has seen enhanced regulatory scrutiny, at a time when both financial services institutions and the regulators were effectively learning how to capture the amount of data needed to understand what had gone on. From Engel’s experience the regulator would issue a notice and the Financial Services staff would scramble over the weekend to find the required documents.

“It became apparent that as an executive, as the board and as the regulator you needed to have confidence that you could know and show quickly that you could answer the question of assurance; have we met the obligation, are we continuing to meet the obligation and what does the control framework look like.”

These regulatory obligations require a continuing effort and on top of this in 2017 there was the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry which resulted in several new regulations being introduced and a whole new category of capability around Risk Management. Not only were the banks having to “know and show” against existing regulations but also the new regulations as well.

Over the past 7-8 years the financial services industry has seen enhanced regulatory scrutiny,

The regulatory demands on the business and its people were snowballing and not easily addressed by legacy and manual processes. Engel believes “it is incumbent on technology leaders to lift our compliance and risk friends out of the whiplashing environment they are currently in. Technology is now available that can help do this and provide greater levels of assurance that you are meeting your obligations.”

Regulation in any sector be it financial services, government or pharmaceutical sees compliance and risk professionals in a similar position, they all have the same type of burden. Organisations can't keep throwing more people at investigations, inquiries, or information requests in the hope of meeting their obligations, or simply put their hand out for a slap on the wrist and treat this as part of doing business. “Regulators are now looking for root-cause resolution to make sure these issues don’t happen again”, said Bisset.

Engel suggested that as financial markets continue to contract, the banking sector in particular cannot afford to underinvest in this space. And whilst an earlier comment suggested the majority of spending was on front end customer experience initiatives, regulatory compliance spend is more than you might think.

“There’s a lot of analysis that indicates the cost of regulatory compliance is 45-50% of IT spend in FSI and the amount invested in growth, customer experience and finding new markets is a lot smaller than you think it is. The environment that we are creating has to be much more efficient. We need to have higher levels of compliance and assurance at a lower cost and the RegTech services that EncompaaS offers absolutely answers that question,” said Engel.

6. Think about cloud projects differently to deliver high value outcomes

Bendigo and Adelaide Bank prioritised their cloud projects to deliver better services for customers, they chose metrics that reflected the value of work being done in the cloud as opposed to the volume of work being done.

“With our cloud journey we didn’t want our metrics to be we’ve got 500 workloads into the cloud. We wanted the most changed workloads and most critical workloads in the cloud because that’s where we think we can move faster for our customers”, said Cresp.

“That required us to have a really strong cloud governance framework and make sure we could demonstrate to our risk community within the bank, our executive and finally to APRA (The Australian Prudential Regulation Authority) that we were going through good processes and had good controls. The conversation was more about how to move from artefact-based controls to continuous compliance from a delivery perspective.”

The Bank found the regulator to be very understanding but attributes this in part to the large amount of information they provided (to the regulator) on the conversations they were having with the board, the executive team and the risk and compliance committee.

Of note was the alignment found between questions the regulator was asking and those that had been asked by the board, executives and the risk and compliance committee when Cresp met with them.

This gave the regulator confidence that the right conversations were being had at all levels of the business on what they were doing and how they were managing risk.

An unexpected upside to the cloud migration was that service owners who had moved their critical workloads to the cloud had the opportunity to speak in front of the board, the executive, the risk and compliance committee and APRA – an opportunity they would not normally get. This was used as a good coaching opportunity and helped them to get better and better.

7. Recalibrating for the hybrid workplace

Bisset suggested the past two years had resulted in many organisations being forced to address the pent-up demand for collaboration that was previously restricted based on risk and security concerns. “Today we are seeing an interesting intersection of these things and thinking about how technology has a role to play in security, privacy, data protection and accessibility - supporting process simplification”, Bisset said.

At Bendigo and Adelaide Bank, Covid and its associated lockdowns saw electronic signatures rolled out in 6 weeks and Cresp admits it wasn’t the technology that had been holding it back, “there was nothing like the necessity of those quick lock-downs to move some things really quickly”.

The disruption to usual work practices saw a recalibration. Teams connected remotely via a conference call or videoconferencing platform as if they were in the office – this practice was extended to individuals that were not able to come into the office due to symptoms to allow them to remain connected to the rest of their team.

Cresp was conscious of the need to provide an equivalent experience for remote workers to those who were physically in the office. Engel noted Microsoft’s global Work Trend Indexes show approximately 70% of people love the flexibility that hybrid work offers, but they still genuinely want some face-to-face time.

Further making an observation on how important it was to facilitate remote work and to think back to the concept of work being an activity and not a place (more information can be found here: Work Trend Index: Microsoft’s latest research on the ways we work).

The recalibration of the workplace and the move to remote working has highlighted the challenges associated with managing vast amounts of corporate information. Governance and Legal professionals don’t know about everything that is created, by who and where it is stored.

This is where technology has a role to play in helping discover, classify, understand and manage content across the enterprise so organisations are not relying on individuals to know where to put it or what to classify it as. Industry statistics have indicated typically less than 10%-20% of data ends up in the Records Management system as intended. This opens the organisation up to significant risk.

The Banks choice to consolidate its 13 document and records management systems by moving to SharePoint as a supported hub with an automation and supervision layer provided by EncompaaS over this (and other enterprise systems) is going to give staff a consistent experience and help fill in the blanks.

Bisset poses the following question to Cresp; “so, thinking about doing the heavy lifting with tech as a starting point what are you thinking about heading towards in the future? Is this getting you more towards robotic process automation or preventative measures?”

“From my perspective it is about improving the integrity of the data that we have and then determining what can we use this for that’s going to add business value. I don’t know the answer to that but people in our document management team are figuring out how to make processes easier for our customers.

“ It is definitely about getting that information into shape and providing a consistent experience. The benefit of having SharePoint as the central record is it is very familiar but the flip side is that people think it is easier to setup than it is when you’re configuring for enterprise use”, said Cresp.

Final reflections

Before closing out the discussion Bisset asks both Cresp and Engel for their final take aways. These final reflections have been distilled into seven key pieces of advice:

1. Technology is essential to address today’s regulatory requirements
2. Regulations such as GDPR and CPS234 are changing the way we think about data and demanding we know where documentation is held and that we can safely remove it as part of the information lifecycle
3. When moving through digital transformation you don’t have to start with everything, today’s technology allows us to tackle projects modularly
4. Building the monolith takes time and in that time business change has occurred. You could be implementing a solution that is already out of date
5. Accept there will be trade-offs because you can’t always follow the same process with legacy systems and business flows.
6. Establish a genuine learning culture, augment it to be more innovative and inquisitive
7. Look outside yourself and your industry to find places of improvement.

Making PDF/A conversion easier

By Dietrich von Seggern

PDF/A – the ISO standard for long-term archiving – now has four sub-standards. This raises an obvious question: which one should businesses use for document conversion and archival?

PDF/A has been the international ISO standard for long-term archiving since 2005. It guarantees reliable reproduction of documents for years to come, regardless of any technological, hardware or software innovations that may arise. It enables homogeneous archives of both born-digital and scanned documents.

Today, there are four variants of PDF/A, namely -1, -2, -3 and -4. Among these, PDF/A-3 stands out because, while the PDF file is still subject to design limitations (as with the other variants), it is also possible to embed any other file format into it. PDF/A-4 also permits this, but only in a special level of compliance known as PDF/A-4f.

There is no doubt that PDF/A-3 and PDF/A-4f should only be used in very specific contexts, since a diverse range of archive formats is to be avoided. But more on this later. For now, we will concentrate on the other variants.

PDF/A-1 vs. PDF/A-2 and PDF/A-4

The PDF/A-1, PDF/A-2 and PDF/A-4 sub-standards have some features in common: in general, they limit what features can be used in a PDF file. This means, for example, that no external content, JavaScript, encryption or videos are permitted. Fonts must be embedded and colours must be defined independently of any device (using ICC profiles for instance).

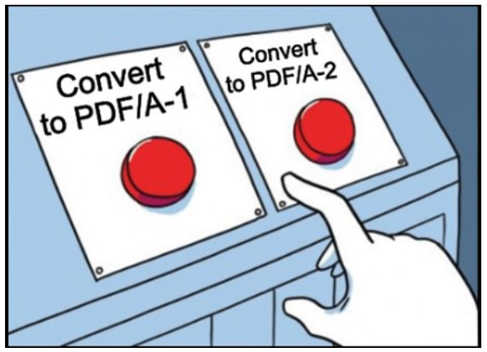
But how do these variants differ, and which should you use when? The key factor in this decision is the base PDF standard used in the variant. PDF/A-1 is based on PDF 1.4 (2001), PDF/A-2 on PDF 1.7 (2006), and PDF/A-4 on PDF 2.0 (2017). Each of these base standards introduced new features when it was launched. For example, layers and transparent objects can therefore not be used in PDF/A-1. This means that when converting to PDF/A-1, these kinds of objects need to be modified (flattened) and that means that information is permanently lost.

Another consideration that can have even more serious consequences is related to the fact that each new version of the base PDF standard also expanded the range of permitted internal values within a PDF file.

A PDF 1.4 file had to be processable at a reasonable speed with the kind of hardware that was used in 2001, and the specification therefore applied some limits to internal structures. We all know how hardware performance has increased since then, which allows for much wider ranges for such structures in newer PDF files. However, when converting a contemporary PDF file to PDF/A-1, you need to meet the values specified for PDF 1.4. In rare cases, that means making changes at the PDF's low-level internal structure.

Such low-level changes are sometimes only possible by replacing all content on a page with an image. This leads, of course, to a loss of information: for example, text stops being text and is now only an image of text.

A good converter will only take such drastic measures in very, very rare cases. However, the question is: why does this have to happen at all? There is no chance



that future hardware will drop back to a level of performance comparable with the year 2001. So, the easy answer to the question "Which archive format is the best?" is to make sure that the base PDF standard for the PDF/A variant is not older than the version of the archived PDF file. In most cases these days, this means PDF/A-2.

It is worth noting at this point that PDF/A-1 remains a valid sub-standard and has not been replaced by PDF/A-2, nor will that ever be the case with PDF/A-4 and PDF/A-2. PDF/A-1 files can remain to be in the archives forever; they don't need to be converted to a more recent standard. However, it is strongly advisable to archive new files in PDF/A-2. As of yet, it is not possible to give a strong recommendation for PDF/A-4, as the base PDF format, PDF 2.0 is still rare as of today.

Regardless of when PDF/A-4 will become the dominant variant, though, we don't consider it a good goal to have an archive only made up of PDF/A-1, PDF/A-2 or PDF/A-4 files. These variants build upon one another, so the better strategy is to adjust the variant used as needed—to the PDF/A variant that corresponds to the newest base PDF version of the files to be archived.

Use cases for PDF/A-3 and PDF/A-4f

Before we go, one final word on those special cases we mentioned before – PDF/A-3 and PDF/A-4f. From an archiving perspective, it is essential to limit the variety of file formats used; these variants therefore require a framework of additional rules. But there are striking use cases for them, that all have in common that there is a specific, defined relationship between the actual archive file and the files that are embedded within it.

An example are embedded source files – say, saving a spreadsheet alongside a PDF copy, digital invoices containing machine-readable datasets embedded into a human-readable PDF/A-3 file (for example ZUGFeRD invoices). Email archiving is another classic use case for PDF/A-3 and -4f. Here, the original email can be embedded in EML or MSG format, along with attachments.

In short, we can say that:

- Existing PDF/A-1 files don't need to be converted to a newer standard.
- It is a good idea to convert new files to PDF/A-2.
- PDF/A-4 is worth keeping an eye on, and:
- PDF/A-3 and PDF/A-4f should only be used in contexts where the nature of the embedded files is defined.

Dietrich von Seggern is CEO at callas software GmbH.

Top five ChatGPT uses in the workplace

by Chris Ellis, Nintex

It's both my job and my passion to keep up on the latest developments in technology. But for my dad, who is happily retired and can go days without opening his email: not so much.

When I was visiting my folks last week, I introduced my father to ChatGPT. After less than an hour of playing around with the sophisticated AI chatbot, he was obsessed and has since called me multiple times to discuss how he's now using this AI in his day-to-day life.

Sure, there is a lot of hype about ChatGPT and how it will transform work and society. But we've already heard that recently about blockchain and the metaverse, only to see both struggle to gain mainstream traction - so far, at least.

However, seeing my dad's reaction to ChatGPT really got me thinking. If someone like my father can find so many inspirational applications for ChatGPT, I can only start to imagine what it can and will do for organizations. And utilizing ChatGPT will only help to reveal new questions, ideas, and use cases.

Here are my recent thoughts about the top five applications of ChatGPT in the workplace:

1. Customer service

When contacting customer service, nearly 80% of people prefer to interact with a human versus an automated response.

