

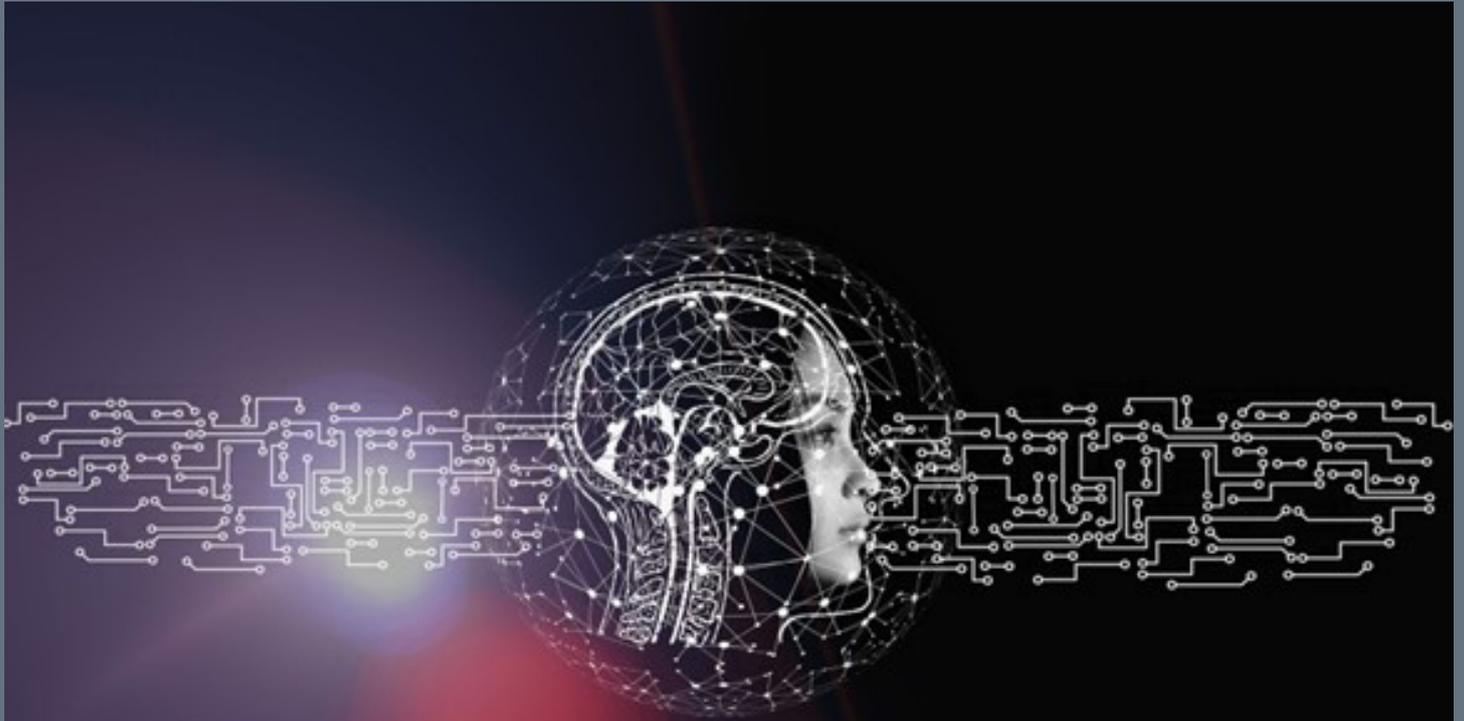
idm.

information & data manager

JUNE-JULY 2023



Why companies shy away from automation



AI's Potential Impact on IDP

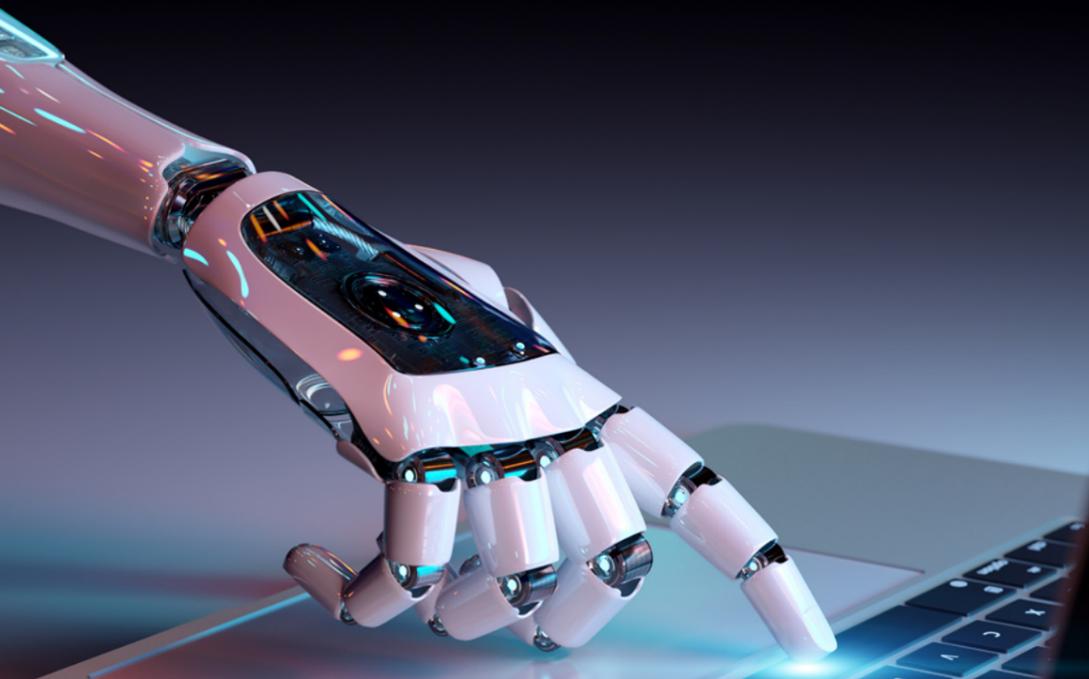
The Top 5 Cloud Security Risks of 2023 (so far)

The Importance of Capture in Document-Based Process Automation

What is enterprise application integration?

Can ChatGPT and large language models streamline records management?

GONE DIGITAL but still doing manual data entry?



ezescan. 

Automated Intelligence

- Process Automation
- Corporate Email Capture
- eForms Capture
- Digital Mailroom
- Backscanning Projects

Call: 1300 EZESCAN (1300 393 722)

www.ezescan.com.au

Nuix Acquires Rampiva

Nuix has entered into an agreement to acquire US form Rampiva, a workflow automation and job scheduling software provider.

Rampiva is a long-term technology partner of Nuix, founded in 2016 to meet the needs of Nuix customers who wanted to achieve greater productivity by automating their data processing tasks.

The Rampiva team collaborated with Nuix customers to build a specialized subscription revenue business from the efficiencies that customers gained from automating the Nuix Engine and exporting data into their wider legal technology stack, including Nuix Discover.

"Joining Nuix is an exciting opportunity to align our efforts to be a Force for Good and ensure Nuix customers can use their data analysis expertise as productively and efficiently as possible" said Daniel Boteanu, Rampiva Founder and CEO.

Nuix Group Chief Executive Officer, Jonathan Rubinsztein, said: "Rampiva is a complementary technology to the Nuix Engine and is used by our customers where the cost, ease, and administration of hype-scale data processing is not sustainable manually.

OnePlace UK buyout

UK multinational Ideagen has acquired Australia's OnePlace Solutions, a developer of solutions to simplify document and records management in Microsoft 365.

James Fox, founder of OnePlace Solutions, headquartered in Sydney, said: "When we looked at our ambitions for the company - to execute on our product roadmap and continue to lead the market with innovative solutions to help our customers - then this alignment with Ideagen made complete sense.