Frustrating bot-based customer service is bad for a brand. Yet, it is difficult and expensive to offer comprehensive human customer service. ChatGPT upends this calculus.

ChatGPT can learn and build upon answers and responses. When connected to an internal database, it will change our ability to respond to organization-specific customer service requests like "How do I get a permit?" or "Where is your nearest office?"

Moreover, it will be able to create content and lay out answers in a visual format, like "Please send me a report of last month's sales."

2. Language translation

We live in a shrinking world where it is increasingly essential to communicate across regions, languages, and cultures. Existing translation technologies help with short questions and commands and can interpret small blocks of text.

That is a start, but ChatGPT has the reading and comprehension capabilities to understand longer materials—and take translation to the next level.

ChatGPT can determine an employee's location and automatically translate pages of content into the person's local language.

For developers and other technical talent who don't speak English or Mandarin, this will save an immense amount of time, effort, and expense to bring their work to market — time that can be rededicated into improving the experience of the end user.

There is also great potential for ChatGPT to build automated assistive workplace technologies like real-time screen readers and sign language translations for people with disabilities.

3. Summarizing

Email was supposed to speed up work correspondence, so we'd all have more time to focus on deep work. Instead, we ended up filling our days with ever more correspondence with more and more people.

Newer work messaging platforms have only increased the deluge of communications. From emails to messages to reports, ChatGPT can summarize and deliver key information to busy employees.

When incorporated with Word or Outlook, ChatGPT will be able to distill information and separate out what you really need to know. It will be able to take an email, turn it into an action item, and place it into a workflow that is shared with a wider team.

Less time spent responding to correspondence and playing catch-up means more time spent on work that adds value to your company.

4. Content creation

The other side of the "ability to summarize" coin is the ability to create outgoing writing and visuals from email responses to reports to external-facing online content.

Employees may not be able to turn all of their writing duties over to ChatGPT, but they will definitely be able to unload a number of the more routine responsibilities and get writing ideas and support where they need it.

Yes, ChatGPT can answer an email and fill out a leave request form or other in-house paperwork. But it can also create a 10-step health and safety hazard report or a blog detailing business performance or a new trend.

In recent years, even the most technical of employees have been tasked with a degree of creative writing responsibilities in their communications and internal marketing of their work. ChatGPT can be a dependable partner to greatly alleviate that burden and, sometimes, remove it altogether.

5. Code validation

From workflow builds to suggestions, ChatGPT can kick off, review, and improve code. Whether getting you going with a solid framework or drilling in on existing work to determine how to enhance and optimize, ChatGPT supports coding much in the same way it supports writing.

Technological innovation increasingly relies on citizen developers who have a great idea or insight to meet the needs of their organization but have little or no formal training in programming.

ChatGPT is a crucial tool to facilitate the work of citizen developers and help them to achieve coding goals that were once beyond their reach.

As I've seen with my father, ChatGPT has struck a chord with people who previously didn't understand that AI could have a role in their lives. When AI goes from the theoretical to the practical, as in the case of ChatGPT, it creates a juggernaut of use cases and applications. And it will have a profound impact on automation and the world of work. There are still a lot of things that ChatGPT can't do. But we can keep learning and defining new ways for it to enable us to work in ways that are ever-more to our liking.

Chris Ellis is Technical Director at Nintex This article originally published here.

20% of Inbound Contact from Machine Customers by 2026: Gartner

By 2026, 20% of inbound customer service contact volume will come from machine customers, according to Gartner, Inc. Advances in Conversational AI, Automation, and Low Code Resources will have a huge impact on interactions with Customer Service.

Machine customers are nonhuman economic actors that obtain goods or services in exchange for payment. In customer service and support, they will resemble virtual assistants or smart devices that perform customer service activities on behalf of their human customers, such as reporting issues or gathering product information.

"Machine customers will reset customer expectations about what constitutes a low-effort experience, creating a greater competitive gap," said Uma Challa, Sr Director Analyst in the Gartner Customer Service & Support practice.

"Organisations that embrace them will be able to differentiate their value and close the gap by meeting this new standard for effortless service."

By 2024, Gartner anticipates 100 million requests for customer service will be raised by smart products.

Initially, machine customers will be best served in enterprise chatbot channels due to that channel's ability to serve these requests at scale. Smart organisations will start to invest in conversational AI platforms (CAIP) to enable bot-to-bot communication.

"Organisations without a machine customer strategy in place won't have a good way of distinguishing between human and machine customers," continued Challa. "They may see their non-chatbot channel performance get worse without understanding why."

Customer Service Rep Automation Also on the Rise

Customer service reps are increasingly automating portions of their job to make their work easier, often but not always using company-provided tools to do so: Gartner anticipates 30% of reps will do so by 2026.

Examples of self-automation activities include using quick auto-response technology in emails to customers or using an unauthorised third-party call recorder to transcribe customer calls.

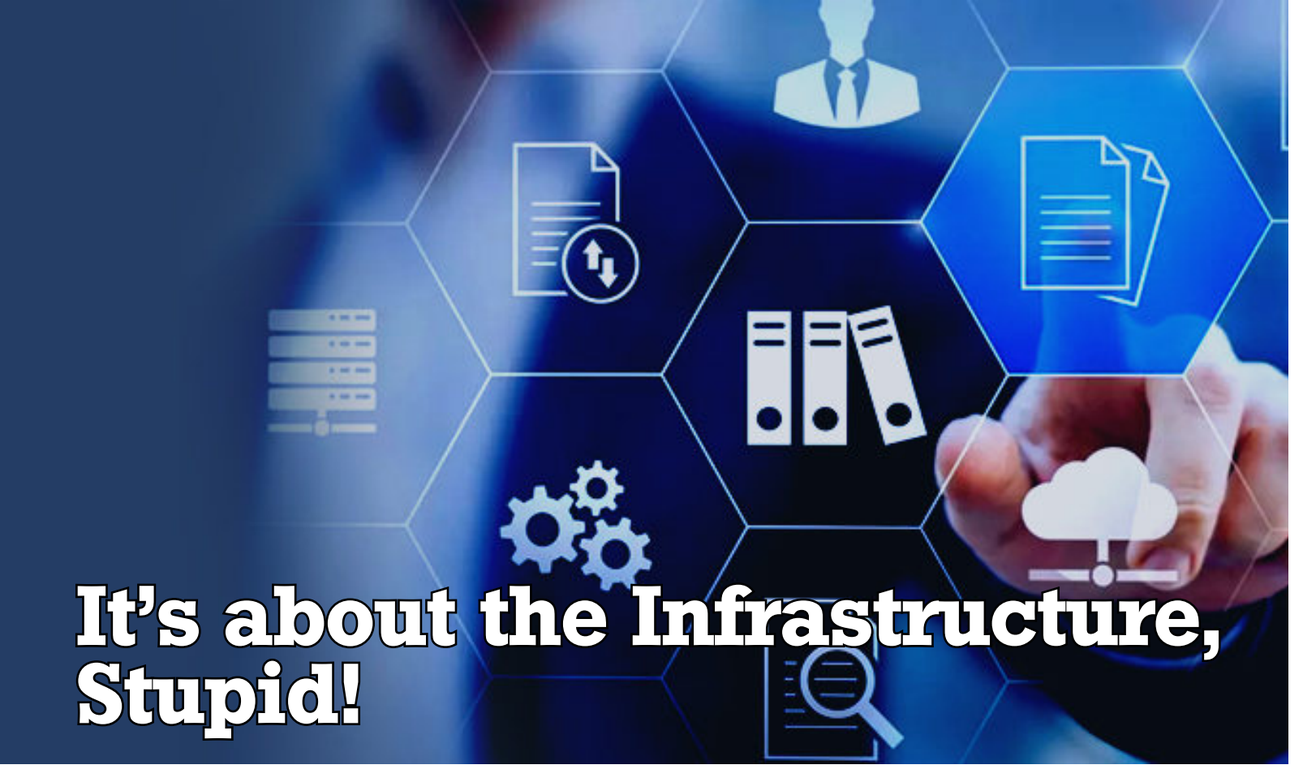
"While self-automation has been happening for a while in the software space, this trend will become more present internally in customer service because reps now have improved access to automation tools," said Emily Potosky, Director, Research, in the Gartner Customer Service & Support practice.

"Emerging resources such as AI models (e.g., Github Co-pilot, OpenAI's ChatGPT and Codex) will continue to make coding more accessible to reps, regardless of their skill level."

With this in mind, Gartner expects there will be a greater variety of products in the marketplace centred around employee automation, specifically, low- or no-code solutions targeted at reps to help them self-automate. Vendors that offer collaboration platforms may also increase investment in coding features to allow for groups of reps to work together to self-automate.

"Customer service and support organisations that not only allow but authorise self-automation will become more competitive than those that don't, as reps will notice and correct inefficiencies that leaders are unaware of," said Potosky.

"These organisations may also become more attractive employers, because potential job candidates are likely to appreciate the organisation's flexibility and openness to innovation."



It's about the Infrastructure, Stupid!

Arnold von Büren, CEO of TCG Process, is a Swiss entrepreneur with three decades of experience in capture and input management. On a visit to Australia in February, IDM asked Arnold to outline his views of the current state of Intelligent Document Processing (IDP).

IDM: What is the source of the technology behind TCG Process

AvB: It's all our IP and the only technology we integrate is for document classification. We've been developing the platform for 10 years since going it alone and moving away from external providers as well as expanding internationally to go global into many countries around the world. We have expanded into areas we are happy with, and I am very much a believer that we need a local presence in countries where we are looking to play. (TCG Process' ANZ subsidiary opened in Sydney in 2020 under Managing Director Frank Volckmar).

We use the word orchestration quite a bit. Some might refer to it as workflow or Business Process Automation (BPA) We consider ourselves more in the BPA space than the capture space, providing a level of verification that can increase the success of capture and recognition to much higher levels.

IDM: Can you explain in a bit more detail how TCG Process leverages AI and other technologies to deliver fast and accurate outcomes?

AvB: The only place where we use AI at the moment is in our classification technology and the rest is machine learning or self-learning. We are cheating in a way. We always try to get what we find and compare it with the customer's data and that gives us a lot of hints as to what's right and what's wrong. That's another disadvantage when you are somewhere in the cloud and your AI is 100% OCR but it's not validated against your data. What we try to do is provide very early access to the database and use that data to verify what we find in the document. So, yes, we need access to the data which is sometimes not that easy because people are reluctant to provide it, but when we have that we get much better results.

We try to differentiate between validation and verification. Validation is making sure the content that was on the document is now in the fields. Verification is making sure the field content corresponds with the database content. Turning it from business data into business information.

But we are not only comparing against the database we also establish rules within the system so we can be really sure that when data leaves our system it is absolutely correct with no more steps needed and you can run the transaction.

IDM: Where do you think the main opportunities lie in this region for intelligent document processing solutions?

AvB: Everywhere. We thought that Invoice Processing was only a replacement business, but it's still a huge opportunity. Many companies are still lagging far behind with digitisation and are upgrading their AP OCR platforms to enterprise IDP so they may use the same platform to automate ingestion of all business information. And you can only automate if you digitise and normalise all the incoming documents and data streams. There are still huge opportunities.

Companies that have "digitised", they may have a portal and take things in by email and other means but they haven't automated. But there is a huge gap between those inputs and their backend systems, with all kinds of administrative staff performing a lot of mundane tasks. That could be elevated with automation and done much better without mistakes and errors.

Customers, suppliers and employees are hammering your business everyday with emails. Enter the new ingestion challenge - emails with a multitude of file formats attached, or embedded, or emails attached to another email. Download TCG's Solution Guide **HERE**

Its fine to digitise incoming content but you may end up with 59 different document file types, which is impossible to open and review. You need to "normalise" those files so they fit on one screen and then extract the information and run rules and processes as a starting point for automating processes.

Many companies have created a Chief Digitalisation Officer. I think it's the wrong title, it should be Chief Automation Officer. Digitising is just the first step; you must then normalise and automate.

IDM: Do you think organisations need to take a step back and reconsider the suitability of public cloud capture offerings?

AvB: People are hesitant about going into cloud. First it must now be a local cloud for the local country which makes it a little tougher for the suppliers. But it's no longer an issue about the software technology, the important thing is to have a tool to orchestrate all these services. In the beginning you must do capture well and then deal with the document, the OCR, the AI, the classification.

What's interesting for me is that everybody gets so excited about the technology and sometimes I say, 'amateurs are excited about technology, experts talk about the infrastructure'. Everyone's excited about new technology, everyone's excited about ChatGPT, but how do you bring it into your system, how do you integrate it? That's where the strength of our product lies. The interesting thing for me is that many of these AI offerings pretend to have a solution but they only have the OCR, a sliver of the whole project. OCR is the enabler of a solution but not the answer. The cloud offerings are great but they must be orchestrated to create value.