"We like that Ideagen's values mirror our own, it feels like a good fit, and it already has a footprint in the sectors and countries we operate in, so understand what we are trying to achieve.

"The opportunity this presents is exciting and I'm looking forward to the journey ahead of us."

James will remain with Ideagen as Head of Ideagen OnePlace Solutions.

The acquisition, Ideagen's second of 2023 following food safety software Ideagen Qadex in January, builds on Ideagen's presence in Australia which already includes Ideagen CompliSpace, providing governance, risk and compliance support for sectors such as education and aged care.

It also adds to Ideagen's collaboration portfolio: Ideagen Huddle, its customisable secure client portfolio, Ideagen PleaseReview, a document review, co-authoring and redaction software application and Ideagen Mail Manager, which solves the problem of storing and sharing important information contained within emails.

Paymerang acquires KwikTag and Syph

US accounts payable automation specialist Paymerang, LLC, has announced the asset acquisition of KwikTag, an invoice automation provider for Microsoft Dynamics ERP systems, and the share acquisition of Syph, the Australia-based AI data platform.

KwikTag offers a cloud-based AP automation solution to clients across multiple industries and was the first to create a fully integrated Microsoft Dynamics document management and workflow platform designed for accounting teams. Syph is an innovator in AI-powered data extraction and analytics.

This acquisition fits squarely within Paymerang's strategic roadmap:

- It adds products with deep domain expertise and native integrations in the Microsoft ERP ecosystem, with a valuable community of channel partners.
- It adds a proprietary AI platform, with modern APIs and multi-document capability, that will help Paymerang expand its solutions for the office of the CFO.
- It adds an international presence with users in over twenty-five countries.

Both companies are SaaS-based, which will advance their integration into Paymerang. KwikTag customers will immediately get access to Paymerang's payment automation solution. Founded in 2010, Paymerang provides a streamlined invoice and payment automation platform.

www.paymerang.com

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

All material in Information & Data Manager is protected under the Commonwealth Copyright Act 1968. No material may be reproduced in part or whole in any manner whatsoever without the prior written consent of the Publisher and/or copyright holder. All reasonable efforts have been made to trace copyright holders. The Publisher/Editor bears no responsibility for lost or damaged material. The views expressed in Information & Data Manager are not those of the Editor. While every care has been taken in the compilation of editorial, no responsibility will be accepted by the Editor for omissions or mistakes within. The Publisher bears no responsibility for claims made, or for information provided by the advertiser.

BOM Launches into the CM Cloud

It may have difficulty predicting their arrival at times, but Australia's Bureau of Meteorology (BOM) has determined that cloud is the future of Enterprise Document and Records Management, taking up a half-million dollar hosting deal with Micro Focus Australia.

The one-year deal from May 2023 will see the BOM move from its on-premise deployment of Content Manager to a licensing and hosting arrangement with Micro Focus, now a part of OpenText.

The agency had originally advertised for a simple CM version upgrade in March 2023, but has obviously been won over by the promise of a hands-off externally managed cloud EDRMS.

The BOM is Australia's national weather, climate and water agency. Bureau staff are located across Australia, on remote islands and in Antarctica. The Bureau's Victorian Office in Docklands, Melbourne, is a centre for administrative and operational activity, and provides overall national strategic planning, management and coordination of the Bureau's services.

As at 30 June 2022, the Bureau had 2161 total staff, including 1456 ongoing staff, 235 non-ongoing staff and 470 contractors. Content Manager Cloud is a fully managed, cloud-based, ISO27001-certified platform provided in a SaaS model.

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

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.

iCognition launches new Content Platform

iCognition has announced the launch of Ingress, its next-generation Content Services Platform designed to transform the way organisations manage and secure content, records and other information. Ingress integrates search, records and information management, security and compliance across multiple repositories including Teams, SharePoint, Exchange, OneDrive and OpenText.