Artificial Intelligence (AI) in a way is a scam, as its never right. There are so many places in business that you need to be 100% right. In classification you can get to 70% with AI but that's as far as you can get, so for 30% you are back to manual and need some diligent eyes and hands somewhere to manually process. When we apply our technology, we get up to 85-90% automated throughput.

IDM: Following events in 2022, information security is now very much front of mind in Australia. You highlight some of the issues in in hosting data sets for training AI. Do you think there is a lack of awareness of the risk?

AvB: Absolutely. And something has to happen first before people will realise. Just recently we had Microsoft go down with certain services in the cloud. The risk of a data leak is always there. We see even today that companies are very reluctant to put everything in the cloud. I think it will remain a very hybrid environment with the really crucial data kept on-premise or in a private cloud.

It always makes me nervous when I see hype. It should be all about the integration, the infrastructure, that's what you need to be concerned about.

IDM: Microsoft has announced a number of solutions such as Syntex, AI Builder and Azure Applied AI Services. Is Microsoft offering a competitive platform for Intelligent Document Processing (IDP)?

AvB: No. I mean look at how many customers Microsoft has. Billions. They can't have a technology that fits everybody. It has to be very, very generic. We are very much a Microsoft shop but it's important to find a solution that works for your organisation. It might include a piece of Microsoft AI it might be some Google Cloud technology, or something else from a third party. The great thing now is its all open so you can integrate almost anything (plus you can also throw out things when you see that they do not work.) I hold Satya Nadella in high regard, but it seems almost childish the way they jumped straight onto ChatGPT which wasn't even grown in their garden, they were just the quickest to give them massive computing power and now they are hyping it. Then Google brings out Bard.

OCR is now quite commoditised and what's important and adding value is process automation. Microsoft and Amazon are now providing generic OCR which you can access as a service, but it will only get you part of the way there.

IDM: Can you discuss the future developments and advancements in intelligent document processing technology?

AvB: IDP is excellent for collecting and understanding incoming business information, whether structured, semi-structured and more recently unstructured, from forms to invoices to medical reports, and we are focused on continuing to improve the options for how organisations "act" on the information. This is today's process automation or orchestration value add. By being able to ingest any type of document from any channel, IDP platforms must be able to integrate, at any scale, into a customer's infrastructure, flexibly, securely and simply to ensure business information is automatically acted on quickly and cost effectively.

IDP is becoming more about the underlying architecture and fit with infrastructure to ensure organisations are able to leverage every opportunity to verify data and act upon it effectively. The architecture of IDP offerings is evolving and legacy applications will find it increasing difficult to adapt.

The beauty of our platform is it can use any new technology that is developed, which we can then integrate. Our platform uses Microsoft Cognitive Services if you choose to, it can use one of our competitor's OCR engines if you choose to, Tesseract, Google, all those are integrated on the platform. So, whatever you believe is the best OCR engine for your application we will integrate and then plug into different information sources and leverage all the data points in your infrastructure to make sure that what you are looking at when you have captured something is right.

www.tcgprocess.com/en-en/australia/

Arnold von Büren, CEO of TCG Process, was a founding member of DICOM Group plc. and played an instrumental role in the acquisition of Kofax, Inc. USA, becoming Kofax CEO in 2000. Since 2007 he has been CEO of TCG Process, providing leading process automation software to businesses of all sizes and growing the company into a global organization with more than a dozen subsidiaries across Europe, the Americas and Asia Pacific.

Assessing ROI for Intelligent Document Processing (IDP)

By Jeff Leibovici, TCG Process

Measuring return on investment for document automation solutions used to be pretty simple: reducing data entry reduces headcount. But simply reducing resources to measure ROI and business benefits isn't as straightforward as it used to be. In fact, many companies would prefer not to reduce headcount but rather ensure resources are working in harmony with advanced technologies to drive scale and innovation.

Let's start at the beginning; nearly every business process starts with a form or document, digital or paper, one that contains key information which requires action. Optical character recognition (OCR) technology, often tasked with getting that information from these documents, has been around for several decades.

What began as basic OCR to eliminate re-keying of data from scanned paper forms (structured data), progressed to recognition of semi-structured data such as that from invoices, and has evolved to what we have today: a combination of artificial intelligence (AI), machine learning (ML) and OCR to process unstructured data, information from the most complex (non-standard) document types. It's most often referred to today as intelligent document processing or IDP.

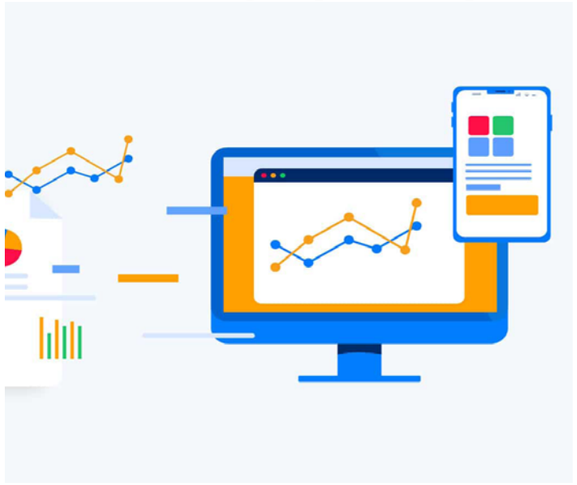
Through this technological evolution, automating business processes has also evolved, from forms and invoices to insurance claims, loan applications, human resources processes, digital mailrooms and all document-driven processes in between.

Companies have been automating accounts payable (AP) for years because the tech is proven and has clearly demonstrable hard and soft benefits: lower operating expenses by reducing administrative overhead; eliminate lost invoices and duplicate payments; improve supplier relations; capture early payment discounts, and so forth.

When digitising your mailroom or automating loan processing, business leaders focus on the commercial business case, largely hard costs, yet may trip up on the hidden, and often future cost of using outdated document processing technologies. Soft cost saving or earnings are often ignored or treated as rounding errors with business cases being approved on 12 month hard cost return on investments.

While automation does yield substantial savings, it is important to future proof investments through careful selection of underlying IDP technologies.

Over the last few years, more of us have been working from home and companies have had to quickly adapt their IT landscape to ensure employees could work remotely without interruption to their daily business activities (or security risk). This has meant, in many cases, expensive upgrades to existing systems that weren't browser based (and therefore accessible anywhere, anytime). Nowhere in an organisation was the impact greater than in the mailroom.



Many have had to rely on fewer resources on site, and therefore companies are far behind in mail processing. And this, as we'll discuss, has directly resulted in poor customer and employee experiences.

Often, when companies start to dig into upgrading systems, it comes to light that there are many solutions that have been purchased to satisfy capture and document automation. Often, there is a complex mix of IDP, RPA and BPM as well as department-specific solutions that all are being supported by the IT organisation, and don't take advantage of economies of scale. Reducing the volume of technologies supported, in addition to adopting solutions that are multi-departmental or enterprise in scope, is a great area to realise cost and efficiency savings.

Of course, software isn't going to solve opening an envelope but investing in browser-based solutions, IDP or otherwise, reduces hardware and IT costs, such as hardware (lap/ desktops) for the remote worker, upgrade costs, additional security for remote access (e.g., Citrix and two-factor authentication), more processing power; and additional licenses. It has well-documented and proven operational benefits, too. Simply login and start working, anywhere, anytime.

Invest in a modern IDP solution to ensure efficiency and collaboration gains

As with anything you purchase, no two solutions are created equal. Nowhere is this truer than among the myriad of IDP offerings in the market.

A shared soft cost between IT and the business user (also known as a subject matter expert) is time spent documenting processes and then mapping these new process flows into the selected solution. BPMN, the acronym for Business Process Modelling and Notation, is often used to collaborate on specific business processes in a business process model.

Simply put, it means the subject matter expert (SME) and IT can easily collaborate on the design of a process; when organisations select solutions that offer in-built BPMN functionality, it means processes are in production far quicker than if an organisation is solely reliant on IT for design. Faster time to deployment means you can realise the business benefits of automation more quickly and less reliance on IT means you are saving IT resources, and therefore costs.

The no-code dream is often not the reality

Many technologies today claim to be fully "no code", promising to eliminate a dependency on custom development costs. However, there can be a limit to scalability and flexibility. The best solution is one that is no code where it should be, and low code where it needs to be. With this type of solution, anyone who understands the business process and has good PowerPoint or Excel skills can design a process.

This allows for a configuration-led approach for non-technical users that increases the speed in which process changes can be made, but also provides extensibility opportunities for developers, allowing for ongoing innovation. With modern solutions, an SME can often make the change themselves and the organisation is back in production in a matter of minutes, not weeks.

Measure twice, cut once (but for similar processes)

In addition to cost savings and efficiency of collaboration, a no-code solution with reusable processes means you can onboard new departments, stakeholders or customers with the same process quickly and again, with far less IT overhead to do so. This has proven to be especially beneficial to outsourcing organisations or service bureaus (BPOs) who often repeat the same process for many customers.

Machine Learning and AI in IDP represents a plethora of business and technical benefits

One of the most widely used processes for ML and AI is in the mailroom, processing high volumes (of unstructured documents) quickly and accurately. ML and AI has been specifically developed to automatically determine (classify) each document type and its content and do something with it. Whether sending the document to a person, department or into an automated solution for AP, claims or loans, imagine never having to open a corporate email again?

And as you keep using the solution, the rate of straight-through processing is going to improve exponentially - realising huge time and process efficiency gains.

Consider the commercial impact of the solution in place today

Consider how many people you have administering your corporate mailboxes, opening every email and attachment (let's hope they all have the supported viewers for all the various file types you receive), determining the content and taking action. It's a painful and time-consuming task.

And if you're like many of our customers, these administrators aren't adding customer value by confirming receipt to the customer or connecting the mail to downstream processes - they're simply gathering and redistributing mail. Most often these administrators are saving communications to a shared folder where users are required to access and find their own information, too. All of which is incredibly time-consuming and inefficient.

In the last few years in particular, organisations have seen the volume of documents grow by almost 60% across verticals such as insurance, banking, government, and healthcare. However, customers, suppliers and regulators are still expecting a digital experience and timely responses.

Manual processing means you can't control costs, but there's a bigger threat too: regulatory breaches, risk of fraud, and poor customer experience, to name a few. Automation will drive down operating costs and prevent security and compliance risk around the document, dossier (or case) and entire process. Advanced automation helps drive operational excellence, such as database look ups and integration to your existing business rules and business systems.

Estimating commercial impact and returns requires a thorough analysis of the resources deployed to current processes along with the associated performance metrics and their impact on customers, employees and cadence.

The "to be" process is then designed and evaluated through the same detailed lens to identify improvements to customer experience, employee experience and operating costs. The monetisation of the soft or hidden benefits is difficult to find agreement on across all stakeholders so is usually omitted from the ROI equation.

It is used, however, to check alignment with overall strategy and values - for example, is it a step in the direction of improving the digital experience for customers that we will have to take someday; does it align with workforce or market trends; does it align with our purpose and is it viewed favourably as such by employees?

Let a next generation solution prove the ROI for you

To achieve true ROI, both commercially and technically from an IDP investment, be selective with your vendor choice. Consider how you'll centralise your processes digitally, encourage customers and suppliers to submit everything electronically and, when choosing an IDP solution, look for a cloud-enabled platform. No-code, AI- and ML-enabled solutions will offer the best potential for improving the experience for your customers, suppliers, employees and shareholders.

IDP automation is a well-trodden path with 20 years of proven benefits, and it is now the first-and most important-step in driving the digital enterprise. Organisations need greater vision and leadership in taking their document-driven business processes to the next level, the level customers and stakeholders are coming to expect.

TCG Process offers an enterprise-wide solution to tackle intelligent document processing and automation with significant ROI. Swisscom not only realised efficiency savings but identified a new revenue stream with its DocProStar solution; read more about it at TCGProcess.com.

Jeff Leibovici has over 20 years' experience working with leading APAC companies automating document driven processes. from the early adoption of OCR to the latest Intelligent Document Process Automation technologies, Jeff is a digital transformation expert. Jeff leads the TCG Process enterprise sales team in ANZ and is engaged with senior executives and their outsourcing partners to help improve the customer experience, reduce operating costs, mitigate risk and ensure regulatory compliance.

Kodak Info Input Solution

Data Capture and Automation for Everyone, Anywhere

Digital Transformation Challenges

When organizations look to implement enterprise level capture and automation, they're faced with an array of challenges. They must find innovative ways to handle the complex nature of fragmented office locations. With the influx of home and remote workforces growing, these locations often span across multiple countries, amplifying the pain points associated with digital transformation.