Offering to change the way large-scale organisations manage information and developed on the back of iCognition's expertise and success in delivering cloud-based solutions, Ingress provides a single framework for compliance and records management purposes.

In a time where organisations are seeing more breaches of sensitive data, safeguarding information, and having a strong information governance process that is efficient, adaptable, and easy without disrupting the user will be a game-changer for large and complex organisations.

"Ingress turns the information management problem on its head," said Nigel Carruthers-Taylor, iCognition Executive Director.

"No longer will users need to navigate to separate

information management interfaces. We provide information management functionality directly within your corporate applications – enterprise search, automated or deliberate records management, information sharing and use, and automated business processes, all accessed from within Microsoft 365 Teams, SharePoint, OneDrive and Outlook. Later versions will expand to other common corporate applications."

With the ability to fast track your information processes securely, Ingress provides many benefits from keeping the team productive. It will provide them with the right information at the right time, regardless of which repository it lives in, while ensuring your vital corporate information is protected and secure from both external parties and internal agents.

A trusted key partner for large Government departments, Councils, Universities, and Not-for-Profit organisations, iCognition's expertise spans over 20 years in the Information Management and Governance space.

"Ingress will help clients manage their information sprawl – particularly the mess that has been created by the sudden adoption of Teams and SharePoint during COVID," said Joe Mammoliti, iCognition CEO.

"What we are releasing today is our first step toward a comprehensive content services platform that clients can build their digital transformations upon."

The next-generation Ingress platform expands on iCognition's current offering with IRAP and ISO27001 security credentials.

Learn more at <https://icognition.com.au/ingress/>

Ricoh Australia takes on Powell Software

Ricoh will bring a SaaS solution for Microsoft 365 to the Australian market following an agreement with Powell Software. Powell Software's digital workplace solutions empower more than 400 companies and over 1.5 million users worldwide, enabling hybrid workforces to be more productive and engaging from anywhere through desktop, mobile, or Teams.

Powell Software helps companies using Microsoft 365 in two ways: through Powell Intranet, which enhances corporate culture by keeping employees engaged, informed, and connected with a superior user experience through a customised SharePoint-supported intranet, and through Powell Teams, a governance and security tool for Microsoft Teams that addresses the need for governance in response to the surge in Teams usage and the desire to centralise Microsoft 365 applications for streamlined business processes.

Pierre Delage, Australia Country Manager at Powell Software, said "By combining our cutting-edge digital workplace solutions with Ricoh's expertise in designing and supporting enhanced employee experiences, we are committed to delivering a seamless digital transformation journey for businesses across Australia."

Powell Software partners guide customers through their digital transformation journey, supporting end-user organisations with consultation and design, project implementation, change management, and configuration.

<https://powell-software.com>

There must be a better way?



Scanner Rentals POWERED BY ezescan.

- ✓ The Right Scanner
- ✓ Expert Advice
- ✓ Quick Deployment
- ✓ EzeScan Software
- ✓ Pay As You Go
- ✓ No Warranty Hassles

Call: 1300 EZESCAN (1300 393 722)

www.ezescan.com.au

Transforming Records Management

Making You Digital-ready
for Today and Tomorrow!

Top 8 Considerations for Modern Records Management Solution

1. Secure indexing and archival
2. In-place records management
3. Taxonomy and metadata management
4. Security and confidentiality
5. Well-defined retention and disposition policies
6. Comprehensive ready-to-use adaptors
7. Compliant with DoD 5015.02, ISO 15489, ISO 16175, VERS
8. Cloud-native and support for large files

[Request a Demo](#) ▶ ▶

Newgen Software a “Leader” in The Forrester Wave™: Content Platforms, Q1 2023

About Newgen

Newgen is the leading provider of a unified digital transformation platform with native process automation, content services, communication management, and AI/ML capabilities. Globally, successful enterprises rely on Newgen's industry-recognized low code application platform to develop and deploy complex, content-driven, and customer-engaging business applications on the cloud. From onboarding to service requests, lending to underwriting, and for many more use cases across industries, Newgen unlocks simple with speed and agility.