Enterprise Level Complexity

Each day throughout your organization, people use different devices and applications to capture business-critical data. The spectrum of capture needs is constantly expanding across organizations, requiring agile and efficient solutions. Legacy capture systems demanding high-touch maintenance are no longer an option.

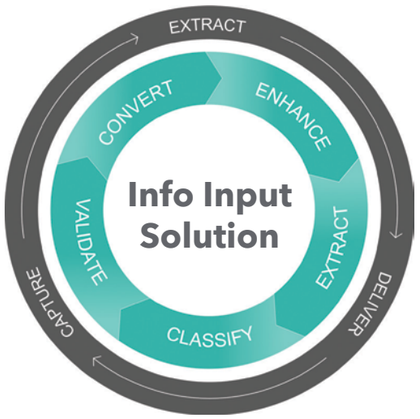
These locations will also have made investments in enterprise business applications requiring integration. Having downstream automation capabilities without automated capture capabilities means you are only automating half a process. In a mobile world, work happens everywhere. This is where web-based capture solutions are critical to your success.

Kodak Alaris is where Digital Transformation Starts

Info Input from **Kodak Alaris** is like a conductor, directing your data from various sources across the enterprise. It's a powerful web-based solution that intelligently captures, extracts, and delivers information to drive business results. This gives your entire organization the flexibility to connect people to documents, documents to processes, and processes to systems.

Web-based Automation for All

Info Input requires just a single instance in a single location, giving all users access to consistent automated processes through an intuitive web-based interface. It greatly reduces your IT workload and shortens maintenance time with the central administration of all users and business rules.



Automatically turn volumes of scanned data into information that's ready to use

"This solution has virtually 100% uptime, which is amazing considering we have over 6,000 users throughout the state responding to requests for vital services."

– IT Director, State Department of Human Services

Extend your capture and automation to the edge of your enterprise

With **Info Input Solution**, you can easily capture complete, accurate information on the first scan. The intuitive user interface requires minimal training and reduces errors with one-button easy scanning from within your business applications.

Capture data using a mobile app or extract it from a variety of digital file types across your organization, even off-site. Intelligent features like **classification**, advanced indexing and extraction get information into your business processes quickly and accurately.

Benefits you can expect with Info Input Solution

- **Scalability:** Grow with your data capture needs - from a single department to complex, high-volume enterprise requirements
- **Customer Satisfaction:** Streamlined, efficient business processes empower your decision makers and increase customer satisfaction
- **Increased Productivity:** Automatically determine document types and extract data without having to manually sort files
- **Reduce Costs:** Realize savings in setup, maintenance, and software updates using web-based deployment and management

Enterprise Level Integration

In today's connected world, integration and connectivity is everything. **Info Input** can be integrated into multiple business systems, which is key to driving productivity on an enterprise scale.

The process of digital transformation does not necessarily have an end goal, rather a constant state of opportunity that businesses need to capitalize on. That's why **Info Input Solution** has integration into some of the leading document management, ECM and workflow solutions in the market.

Enterprise-level Automation that Scales with you

Changes in the way we all work have led to a boom in digitization efforts and the need for distributed data capture solutions. Regardless of your size, you need a flexible solution that goes to work for you.

Info Input provides a simple and flexible way to deploy and manage your information capture and automation systems. It transforms your data input sources in a distributed environment to improve processes across the enterprise.

Get in contact with a Kodak Info Input Solution Specialist to see how we can help streamline your document capture process across your enterprise.

Kodak Info Input Solution integrates with leading ECM, workflow solutions

Want to learn more?

Contact the Kodak Alaris Australia Team
Email : Service-Anz@KodakAlaris.com
Dial Toll Free No : 13002 52747

Services from Kodak alaris

Infosource ranks Capture & IDP Vendors

Infosource Software has released its annual Capture & Intelligent Document Processing (IDP) Vendor Matrix and accompanying report. The Global Matrix and Report ranks 20 leading Capture & IDP SW vendors, based on Strategy and Capabilities (y-axis) and Execution in the market (x-axis).

The vendors are divided into four categories: Star, Disruptor, Contender, and Explorer.

"The Capture & IDP market has exploded with entrants over the past five years; the impetus being the widespread introduction of AI and machine learning into applications in this market," said Ralph Gammon, Senior Analyst for Infosource Software and the lead author of the report.

"This has made our job in ranking the vendors more complex than ever. Applied intelligence is one factor we consider; we also look at capabilities in areas like cloud services and multi-channel input, as well as the vendor's vision for end-to-end automation.

"On the Execution axis, market share, strength of partner channel, ease of implementation and competitive advantages are all considered."

Vendors classified as Stars show strength on both axes. Disruptors are stronger in Strategy and Capabilities, while Contenders are stronger in Execution. Explorers show potential to emerge as leaders in the future.

The Stars from last year's matrix remain unchanged with OpenText, IBM, and ABBYY leading the way.

For this year's matrix, Infosource, which also publishes a report that sizes the Capture & IDP market, increased the weighting of market share.

"OpenText's strong market position and partnership programs make them a leader in Execution, while their continued innovation, vision for the future, and ability to incorporate Capture & IDP as part of an end-to-end solution make them a leader in Strategy and Capabilities," said Gammon.

"These strengths enable them to once again earn a Star position in our matrix."

Microsoft, as a new entry in market study, positioned next to TCG Process as leaders in their quadrant.

"TCG Process' aim of offering a solution that focuses on end-to-end process automation aligns with our vision for the future of the market," stated Gammon.

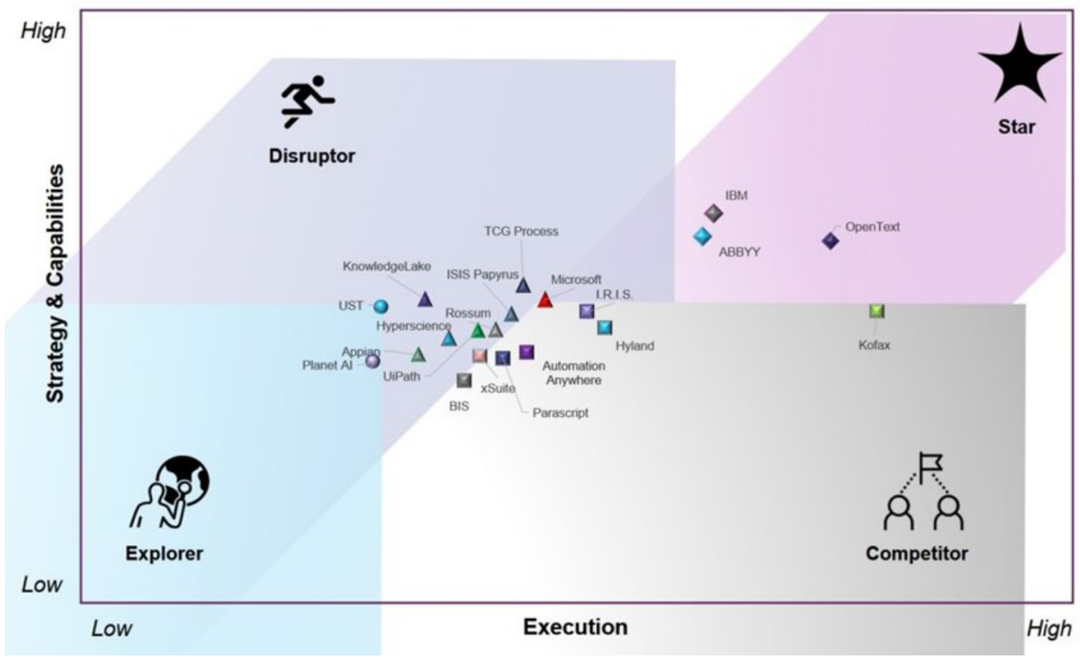
"TCG Process offers a scalable solution that goes beyond Capture. It features the ability to model and orchestrate an entire document-driven process.

"TCG leverages its own IP as well as that of third-party offerings from vendors like Microsoft, Google, and Amazon to automate classification, extraction, and document flow. This creates an extensible and flexible solution that stands out in the market."

TCG Process CEO Arnold von Bueren commented, "We are pleased to be featured again as a mature vendor and leading disruptor in Infosource's 2023 report and be positioned next to Microsoft, a company that we have great respect for.

"We feel our unique approach to process modelling and orchestration alongside advanced intelligent document processing capabilities set TCG Process apart, and we look forward to continuing to scale our growth as 2023 will bring some exciting new expansion announcements."

2023 Infosource Global Capture & IDP Vendor Matrix



COMPANIES WITH ANSWERS AND SOLUTIONS FOR YOUR DIGITAL TRANSFORMATION INITIATIVES

ezescan
making digital work

EzeScan is one of Australia's most popular production capture applications and software of choice for many Records and Information Managers. This award winning technology has been developed by Outback Imaging, an Australian Research and Development company operating since 2002. Solutions range from centralised records capture, highly automated forms and invoice processing to decentralised enterprise digitisation platforms which uniquely align business processes with digitisation standards, compliance and governance requirements. With advanced indexing functionality and native integration with many ECM/EDRMS, EzeScan delivers a fast, cost effective method to transform your manual business processes into intelligent digital workflows.

EzeScan benefits include: initiate intelligent automated processes; accelerate document delivery; minimise manual document handling; capture critical information on-the-fly; and ensure standards compliance.

www.ezescan.com.au | info@ezescan.com.au | 1300 393 722

newgen

Newgen offers a unified digital transformation platform that includes native process automation, content services, and communication management capabilities. Globally, many successful enterprises across various industries rely on the NewgenONE digital transformation platform—a comprehensive and unified cloud-based platform with low code capability for rapid development of content-driven, customer-engaging business applications. The platform can transform and simplify complex business processes. Equipped with cutting-edge technologies, including mobility, social listening/sensing, analytics, cloud, artificial intelligence (AI), machine learning (ML), and robotic process automation (RPA), the NewgenONE platform helps enterprises stay ahead of the curve. From grass-root citizen experience management, dynamic case management to electronic documents and records management, lending to underwriting, the platform solves multiple use cases across various industries, including government, banking, insurance, and others. Furthermore, Newgen has a robust partner ecosystem, including global system integrators, consulting and advisory partners, value-added resellers, and technology partners.

newgensoft.com/home-anz/ | info@newgensoft.com | +61 2 80466880

INFORMOTION
SMARTER SAFER FASTER

INFORMOTION is an innovative professional services organisation specialising in the design and implementation of modern information management, collaboration and governance solutions – on-premises, in the cloud or hybrid. INFORMOTION's workflow tools, custom user interfaces and utilities seamlessly combine to deliver compliance, collaboration, capture and automation solutions that provide greater business value and security for all stakeholders. We can help you map and successfully execute your digital transformation strategy. Boasting the largest specialist IM&G consulting teams in Australia with experience that spans over twenty years, INFORMOTION consultants have a deep understanding of business and government processes and the regulatory frameworks that constrain major enterprises. Our compliance experience is second-to-none. INFORMOTION is a certified Micro Focus Platinum Partner and global Content Manager implementation leader. We are also an accredited Microsoft Enterprise Business Partner, Ephesoft Platinum Partner and EncompaaS Diamond Partner.

informotion.com.au | info@informotion.com.au | 1300 474 288

AvePoint

Collaborate with confidence. AvePoint is the largest Microsoft 365 data management solutions provider, offering a full suite of SaaS solutions to migrate, manage and protect data. More than 8 million cloud users rely on our solutions to make their organisations more productive, compliant and secure. Founded in 2001, AvePoint is a five-time Global Microsoft Partner of the Year and headquartered in Jersey City, New Jersey.

AvePoint Cloud Records is a SaaS based, IRAP certified and VERS compliant solution used to manage the information lifecycle including content classification; retention and disposal; comprehensive auditing; reporting; and physical records. The Public Office Record of Victoria (PROV) has certified that government agencies and enterprise customers alike can leverage AvePoint Cloud Records to overcome physical and electronic records management challenges around authenticity, reliability, and ensuring content is maintained in a compliant format long-term.

www.avepoint.com| sales@avepoint.com | (03) 8535 3200

CyberRes
A Micro Focus Line of Business

CyberRes is a Micro Focus line of business. We bring the expertise of one of the world's largest security portfolios to help our customers navigate the changing threat landscape by building both cyber and business resiliency within their teams and organizations. Today, data is at the core of both value and risk. Organizations need to know what data they have. As data volumes continue to grow in both structured and unstructured applications, many organizations have also seen their cloud object and file stores grow as they accelerate their cloud objectives. Voltage Data Discovery enables organizations to gain a deep understanding of the data contained within structured and unstructured data repositories. This understanding helps detect value and risk, and protect sensitive and high-value data, while providing flexible approaches that evolve to serve your needs over the different use cases throughout the lifecycle of your data..

www.microfocus.com/en-us/cyberres | (02) 8281 3400

Kapish®
a Citadel Group Company

Kapish is a member of the Citadel Group (ASX:CGL).Citadel solve complex problems and lower risk to our clients through our tailored advisory, implementation and managed services capabilities. With over 250 staff nationwide and an ability to 'reach back' and draw on the expertise of over 1,500 people, we are specialists at integrating knowhow, systems and people to provide information securely on an anywhere-anytime-any device basis. Servicing both large and small, public and private sector organisations across all industries, our team of highly qualified staff have global experience working with all versions of Micro Focus Content Manager (CM). It is this experience coupled with our extensive range of software solutions that enable our customers and their projects to be delivered faster, more cost-effectively and with more success. At Kapish we are passionate about all things Content Manager. As a Tier 1, Micro Focus Platinum Business Partner, we aim to provide our customers with the best software, services and support for all versions of the Electronic Document and Records Management System, Content Manager. Quite simply, our products for CM make record-keeping a breeze.

kapish.com.au | info@kapish.com.au | 03 9017 4943

ESKER®
Document Process Automation

Esker is a global leader in cloud-based document process automation solutions. Esker's solutions are compatible with all geographic, regulatory and technology environments, helping over 11,000 companies around the world improve efficiency, visibility, and cost-savings associated with the processing and exchange of information. Founded in 1985, Esker operates in North America, Latin America, Europe and Asia Pacific with global headquarters in Lyon,

France and U.S. headquarters in Madison, Wisconsin and AUS/NZ headquarters in Sydney, Australia since 1997. Esker's solutions span the order-to-cash and purchase-to-pay cycles — allowing organisations to automate virtually any business process:

- Order Processing: automated entry and routing of incoming customer orders
- Accounts Receivable: automated sending and archiving of paper and e-invoices
- Collections Management: streamlined post-sale collection interactions
- Accounts Payable: automated entry and routing of incoming supplier invoices
- Purchasing: electronic processing and delivery of supply chain documents.

www.esker.com.au | info@esker.com.au | 02 8596 5100

UPFLOW

UpFlow is a channel-first provider of Document Capture, RPA, Document Management, Workflow, Electronic Forms and Integration software products and services. UpFlow distributes and resells products such as PSIcapture, Flow and FileBound. FileBound is a full functioned document and workflow management platform. It can be cloud or locally deployed. PSIcapture is an innovative document capture platform engineered to combine automation, efficiency, stability and Enterprise-class scalability. PSIcapture provides unmatched integration with just about any ECM or ERP platform [e.g. SharePoint, Xero, Trim, Objective etc.] and allows the utmost in flexibility for deployment in large or small organisations. UpFlow's mid-market Robotic Process Automation solution provides attended or unattended Bots for the automaton of enterprise work. Flow is a fully featured Integration Platform that can connect an exhaustive list line-of-business systems with each other.

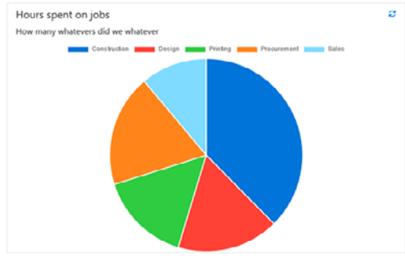
www.upflow.com.au | info@upflow.com.au | 1300 790 360

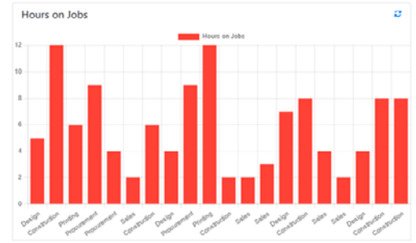
FileBound
Solutions

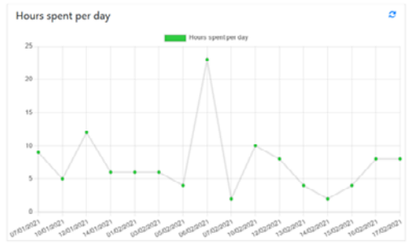
FileBound Solutions offers cloud-native, work automation and document management solutions that can be used to underpin any organisation's digital transformation program. These solutions are based around the FileBound software platform and are able to be deployed in organisations of all sizes. The solutions can include capture, document management, workflow, electronic forms, analytics, mobile access, advanced business system integration capabilities and much more. Solutions from FileBound Solutions deliver organisational efficiencies, drive out manual paper-based processes to decrease costs, increase productivity and support compliance with internal and external mandates. FileBound Solutions customers have the flexibility to create a variety of solutions from complex A/P automations to simple document archival and retrieval processes.

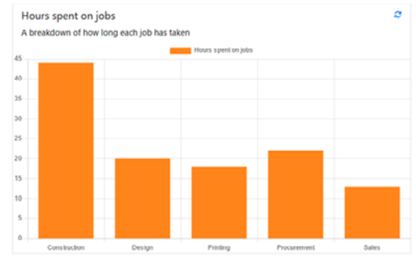
www.filebound.solutions | www.filebound.solutions/contact | 1300 375 565

EzeScan WebApps charts a new course









WebAps is EzeScan's web-based solution that can be accessed from anywhere, allowing users to capture and process documents with ease. EzeScan's Data Panel Dashboard (DPD) module provides users with a central area within EzeScan WebApps to have clear visibility of their organisation's data.

The Data Panel Dashboard has been made even more useful with the addition of charting capabilities. This allows users to easily create charts to help gain insights into document data and make informed decisions about processing or management.

Some examples of how customers are using charts:

- How many documents are being processed each day and by who?
- Which document type is being processed the most?
- How many hours are being spent on each task and how can we monitor improvements?

EzeScan is also able to collate from multiple integrated sources to provide further insight, including finance and ordering systems capturing data such as total number of orders, to outstanding invoices and chart them for visual reporting.

The system is designed to be user-friendly, easy to navigate and simple for any business to use. It allows users to quickly gain insight into their document data and make informed decisions about processing or management.

EzeScan has announced a range of new features and product enhancements for WebApps and EzeScan Desktop/SERVER.

WebApps updates include:

- added the ability to sync users Manager from authentication providers;
- added the ability to selectively sync groups from authentication providers;
- added ABN lookup external API field;
- added "time spent in queue" as metadata for indexing items;
- added more configuration options for date fields to allow users to offset the default date by an amount;
- added clean-up of old generated reports;
- added the ability for user info fields to display the manager of the users information; and
- added the ability to bulk export, enable, disable and delete selected app pages.

EzeScan Desktop/SERVER now features:

- improved error messaging for database lookup fields;
- improved error messaging for items that have failed processing;
- improved colour image compression for PDF output;
- added PDF 1.7 and PDF/A-2b file output support;
- added connection profile redirection for simplifying migration between DEV, TEST and PROD;
- EzeScan SERVER web page now reports number of documents pending in document queues;
- simplified Microsoft 365 Outlook import options;
- added various support options to help menu;
- numerous online document updates (view documentation here);
- layout and style improvements to the Authority Server web page;
- license files can now be downloaded via web page; and
- configuration Profiles can now be downloaded via web page.

For more information on recent product improvements contact support@ezescan.com.au

AvePoint assessed IRAP Protected

AvePoint Online Services (AOS) have been assessed to the security classification of PROTECTED, the highest level possible for an independent software vendor. AvePoint's platform and services including Cloud Backup, Cloud Governance, Policies & Insights and Cloud Records solutions were assessed against the Information Security Registered Assessors Program (IRAP) official controls.

Through the Australian Cyber Security Centre (ACSC), the Australian Signals Directorate (ASD) initiated the IRAP to ensure the highest standard of cybersecurity and information security assessments for ICT systems processing or storing government information.

In 2021, AvePoint partnered with The Australian Transport Safety Bureau (ATSB) to initiate its IRAP assessment process to help modernise and further automate the ATSB's record management. This year's assessment, conducted in partnership with Security Centric, further validates AvePoint's expertise in helping government organisations secure their digital collaboration data while adhering to the highest standards of security and data protection. More than 230 government entities in Australia use AvePoint to migrate, manage and enhance protection of their Microsoft 365 and SharePoint data.

As Australian government agencies continue to shift to and conduct business in cloud environments with modern approaches to digital collaboration, it is important to implement the right policies and backup plans to mitigate risks and meet records management compliance and security standards, while empowering employees to utilise the tools they need to do their jobs securely. AvePoint's data management solutions enable governance and compliance with the latest standards and regulations such as NAA, VERS and the Essential Eight Model.

Jared Seminoff, Senior Account Executive at AvePoint Australia said, "The Australian Government has demonstrated an ongoing commitment to transition its workforce operations to the cloud by leveraging cloud-based collaboration platforms such as Microsoft 365. As trusted partners of hundreds of public sector organisations in Australia, this latest assessment shows our expertise in safely and efficiently helping government agencies manage and protect their data in the evolving digital workplace."

Sash Vasilevski, Principal at Security Centric said, "AvePoint has demonstrated good levels of compliance with most of the fundamental controls in the Information Security Manual (ISM). They have a diligent security team and in general have good internal security policies and security fundamentals which have flowed into the AOS system. We were engaged to conduct their previous and latest IRAP assessments, and the results show AvePoint's ongoing commitment to helping government agencies protect their data at the highest standards."

For more information visit https://www.avepoint.com/au/solutions/au-public-sector.

Document Simulator to help train your AI

AYR, a company specializing in Intelligent Document Processing (IDP) and Intelligent Automation, has announced the launch of the 3.0 version of its patent-pending Intelligent Document Simulator (IDS). IDS is claimed to solve two of the most significant challenges in the industry: the scarcity of training data for customer use cases and the ever-evolving formats and layouts of business documents.

Businesses struggle to provide training data for intelligent automation due to the sensitive nature of their documents, containing confidential or personally identifiable information. Additionally, technology teams may have limited access to business documents, making it challenging to gather the necessary data to train Intelligent Document Processing systems.

IDS promises to overcome these challenges by generating synthetic data that mimics the appearance and content of real-world business documents. The first version of IDS, released in early 2022, enabled users to change the business fields of documents to a random selection from user-provided dictionaries, which could be automatically created or manually assembled. This allowed users to generate as many sample documents as needed to train their IDP models.

"While this proved helpful, the latest breakthroughs in IDS take this capability to new heights by enabling users to input a sample document and generate various layouts, such as swapping columns in a table containing line items or shuffling sections of the document horizontally or vertically and therefore creating new training documents," said Dr. Tianhao Wu, CTO and co-founder of AYR.

"This makes it possible to train AI and machine learning models to recognize and process a wide range of document layouts, which is crucial for handling the diverse and ever-changing documents that businesses deal with daily."

The AYR team's latest innovation goes further by allowing users to change all words to similar fields or values, making the synthetic data even closer to real-world documents.

Instead of using dictionaries like the first iteration, AYR supports two mechanisms to produce synthetic contents: AYR's own language model to produce similar phrases, words, or lines of text; or leveraging the widely-used GPT-3 engine to produce similar contents dynamically.

As with previous IDS versions, users are still able to further augment their data and document samples, including blurring, rotating, and making source documents more difficult to read, similar to the challenges companies face in the real world. The augmented data is used to push the boundaries of machine learning models and increase speed to market.

https://ayr.ai/

Automated Infosec Risk Assessment

Israeli developer Cognni has launched a new information risk-assessment product that uses proprietary AI to provide a comprehensive analysis of direct and indirect threats to critical business information, with a scan taking just minutes to complete.

Cognni claims its technology goes beyond the limits of many existing data discovery tools that only detect personal identifiers and can map an organisation's sensitive information without any training.

It uses a new generation of AI that uses prior knowledge to mimic the way humans understand and give meaning to information. This enables the technology to detect and classify critical financial, business, and legal information at a granular level, like a human would, rather than only extracting regulated personal identifiers.

Organizations can perform the security scan remotely via Cognni's online platform and will receive a detailed information risk assessment report within a couple of minutes of the completion of the scan.

While there are other such tools on the market, Cognni claims its platform is unique in its ability to detect information risks in an organization's sensitive information without the need to teach the AI and the speed at which it can complete this in just a few minutes.

"Our AI-powered Information Risk Assessment Tool is a game-changer when it comes to how companies can audit their data posture and detect information risks that they couldn't detect until today," said Guy Eisdorfer, Co-Founder and CEO of Cognni.

"Given the size and complexity of the data now stored by many organizations, the only scalable solution to managing the risks associated with this is to use advanced AI tools to achieve in minutes what a human would take months to do."

To receive a risk assessment, clients can register and connect to the Cognni Information Security Intelligence Platform. Following the scan, a full report is produced and delivered to the user. The report provides an in-depth assessment of key security findings in an easily-digestible format that includes an executive summary and a breakdown of data vulnerabilities.