For SALES Query

AUSTRALIA: +61 290 537174
AMERICAS: +1 (202) 800 77 83
CANADA: +1 (202) 800 77 83
INDIA: +91 11 407 73769
APAC: +65 3157 6189
MEA: +973 1 619 8002, +971 445 41365
EUROPE: +44 (0) 2036 514805

info@newgensoft.com
www.newgensoft.com



Only 16% Recovered All Data After Paying Ransomware: Survey

Almost all IT and security leaders (96%) globally are concerned their organisation will be unable to maintain business continuity following a cyberattack, according to a new study released by Rubrik.

Rubrik Zero Labs commissioned its second global study with Wakefield Research to gather insights from more than 1,600 IT and security leaders- half of which were CIOs and CISOs- across 10 countries.

Supplemented by Rubrik telemetry, key findings of the report include:

Everyone is “Doing” Data Security, But Reality & Results Vary:

■ Data security is becoming increasingly complex and the datasets that require securing are growing rapidly. Rubrik internal data revealed that on average, the growth of data secured in 2022 was 25% (on premises grew 19%, cloud grew 61%, and SaaS data secured grew 236% last year).

■ More than half (56%) of organisations currently employ at least one zero trust initiative.

■ However, only 56% of IT and security leaders developed or reviewed an incident response plan in 2022, and 54% tested backup and recovery options.

Legacy Data Backups, the Last Line of Defence for Many, are Falling Short:

■ 99% of external organisations reported having backup and recovery technology, with 93% encountering significant issues with their solution.

■ Nine out of ten external organisations reported malicious actors attempted to impact data backups during a cyberattack, and 73% were at least partially successful in these attempts.

■ Nearly three quarters (72%) of organisations reported

paying a ransomware demand.

■ Only 16% of all global organizations recovered all of their data via attacker decryption tools.

New and Constantly Evolving Problems Are Met with the Existing Challenges Pre-dating an Intrusion:

■ Almost half (47%) of IT and security leaders believe their 2023 cybersecurity budget is not enough of an investment.

■ 27% expect their IT and cybersecurity budgets to decrease in 2023.

IT and security leaders will need to work at bringing their teams together with only 4% stating there are no factors limiting the IT and security alignment requiring their attention this year.

“It’s clear organisations understand the gravity and impact of cyber incidents, but we also see a range of roadblocks from a lack of preparation, misalignment between IT and security teams, and over-reliance on insufficient backup and recovery solutions,” said Steven Stone, Head of Rubrik Zero Labs.

“In the current era of cybersecurity, the best outcome is ensuring cyber resilience. Incidents are inevitable, so it’s critical to reduce the risk before a response is needed, and - at all costs - protect the crown jewel: the data.”

Download the full report [HERE](#)

Methodology: The research was conducted among 1,625 IT and Security decision makers at companies of 500 or more employees by Wakefield Research in the US, UK, France, Germany, Italy, Netherlands, Japan, Australia, Singapore, and India between February 10th and February 21st, 2023. Respondents were made up of approximately half CIOs and CISOs and half VPs and Directors of IT and Security.

Despite Widespread Data Breaches, Cyber Risk still not prioritised

In 2023, MinterEllison conducted its eighth annual survey to assess contemporary perspectives on cyber risk. In both 2022 and 2023, only around half of survey respondents ranked cyber risk as a 'top 5' priority.

"Despite the current landscape, our findings reveal no apparent shift in the importance that organisations attribute to cyber security.

"However, as organisations face increasing exposure and risk as technology evolves, community expectations around data management grow, and regulators increase their scrutiny, organisations that regard cyber risk as a low or medium priority are vulnerable," the law firm found.

Some of the survey results include:

■ 78% of respondents told us that they have a cyber security incident response plan in place.

■ However, only 53% had assessed their cyber security arrangements against an established framework (such as the NIST Cybersecurity Framework or the ASD Essential Eight).