Founded in 2019, Coggni is a member of the Microsoft Intelligent Security Association, and offers Information Intelligence for M365 on the Azure Marketplace.

https://cognni.ai/

Parashift banking industry AI

Parashift, a provider of advanced machine learning-based document classification and data extraction software, has announced a technology partnership with BSI, a leading CRM and CX software company.

BSI has a strong foothold in the banking sector. The integration of Parashift's AI technology with BSI's solutions enables companies in the banking sector that need to process hundreds of complex and unstructured documents every day in the shortest possible time and with great efficiency.

The company states that using its Document Swarm Learning technology, AI models are trained at the field level and across use cases, significantly reducing time-to-value.

"BSI has an amazing footprint in the banking and insurance sector. We're delighted to work with BSI in the future and improve efficiency through the combination of the two platforms" Alain Veuve, Founder & CEO of Parashift.

With hundreds of document types, the volume of information the banking sector has to process each year is immense. Especially in the case of mortgage files, there are many different document types with widely varying layouts.

In addition, the documents are in structured and semi-structured as well as completely unstructured form, which makes smooth processing difficult. For employees, it is a manual and tedious process, as the traditional data extraction solutions being used are too weak for the complexity of the document types.

BSI already uses Parashift successfully in collaboration with clients to automate the mortgage process. With this combination clients can automate any document-based process by separating, classifying and extracting all the data.

The benefits are significant. For example, there is a reduction in costs and processing times (a few hours instead of weeks). This frees up more time to process additional mortgage files and acquire new customers.

"Thanks to the technology partnership with Parashift, our customers can significantly optimize document processing and reduce process throughput times. Parashift combined with BSI is the perfect match for intelligent document processing in customer management." Kai Jesse, Community Manager Retail at BSI.

www.bsi-software.com, www.parashift.io

From Basic to Modern Authentication: Implications for security and migrations

By Stacey Farrar, BitTitan

The use of Basic Authentication over the internet is as old as the basic standard for the world wide web. Its use was outlined in May 1996 as part of the standard for version 1.0 of the Hypertext Transfer Protocol.

At the time, it was acknowledged as being inherently insecure because a username and password are sent in clear text, and the authors called out the need for additional security.

Over time, subsequent RFCs improved on the security of the standard - most notably by encrypting the credential exchange - but at its core, Basic Authentication can still be thought of as authentication using only a user name and password.

So... Basic Authentication has been around for more than 25 years. Given the current state of cybersecurity threats, its continued use is almost unconscionable.

Microsoft has recognised the high risk associated with this legacy authentication approach and has pushed for a shift to a more secure form of Modern Authentication.

There are only two exceptions. Basic Authentication will remain supported in Exchange Server on-premises products, and for SMTP-AUTH in Exchange Online. The latter is to support multi-function devices such as devices and scanners that cannot be updated to use Modern Authentication.

Still, Microsoft urges customers to move away from using Basic Authentication with SMTP-AUTH whenever possible. With those few exceptions, on December 31, 2022, Basic Authentication was disabled for good, which extends to migration projects. In our opinion, that's a good thing.

Modern Authentication as implemented by Microsoft is more secure and provides a better user experience given the distributed, federated nature of the modern web experience.

While it still requires usernames and passwords as a first line of establishing identity, Modern Authentication minimises the number of times those credentials are exchanged or stored on separate servers.

Replacing username and passwords with tokens -p packets of information that can be exchanged and validated by the parties to the transaction - is a far more secure way of confirming the identity of a user while verifying that they are authorised to access applications and resources.

Users get a single-sign on experience when they access multiple resources that are related - an experience that they naturally expect.

Modern Authentication supports additional, extended methods for confirming user identity, especially when accessing from locations or devices that are new for that user, making it a vital tool for defending against phishing attacks that can lead to account takeovers, business email compromise, and ransomware attacks.

Modern Authentication in Exchange Online, as implemented by Microsoft, is built on three main components: Active Directory Authentication Library (ADAL), OAuth 2.0, and ID Connect.

It leverages ADAL to enable applications to support a variety of sign-in capabilities including smart card+certificate-based authentication. Notably, it supports two-factor/multi-factor authentication (2FA/MFA), which allows additional authentication factors to further establish the user's identity.

Additional factors may include possession of a device such as a smart phone, or biometric factors such as a fingerprint or facial recognition. Once a user is authenticated, ADAL then obtains tokens for securing API calls on behalf of the user.

All Microsoft support and development for ADAL, including security fixes, will end in June 2023, in favour of an updated version now termed Microsoft Authentication Library (MSAL); ADAL on existing operating systems will continue to work although according to Microsoft, ADAL will become increasingly vulnerable to new patterns of attack.

OAuth 2.0 is the industry-standard protocol for authorisation; note that "Auth" stands for authorisation, not authentication. Its primary role is to authorise applications to share data with each other on behalf of the user, using token exchanges to avoid resending username/password credentials.

Access tokens are specific to the applications and resources for which they are issued and have a limited lifetime, which prevents their reuse.

From the user perspective, the use of access and refresh tokens under OAuth 2.0 reduces the number of times users are prompted to reauthenticate with their primary credentials and perform 2FA/MFA.

While ADAL focuses on authentication and OAuth 2.0 on authorisation, as applications continued to share more data and account information among them, the need for a standard framework for single sign-on became evident.

Open ID Connect is an authentication layer built on top of OAuth 2.0. It provides for issuance of an access token, along with an ID token for proving the user's identity. The ID token contains information about the authenticated user and is digitally signed by the identity provider.

The receiving application can then verify the ID token is valid by using the identity provider's public key to confirm that the identity information has not been tampered with.

Zero Trust

Modern Authentication is becoming a key element of Zero Trust security. Zero Trust is an approach that applies a set of security principles. The goal is to allow users to access only what they need, without compromising security while still making that access convenient for the user.

At the core of Zero Trust is 'never trust, always verify,' regardless of where the request originates or the resources it accesses. The federated model of Modern Authentication provides an ideal framework for implementing a Zero Trust security model.

We understand that other available migration tools have taken a go-slow approach to supporting Modern Authentication. With the temporary exception of Coexistence and Hybrid Exchange, my company's migration app now fully supports Modern Authentication in particular, on endpoints that are involved in mailbox migrations.

This makes organisations more secure, and their migrations secure, too.

Techs might have the following questions about setting up and using a quality migration app to migrate mailboxes, documents and workloads under the new requirements of Modern Authentication.

How do users enable Modern Authentication?

To summarise, register Exchange Web Services with a delegated application in the tenant, and then supply the Client Id and Tenant Id on registering the app to use when authenticating with the Exchange Online tenant.

While we understand that some other available migration tools have taken a go-slow approach to supporting Modern Authentication. With the temporary exception of Coexistence and Hybrid Exchange, our own migration app now fully supports Modern Auth in particular, on endpoints that are involved in mailbox migrations.

Modern Authentication makes organisations more secure - and their migrations more secure, too.

Stacey Farrar is Product Marketing Manager, BitTitan

ChatGPT to RPA integration

Compass UOL, a global company specialised in digital transformation, has developed a new solution that brings together the topic of the moment in the technology industry - ChatGPT – and the very well-known RPA (Robotic Process Automation) platforms.

Today, ChatGPT is considered the most robust Generative AI application in the global technology market because it is built on top of Open AI's GPT 3.5, which has more than 175 billion parameters, enabling several types of interactions, such as extracting information ready and summarised in a chat format, and producing texts of various types. All this in a faster and more precise way.

Compass UOL's new integrated offer unites two technologies - ChatGPT API and RPA - that complement each other and ensure the delivery of a differentiated service to customers.

While ChatGPT performs the ultra-fast collection of information through the use of artificial intelligence, RPA organises the data collected and performs the necessary tasks that, until then, were performed manually.

Due to the efficiency of the artificial intelligence used in ChatGPT, Compass UOL's information extraction and processing solution in conjunction with RPA technology becomes tangible to be offered to customers.

https://compass.uol/en/home/

Open source security alert system

Darktrace Newsroom is a new AI-driven system that continuously monitors open-source intelligence sources for new critical vulnerabilities and assesses each organisation's exposure through its in-depth knowledge of their unique external attack surface.

Darktrace's knowledge of "self" means it can quickly assess which assets are potentially affected by the emerging critical vulnerability and can provide mitigation advice specific to the organization so that it stays protected.

New critical vulnerabilities make news headlines regularly and the average time to exploitation has shrunk to just fifteen days. Cyber security teams need to be able to quickly answer the question, "Are we vulnerable? And where?".

Traditional vulnerability management programs are typically resource intensive, involving the constant monitoring of security news feeds and intelligence sources. Meanwhile, exposure tests from vulnerability scanners take time, leaving IT security teams exposed in the absence of a quick initial indicator of their unique exposure to the emerging threat.

Darktrace Newsroom uses AI to monitor threat feeds and OSINT sources for new critical vulnerabilities and publishes them on the Darktrace PREVENT dashboard as part of the Newsroom feed. Newsroom shows a summary of the vulnerability, the affected software, and reveals how many assets have been found to run this software within the organization.

This capability augments the human security team by quickly determining whether an organisation is affected by a new vulnerability, alleviating lengthy, labour-intensive manual processes. Traditionally, security teams had to take longer periods of time to work out whether they were affected when a vulnerability emerged, allowing a window for aggressive, fast-moving attackers to breach their organisations, often within hours.

Successful exploitation of vulnerabilities can lead to data breaches with accompanying large fines. The insights provided by Darktrace Newsroom allow security teams to understand, within an average of two and a half hours, if and where on their attack surface those vulnerabilities are likely to manifest. As a result, these organisations are able to carry out timely mitigation actions and prevent any exploits.

https://darktrace.com/

AI-Driven Unstructured Data Discovery

US firm DryvIQ has secured a patent for its artificial intelligence-driven (A.I.) data classification and protection technology.

"Businesses need confidence in the platforms they've entrusted to protect their sensitive information. With the cost of a data breach averaging nearly $US10 million in the U.S., organisations can't afford the risk of their data getting into the wrong hands – intentionally or unintentionally," said Steve Woodward, principal inventor and Chief Innovation Officer at DryvIQ.

"With DryvIQ's patented technology, we help organisations find and protect their sensitive information with accuracy and precision."

Seventy-eight percent of organisations lack confidence in their security posture despite increased cybersecurity investments, according to a 2021 survey conducted by IDG Research. These organizations are vulnerable to data security and compliance risks posed by legacy data storage and management architectures, which are limited in their ability to access multiple repositories and are prone to classification errors.

DryvIQ's A.I. and machine learning technologies covered in the patent lower these risks by automating the discovery, classification, and migration of unstructured data across major file storage repositories and business applications at over 100 terabytes per day, at petabyte scale, with proven and industry-leading accuracy rates of more than 92 percent.

https://dryviq.com/

Email Duplicate ID for easier eDiscovery

The Electronic Discovery Reference Model (EDRM), a global advisory body seeking to improve the practice and provision of data and legal discovery, has published the EDRM Cross Platform Email Duplicate Identification Specification.

This specification provides a framework for identifying duplicates across multiple email platforms, allowing organizations to identify duplicate emails efficiently and effectively in a defensible and cost-effective manner.

Currently no means of cross platform email duplicate identification exists, except to reprocess the data using a single vendor platform, often expending significant time and cost.

The solution is a simple, but effective approach which involves the use of the hash value of an email Message ID metadata field which is the EDRM Message Identification Hash ("MIH"). This new approach will not replace current email deduplication methods but will enable cross platform email duplicate identification.

"Our global, multidisciplinary EDRM Committee, comprising legal technologists, forensic professionals, product developers, consultants, c-suite business leaders, data scientists and lawyers, is really excited to bring this solution for email cross platform duplicate identification to the market. We believe it has numerous applications that will save significant time and cost," said Beth Patterson, director at ESPConnect and project trustee.

"We encourage product vendors to implement the generation of the MIH in their products and lawyers, eDiscovery & forensic professionals, service providers, regulators and courts to request the MIH in productions. Like any eDiscovery tool, expertise is required to determine how best to apply the MIH for a particular case."

The global EDRM Email Duplicate Identification Specification project team has developed the EDRM Email Duplicate Identification Toolkit as a resource to support the implementation of the EDRM MIH and use of it for cross platform email duplicate identification. The Toolkit outlines several considerations which should be taken into account when deciding how to utilize the MIH. Comments from the public are welcomed until March 15, 2023.

The project team anticipates that the use of EDRM MIH will lead to significant time and cost benefits. For example, during discovery, disclosure or an investigation, it is often useful to identify duplicate emails in data exchanged between parties. This can deliver many benefits, including the ability for legal teams to rapidly triage emails already reviewed that also reside in data received from others.

"Anyone who has been active in e-discovery for a while has almost certainly run into the situation where they want to de-duplicate data across platforms," said David Cohen, Chair of the EDRM Project Trustees and Practice Group Leader of Reed Smith's Records & E-Discovery Practice Group.