■ Only 52% told us that test or rehearse this plan regularly (at least annually)

"The threat of a cyber incident can no longer be classified as remote or novel. Cyber security and privacy by design must be embedded within the culture and planning of every organisation. Proactive and agile management and response to cyber risk are the new

normal," said Shannon Sedgwick, MinterEllison Partner.

■ 62% of respondents said that they were not confident, or only somewhat confident, that their organisation understood what data it stores, where it is stored, and who has access to it.

■ 52% of respondents said they were not confident, or only somewhat confident, about their organisation's understanding of its contractual and regulatory obligations in the event of a data breach

■ 51% of respondents considered that their organisation had sufficient resources to monitor and respond to its cyber security needs.

"In the last 12 months, data breaches increased in frequency and scale, driven predominantly by malicious or criminal activity. Between July and December 2022, malicious or criminal attacks comprised 70% of all notifications to the Office of the Australian Information Commissioner (OAIC).

Australian organisations across every sector have grappled with the repercussions of compromised sensitive information, disrupted operations and reputational damage, with the health and financial services sectors particularly affected."

The online survey was conducted between February and April 2023. Approximately 50% of respondents were legal counsel, and 20% were C-suite executives. Other respondents included IT, risk and security specialists and Board members.

Click [here](#) to view the report

Voltage Data Security Platform Analyst Tick

OpenText's Voltage Data Security Platform, formerly a Micro Focus line of business known as CyberRes, has been named a Leader in The Forrester Wave: Data Security Platforms, Q1 2023 report.

Voltage received the highest score possible in 15 criteria including data discovery, classification, tokenization, encryption, data masking, data access controls, privacy use cases, data and information governance use cases, among others.

Under the Strategy category, the Voltage platform received the highest scores possible, defined as superior to others in the evaluation, in the product vision and execution roadmap criteria.

As noted in the Forrester report, the Voltage Data Security Platform was praised by customers for its stability, scalability and performance.

Customers spoke highly of product managers and support and called out the support staff for its depth of knowledge of the product itself and real-world customer and industry-specific requirements.

"Threat actors are relentless which means businesses must take better precautionary methods to protect data and create cyber

resiliency. One of the best ways to protect high value sensitive data is through a truly integrated data security platform like Voltage," said Muhi Majzoub, Executive Vice President, Chief Product Officer, Development at OpenText.

"We provide businesses with a powerful solution that delivers data security, privacy and governance in a single integrated platform. We are honoured that the Voltage Data Security Platform has been recognized in the Forrester Wave as a leader."

The OpenText Voltage Data Security Platform helps secure organizations with continuous data discovery, insight, and protection to reduce risk and enable privacy by design.

Voltage's leading format-preserving enterprise data protection techniques, such as tokenization, encryption, and hashing, address privacy compliance, payments standards and regulations, and data security, while also helping organizations achieve their financial and sustainability goals by solving IT issues such as legacy data clean-up, data preservation, application retirement, test data management, and secure cloud analytics.

For more information, view the report: [The Forrester Wave: Data Security Platforms, Q1 2023](#)

INGRESS

by iCognition

The next generation
Content Services
Platform has arrived!

Find the right information at the right time.

UPGRADE TODAY

Fast track your information, securely!

- ✓ Build and deliver your own content services within corporate apps.
- ✓ Find, secure and protect your vital and sensitive records, regardless of where they live.
- ✓ Supercharge your digital transformation and prevent risks.
- ✓ Ensure your vital information is always safely managed in the latest software.

iCognition's trusted service offers:

- ✓ Secure to government Protective Security Policy Framework standards.
- ✓ ISO27001 Information Security Management Infrastructure.
- ✓ IRAP security assessed to the level of PROTECTED.
- ✓ Support team available 24/7.