"For example, that occurs where clients or providers want or need to change processing and review platforms or wish to use multiple tools that have different duplication identification standards. Prior to development of the MIH hash, there was no economical way to deduplicate across platforms, so parties ended up having to pay for duplicative review and analysis of the same documents. Now, thanks to Beth Patterson and her dedicated team, there is a solution that can save parties significant time and money.

"The whole development team deserves credit, including the volunteers from companies that offer some of the leading platforms that can now implement the MIH hash, like Relativity, Reveal-Brainspace, EDT and Nuix."

"The strength of the EDRM MIH springs from its simplicity and economy," said Craig Ball, EDRM General Counsel, Special Master and Texas litigator. "Pairing decades-old technologies in an innovative way, the EDRM MIH enables cross-platform duplicate identification--an unprecedented, disruptive capability that seamlessly integrates with existing tools and workflows.

The EDRM MIH is more than simply a great idea that's been rigorously developed and tested; it's an open-source, collaborative effort of leading companies and technologists backed by the integrity and influence of the EDRM. I'm proud to be part of the EDRM MIH development team.

Esri Open Map Data

Esri has joined the Overture Maps Foundation, a collaboration founded by Amazon Web Services (AWS), Meta, Microsoft, and TomTom. Overture's mission is to create reliable, easy-to-use, and interoperable open map data.

Historically, using open map sources posed challenges for geospatial developers and professionals. These include collecting comprehensive data from disparate sources, curating data of variable quality and currency, combining datasets with different structures, testing data for errors and inconsistencies, and enabling integration with other map products.

These are challenges the Overture Maps Foundation seeks to overcome, building on the work of other open data projects such as OpenStreetMap.

"Ready access to geospatial information has fuelled the innovation of many technologies and products, benefitting organizations and communities around the world," said Deane Kensok, Esri ArcGIS Content CTO.

Members of Overture will provide data and technological contributions, combining their resources to create complete, accurate, and extensible real-world map data that is available under an open data license.

To learn more visit esri.com/arcgis-blog/products/arcgis-living-atlas/announcements/esri-joins-overture-maps-foundation/.

Next Gen Contract Processing AI

Evisort, a no-code contract intelligence platform for legal, procurement, IT and sales operations teams, has announced its next-generation AI contract processing with advanced OCR ingesting. Evisort's proprietary AI has made a massive leap in capacity - now ingesting and analysing up to 450,000 contracts per day.

Evisort's contract processing addresses challenges commonly faced by legacy OCR, including difficulties deciphering handwriting, blurry text, tables, headers, footers, and watermarks.

The platform now recognises multilingual handwriting and typed text, including non-Latin characters from Chinese, Japanese, Korean and other languages.

With these AI enhancements, Evisort's solution empowers enterprise customers to develop a more accurate lens into their worldwide operations, including regional offices, via connected contract data.

Evisort AI Labs has also trained generative AI capabilities that help users draft, redline and negotiate contracts based on existing AI contract data and large language models.

As organisations eliminate siloed contract data, business leaders can strengthen their expanding global ecosystem and educate stakeholders across the business on the importance of data to fuel frictionless global operations.

Allowing AI-powered contract data insights to flow to any employee within the organisation who can benefit from it is critical to accelerating the business impact that AI can facilitate.

Knowing what is in their agreements helps business teams adapt strategically to changes in regulatory landscapes, data privacy laws, macroeconomic conditions, geopolitical institutions, supply chain viability, sales obligations, corporate ownership and cross-departmental priorities.

www.evisort.com

Natural Language Processing Solution

Kensho Technologies, a company of S&P Global, has announced its newest Natural Language Processing (NLP) solution, Kensho Classify. Classify derives value from vast amounts of text and documents by making content more discoverable, enabling analysis of text, smart search, content recommendations, and streamlined research and analysis.

Historically, making sense of vast amounts of text and documents has been incredibly laborious, requiring huge amounts of labelled data and substantial Machine Learning (ML) expertise.

Additionally, existing tools don't allow for custom concepts or excerpt-level annotation.

Classify has been trained on millions of documents and is specifically tuned for complex business and finance use cases, allowing users to find concepts and topics within documents in a fast and efficient way, with no machine learning or technical skills required.

"Classify capabilities are unprecedented, only requiring 30 data points to learn a new concept with three minutes of training time," said Philip Taylor, Lead Product Manager at Kensho Technologies.

"Classify is more accurate, faster, can handle larger payloads, and is easier to use than any other product on the market today.

"We're particularly proud of Classify's ability to benefit business users rather than extremely technical data practitioners. Stay tuned for more updates in 2023 on the Classify roadmap, including an intuitive user interface to make it even easier to operate, and integration into the Capital IQ Pro platform."

This announcement follows the recent launch of the Named Entity Recognition and Disambiguation (NERD) UI, an NLP solution optimised to extract and understand all types of entities in text documents using a context-aware model.

The NERD UI allows users to gain insight into the who, what and where of any document, making research and analysis easy.

Classify stands as a sister offering to NERD. While NERD provides insight on concrete entities, Classify is the other side of the coin, providing insight on more abstract topics spanning sentences or paragraphs.

Together, NERD and Classify can give a complete picture of large amounts of text in a quick and efficient manner.

https://kensho.com./

Process Automation for KnowledgeLake

An update to the KnowledgeLake platform expands its ability to help organizations solve their most complex business process and workflow automation challenges. The update also elevates the customer experience by simplifying document and data collection and providing greater transparency into the status of applications, transactions and other processes.

KnowledgeLake's process automation engine now features an intuitive interface for citizen developers as well as automation and IT specialists.

The process automation engine has been expanded to include conditional routing, looping, error handling, granular permissions and other enhancements that enable basic and complex automations across different applications and systems.

"We've taken a major step forward in our process automation capabilities," said Ron Cameron, founder and CEO of KnowledgeLake.

"We know that not every workflow is the same, and business processes are often messy or non-linear. We've developed an even more powerful process automation engine to support all the various contingencies, conditions and applications modern business processes require.

"Organizations will be able to address their most complex workflows and automate them beautifully in one easy to use interface. At the same time, they can bring customers directly into those workflows."

The update introduces two new capabilities to the KnowledgeLake platform that enable better digital customer experiences:

Digital Experience Portal – An interactive gateway that loops customers and other external participants (such as contractors and third-party vendors) into workflows and provides realtime insight into the status of processes. The portal features an auto-generated task list builder and secure file sharing capabilities.

Secure Electronic Forms - A no-code, low-code, and pro-code tool that enables users to design and customize external-facing online forms that can be used to trigger workflows. The flexible white-label form builder includes embedded data validation and ReCaptcha authentication for security/compliance.

"Digital workflows and processes are getting more complex by the day and involve a growing number of stakeholders," said Jason Burian, VP of Product for KnowledgeLake.

"To succeed in this dynamic environment and satisfy customers, organizations require more technical agility, and that means better tools. The Ontario release loops customers right into workflows and lets IT professionals and citizen developers alike automate complex, end-to-end business processes and create streamlined digital experiences for customers."

www.knowledgelake.com/workflow-automation-software

iDox Document Management

IDox.ai, is an AI-powered document management platform designed to cut back on the hours employees spend on administrative tasks, such as looking for critical information within document review processes, The software can easily and accurately identify the type of document, extract relevant information, and classify it accordingly. It can also detect sensitive information, such as personal data or financial information, and flag it for further review. The company's stringent security protocols and commitment to ensuring the protection of sensitive information are attested to by its SOC 2 and ISO 27001 certifications.

A part of Foxit software, a global provider of PDF solutions, the company counts Google, Amazon, and NASDAQ among its clientele and hopes to expand its reach even further with this new program.

The AI-powered solutions support a wide range of industries, such as healthcare organisations, financial institutions, real estate agencies, law firms, government entities, and beyond – allowing professionals to focus on their core competencies.

iDox.ai is designed to integrate seamlessly with existing business systems and allows documents to be imported from everyday services such as Google Drive and Dropbox.

https://idox.ai/

Algolia adds hybrid search engine

Algolia, the developer of an API-First Search & Discovery Platform, has announced the acquisition of Search.io, whose flagship product is Neuralsearch – a vector search engine that uses hashing technology on top of vectors. Algolia will combine its keyword search and Search.io's Neuralsearch into a single API.

"Our mission, vision and purpose is powering discovery. We've done this to date largely with keyword search. With the addition of the vector search engine from Search.io, we're going to disrupt the search market significantly," said Bernadette Nixon, chief executive officer, Algolia.

"We'll be the only product on the market that combines keyword search with vector-based semantic and image search, along with vector-based recommendations. Vendor consolidation is back in vogue, and being able to get best in class capabilities from one provider is powerful in today's economic climate."

Algolia claims it will now more effectively surface the most accurate and relevant results for users, whether they use specific keywords or natural human expressions. It states any companies claim to offer some form of semantic search, however, these companies do not offer the capabilities of keyword search and vector-based semantic search in a single API cost-effectively, nor do they have the ability to scale. With Search.io, Algolia can empower business users with a better way to manage the automation of unique and engaging end user experiences.

"We are delighted to be joining a world-class leader in search and discovery," said Hamish Ogilvy, chief executive officer and co-founder, Search.io. "Delivering on the promise of AI search has traditionally required tremendous internal expertise and engineering resources to work effectively.

"Beyond delivering better search experiences, this must also be done reliably, fast and cost effectively. Algolia has led the world in delivering highly redundant, globally distributed instant search using more than 100 data centres worldwide. This global search distribution network combined with vector-based semantic search using extremely fast and efficient neural hash technology is an exciting and truly unique solution."

https://www.algolia.com/

Kognitos expands BPA Platform

Kognitos, a developer of Generative AI for Business Automation using Large Language Models (LLMs) such as GPT3 and ChatGPT, has closed a seed round of funding for $US6.75 million. The funds will be used for the expansion of Kognitos's cloud-based Koncierge platform. With the addition of this seed funding, Kognitos has received $US9.35 million venture capital to date.

The Koncierge platform provides an intuitive Generative AI interface similar to ChatGPT – focused on the large global market for business process automation.

The platform is powered by an AI Engine that can interpret the English language just like humans, enabling machines to fully understand a natural language. Combining business data, business logic and LLM technology, Koncierge is able to automate business processes at cloud scale with the safety and auditability of human review in English.

Kognitos claims to be the first company to enable Generative AI for automation in the enterprise, using English as the language of automation, audit and exception handling, enabling automation access to billions of business users worldwide.

Kognitos also integrates with other AI technologies including GPT3, OCR, NLP, common business applications, cloud services and custom on-prem applications.

Kognitos offers patented conversational exception handling, lowering the cost of maintenance and troubleshooting automations. Rather than crashing on exceptions like traditional automations in the hyperautomation space, Koncierge starts a conversation to suggest resolutions and learns new business rules in English.

https://www.kognitos.com/

Appian enhances Process Automation

Appian has announced the latest version of the Appian Platform for process automation. The new release features enhancements in total experience, data fabric, automation, and process mining, underpinned by Appian's low-code design.

The new release makes it easier than ever to build beautiful and intuitive web and mobile Portals that engage external users in a seamless total experience with internal employees.

New features include:

Start Process from Portals: Start any process automation directly from a Portals interface. Appian users can initiate end-to-end process automations directly in a Portal enabling orchestration of AI services, assigning human tasks or executing robotic process automations.

Query Appian's data fabric from Portals: Streamlined ability to query and display record data from Appian's data fabric in Portals, without the need for complex integration calls.

Portals Header Bar and Pages: Engage Portals users with great experiences. Add a header bar for multi-page navigation to connect with your users in more ways, all with no code.

Portals Change Management: Changing and iterating Portals is even easier. With the addition of new proactive actions and recommendations, Appian proactively updates portals and notifies developers when objects change.

The latest Appian release includes enhancements that make working with the Appian data fabric easier, including:

Centralised Record Security: Secure all aspects of your records in one place. Quickly specify who can see which records and record views and what actions they can take.

No-Code Security Rules: Specify security rules for Record Views by answering two simple questions: Who can see the data, and when can they see it?

Simplification: Appian's data fabric features drag-and-drop record type configurations, auto-generation of user record type relationships, database updates with codeless data modelling, the ability to combine data across record types, and more.

https://appian.com/

OpenText launches Cloud Editions 23.1

OpenText has announced Cloud Editions 23.1 (CE 23.1), which simplifies administration of the cloud information management platform. In reference to integrating Micro Focus products and solutions within the OpenText suite, EVP and Chief Product Officer, Muhi Majzoub said, "With our combined organisation we will accelerate innovation to capture the growth in private and public cloud.

"The integration of Micro Focus capabilities will become part of our Project Titanium journey going forward."

Project Titanium is described as "the advancement of our OpenText Cloud Data Platform to create a common platform for our software and services. "

Cloud Editions 23.1 offers greater and visibility across attack surfaces with the introduction of OpenText Webroot Standalone DNS Protection and the availability of the OpenText Webroot portfolio through the Secure Cloud platform.

OpenText Webroot Standalone DNS Protection helps users extend strong network protection by integrating with their existing endpoint protection platform investments.

Network and roaming users are protected from malware download and other DNS based attacks, while maintaining privacy and visibility into internet usage without compromising security or experience.

By integrating the OpenText Webroot portfolio within the Secure Cloud suite of solutions, managed service providers (MSPs) are able to extend protection across attack surfaces via a single interface. MSPs are now able to deliver a full suite of security, compliance, and productivity solutions to scale to their customers.

OpenText has also expanded its forensic offerings with OpenText Tableau Forensic TD4 Duplicator. This stand-alone forensic imaging solution accelerates the pace of forensic investigation with a new compact form factor and an intuitive graphical user interface, so investigators can easily and cost-effectively conduct forensic acquisitions on-scene and find data wherever it is hiding.

With CE 23.1, OpenText customers can speed transformation with integrated applications. New integrated solutions for Salesforce, SAP, and Microsoft are now available through marketplaces and cloud resellers: Salesforce AppExchange, SAP Store, and the Microsoft AppSource:

- Transform Salesforce processes with integrated customer data capture and improve productivity of Sales and Service teams with OpenText Core Capture for Salesforce.
- Simplify and modernise financial workflows with a 360-degree view of everything necessary to complete cross-functional financial tasks with OpenText Extended ECM for Microsoft Dynamics 365 Finance.
- Retire legacy systems and get on the fast-track to SAP s/4HANA Cloud with OpenText InfoArchive Cloud Edition.

For more on all the Cloud Editions 23.1 visit these OpenText blogs.

US patent for document recognition

Scientists of AI-company Smart Engines have patented a system of efficient localization and identification of documents in images in the U.S. on February 7, 2023.

The authors of the invention are Smart Engines computer vision scientist Natalya Skoryukina, Smart Engines CEO PhD in Computer Science Vladimir Arlazarov and Smart Engines CTO PhD in Physics and Mathematics Dmitry Nikolaev, and the fourth inventor is Igor Faradjev, PhD in Physics and Mathematics, who passed away in 2020, and who was also one of the developers of the chess program Kaissa, winner of the first World Computer Championship.

As the authors explain, the essence of the invention lies in the use of features of different nature to efficiently localise and identify documents in images.

"This makes it possible to determine the type of document and eliminate distortions if necessary, i.e. to restore the original coordinate system.

"The invention differs from other works in that we analyse both local and global features on the image (from individual characters to the borders of the document, its colour, brightness, etc.), said Natalya Skoryukina.

"The system is arranged in such a way that it is easy to add new types of documents and remove those that are no longer supported. It does not require retraining and a single prototype image is enough, where you don't even need to see the parts with personal data – you can just 'blur' them."

The patented system can run and works quickly on all possible types of devices, both server and smartphone. In addition, depending on the device, a document feature detection algorithm is chosen. The algorithms used on mobile devices take into account that the document is in the hands of a person and adjusts to their actions.

https://smartengines.com/

SOTI Snap for Optimal Workflows

SOTI Snap – a cross-platform solution enabling organisations to rapidly build in-house apps – has enhanced its workflow optimisation capabilities to facilitate the rapid digitisation of manual processes and streamline businesses workflows.

The new SOTI Snap update includes a drag-and-drop workflow process builder that easily automates and tracks approval-based business processes across multiple departments.

With this feature, workflow apps designed in the SOTI Snap platform are now equipped with complete audit trails to help any organisation streamline approval processes and transparent business procedures, while allowing inefficiencies to be identified and solved.

The SOTI Snap update includes the following features:

Scheduled Reports - SOTI Snap now brings an efficient way to track reports on a periodic basis. App developers can schedule a report for specific console users at the desired frequency, such as daily, weekly or monthly. Developers can customise the report email template with their own wording and appearance.

Granular App Permissions - SOTI Snap opens newer possibilities for building video-related apps such as training apps or lightweight digital signage. With a new video player widget, developers can build a playlist of multiple videos which can be streamed online or offline in the SOTI Snap app.

Enhanced Table Widget - Developers can quickly create a front-end application to view and manipulate records in a private data repository. The table widget allows app developers to create SOTI Snap apps that can determine which end users can create, update or delete a record and access specific database.

https://www.soti.net/

Venmonitor tracks vendor/supplier risk

A new software tool launched by Venminder promises to provide the ability to easily screen vendor or supplier performance across multiple risk domains. Venmonitor provides comprehensive coverage into cybersecurity risk, ESG risk, privacy risk, Know Your Vendor risk, business health and credit risk, and negative news and adverse media.

As outsourcing has become a necessity for almost all organizations, so has the need to implement a strong third-party risk management and monitoring program. Venmonitor can help the many organizations that have struggled to keep up with the evolving risks posed by third parties by providing access to essential data that can be used to highlight initial risks pre-contract and flag potential risks during the ongoing monitoring of existing, contracted vendors.

Venmonitor helps solve these pain points with its two primary frequencies, a point-in-time for on-demand screening and a continuous monitoring solution where data on loaded vendors is refreshed automatically. With Venmonitor, organizations can enhance the efficiency of their third-party vetting, screening, and monitoring workflows, particularly in the following areas:

Screen for Key Risks on Vendors, Third Parties, or Suppliers During Vetting and Onboarding: Venmonitor provides a high-level view into the risk profile of a vendor, third party, or supplier before contracting and during onboarding. This can serve as an introduction to the additional due diligence that teams can use to prioritize and execute on, ultimately creating efficiencies and driving effectiveness in those follow up steps within a risk management program and processes. Venmonitor is particularly useful when organizations run into roadblocks of collecting artifacts, documents, information, or responses from vendors, third parties or suppliers, as it can provide an â€œoutside inâ€ view of a risk profile on these entities for an organization.

Aggregate Risk Profile Across Key Risk Domains: Venmonitor provides a holistic, comprehensive view across key risk domains, including privacy, cybersecurity, ESG, business health / credit risk, Know Your Vendor, and negative news and adverse media. Organizations can use Venmonitor as the centralized, single source of truth for high-level risk profiles on third parties.

Prioritization of Risk Domains to Perform Additional Due Diligence or Ongoing Monitoring: Venmonitor enables teams to quickly identify which risk domains are most critical or may require additional due diligence and ongoing monitoring through signals from the risk ratings and data collected, as well as normalized ratings from the risk intelligence providers. With the limited capacity and bandwidth organizations may have, Venmonitor provides valuable assistance in showing key recurring themes in certain risk domains and allowing organizations to ‘double-click’ on any area that may require more insight, documentation, and diligence.

Venmonitor was built inside Venminder’s third-party risk software platform, enabling its 1,200+ customers to immediately begin implementing the risk profile screening of third parties, however, Venmonitor is also available for purchase as a standalone software tool. Venmonitor compiles risk data from many of the industry’s leading risk intelligence providers. Given each data provider has different datapoints and individual risk scoring or rating methodologies, Venminder has crafted its own proprietary, normalized risk rating on each data provider that rolls up to provide an overall proprietary Venmonitor risk rating.

Within Venmonitor, the key risk domain areas include:

- Cybersecurity: Third-party vendors can be an organization’s weakest link and leave them vulnerable to data breaches, compromising customer data. Venmonitor provides access to cybersecurity data and scores received from multiple leading cybersecurity monitoring partners.
- Business Health and Credit Risk: A third party with poor ï¬ nancial health or credit runs the risk of going out of business before the contract term is up. Venmonitor gives access to key intelligence data that can help an organization determine the risk level of doing business with that third party.
- Privacy: Low privacy scores can be an indicator of inadequate or non-existent policies, no employee training, inadequate data governance, or improper data use. Venmonitor gives access to see an overall score that ranks the third party’s privacy practices as well as the top negative contributing factors to its privacy risk profile.
- ESG (Environmental, Social, and Governance): ESG refers to the specific metrics used to measure and report an organization’s progress against its ethical goals. Venmonitor gives access to view third party’s ESG scores that can help organizations determine if the third party has implemented sustainable business practices and align to an organizationâ€™s ESG goals.
- Negative News: In a world where millions of pieces of information are published daily in official and unoffcial news sources, it can take just one to cause financial or reputational damage. Venmonitor gives access to a wide range of AI-powered predictive analytics that classify, rank, score, and extract meaningful insights from unstructured data sources.
- Know Your Vendor: It is important to establish the identity and legal status of third parties. Sanctioned organizations and individuals, shell companies, obscured legal entities, beneficial owners, politically exposed persons, regulatory enforcement, and legal proceedings are not always discovered during due diligence. Venmonitor will give insight into if the third party has any criminal or regulatory enforcement action against them.

http://www.venminder.com/products/venmonitor/overview

Pay-As-You-Go for Microsoft AI

Microsoft has launched a new pay-as-you-go service for its Syntex platform, which is designed to make it easier to access and utilise the powerful artificial intelligence (AI) and machine learning (ML) capabilities of the platform.

The new pay-as-you-go option allows organisations to only pay for the Syntex services they use, instead of committing to a monthly or yearly subscription. This allows organisations to scale their usage up or down depending on their needs, and to only pay for what they use.

It will be generally available to all Microsoft 365 Commercial Cloud users. The company plans to make it available to government customers in the future.

Syntex usage will be billed to your Azure subscription, specifically charging for the total number of pages processed. Pricing details are available on this blog post. Hybrid environments, with some users on a per-user license and the remainder under pay-as-you-go, are not possible at present although may be in the future.

Microsoft Syntex is a content understanding service that uses AI and ML to analyse and understand unstructured data such as documents, emails, and images. This enables businesses to extract insights and value from their data, and to automate workflows and processes.

With the new pay-as-you-go option, businesses can start using Syntex immediately and only pay for the services they use, without any upfront costs or long-term commitments.

This makes it easier for businesses of all sizes to access the benefits of AI and ML, without having to invest heavily in infrastructure and expertise.

The pay-as-you-go option is available through the Microsoft Azure Marketplace, and businesses can choose from a range of different pricing tiers based on their usage needs. This allows businesses to easily calculate the cost of using Syntex, and to only pay for the services they use.

Microsoft Syntex is already being used by organisations around the world to automate tasks, extract insights from unstructured data, and to improve their operations.

Syntex’s document processing can replace time-consuming and error-prone manual extraction/keying/indexing and also consistently apply retention and sensitivity labels to save time and ensure compliance.

Security Copilot for AI Cyberdefence

Security Copilot is a new tool from Microsoft designed to quickly detect and respond to threats and better understand the threat landscape overall. Security Copilot will combine Microsoft’s threat intelligence footprint with an easy-to-use AI assistant.

Security Copilot is designed to work seamlessly with security teams, empowering defenders to see what is happening in their environment, learn from existing intelligence, correlate threat activity, and make more informed, efficient decisions at machine speed.

In a world where there are 1,287 password attacks per second, fragmented tools and infrastructure have not been enough to stop attackers. While attacks have increased 67% over the past five years, the security industry has not been able to hire enough cyber risk professionals to keep pace.

This has led to defenders who are overwhelmed searching for well-disguised attacks within an impossibly large volume of expanding network traffic and other signals.

Security Copilot will simplify complexity and amplify the capabilities of security teams by summarising and making sense of threat intelligence, helping defenders see through the noise of web traffic and identify malicious activity.

It will also help security teams catch what others miss by correlating and summarising data on attacks, prioritising incidents and recommending the best course of action to swiftly remediate diverse threats, in time.

Security Copilot will also continually learn and improve to help ensure that security teams are operating with the latest knowledge of attackers, their tactics, techniques and procedures. The product will provide ongoing access to the most advanced OpenAI models to support demanding security tasks and applications.

Its visibility into threats is powered by both the customer organisation’s security data and Microsoft’s threat analysis footprint.

Security Copilot helps address skills shortages in cybersecurity by bridging knowledge gaps and enhancing workflows, threat actor profiles and incident reporting across teams.

“Advancing the state of security requires both people and technology — human ingenuity paired with the most advanced tools that help apply human expertise at speed and scale,” said Charlie Bell, executive vice president, Microsoft Security.

“With Security Copilot we are building a future where every defender is empowered with the tools and technologies necessary to make the world a safer place.”

Security Copilot also integrates natively with a growing list of Microsoft Security products, such as Microsoft Sentinel and Microsoft Defender, to help customers create an end-to-end experience across their entire security program.

Microsoft Security Copilot is currently available through private preview. More information can be found at https://news.microsoft.com/AI-Security-2023.