DISCOVER

PROTECT

SECURE

USE

1300 426 400

[icognition.com.au](https://www.icognition.com.au)



5 reasons to explore data governance automation opportunities

By Bluestonex

Data governance is becoming an increasingly critical aspect of modern businesses as organisations rely more and more on data to drive decision-making and create value. Master data governance automation presents a significant opportunity for organisations to achieve these objectives by automating routine data management tasks and improving data visibility, accessibility, and quality.

Automation tools are rapidly changing the landscape of almost every industry around the globe, but rather than replacing workers they're supplementing the hard work that's carried out by trained professionals and serving as efficiency tools to get the most out of human staff.

Automated processes can help to ensure that data is collected, stored, and managed consistently across an organisation. This consistency is essential for maintaining data quality and complying with regulations such as GDPR or CCPA.

It can also help to identify and flag data quality issues, such as incomplete or inaccurate data. This can help data stewards and analysts identify areas for improvement and take corrective action.

Automation is proving to be key in helping organisations achieve better data governance by improving the consistency, quality, and traceability of their data.

Let's look at five key ways in which master data governance automation can support business efficiency, compliance, and performance.

1. Tailor processes to your complexities

Data governance automation solutions can help organisations tailor processes to their specific complexities by providing a customisable framework that can be adapted to meet their business's unique needs. With automation, organisations can define their data governance policies, standards, and procedures, and then automate the enforcement of these policies across their entire data landscape.

Automation can also help organizations identify and manage complex data dependencies and relationships, such as those found in multi-tiered architectures or complex data models.

By automating the tracking of data lineage and flow, organizations can gain a better understanding of how their data is being used and ensure that it is being managed appropriately.

2. Deskill data management roles

Master data automation has the potential to deskill data management roles by automating repetitive and routine tasks. For example, automation can be used to identify and flag data quality issues, reducing the frequency of manual data quality checks. Automated processes can also be used to enforce data

a governance policies and standards, which removes the need for manual oversight and review.

Automation can also help data management professionals manage data at scale by providing automated data lineage tracking and data flow mapping, which reduces the need for manual data discovery and reduces the risk of errors.

3. Focus on the bigger picture

Automation can also help organisations gain a better understanding of their data landscape by providing automated data lineage tracking and data flow mapping. This allows organizations to see how data is being used across their entire ecosystem and identify areas for improvement or optimisation.

By automating these processes, organisations can gain a more holistic view of their data, which can inform their overall data strategy and decision-making.

4. Decrease time to market

Data governance automation can help organisations decrease time to market by streamlining data management processes and reducing the time and effort required to manage and maintain data. By automating routine tasks such as data quality checks, data lineage tracking, and data flow mapping, organizations can ensure that data is accurate and compliant with regulations in a timely manner.

Automated data governance processes can also help organisations improve data accessibility, which can enable faster decision-making and product development.

By providing a unified view of data across the organisation, data governance automation can help ensure that data is available to stakeholders when and where they need it, reducing the time required to access and analyse data.

5. Get full process visibility

Organisations can get full process visibility by utilising data governance automation technology to gain a comprehensive view of their data landscape, including how data is collected, stored, processed, and used across the organization.

By automating data lineage tracking and data flow mapping, organizations can see how data moves through their systems and identify potential bottlenecks or areas for optimisation.

Automation can also help organisations enforce data governance policies and standards consistently across their entire data landscape, ensuring that all data is managed in accordance with regulations and best practices. By automating the monitoring of data quality and compliance, organizations can gain a more comprehensive view of their data and ensure that it is accurate and compliant.

The future of data governance

Automation technology is paving the way for new ways of working in every sector, and data governance is no different. By embracing MDG solutions and data governance automation tools, data governance professionals can improve the quality and consistency of their work in order to better support their cross-departmental colleagues.

Automate ministerials, correspondence, approvals, purchases, FOIs and more.

Easily engage staff in digital business processes using RM Workflow.

Engage them effortlessly in Outlook and web browsers to streamline your business processes, just like Tasmanian Government, Tyson Foods, and NSW Property has.

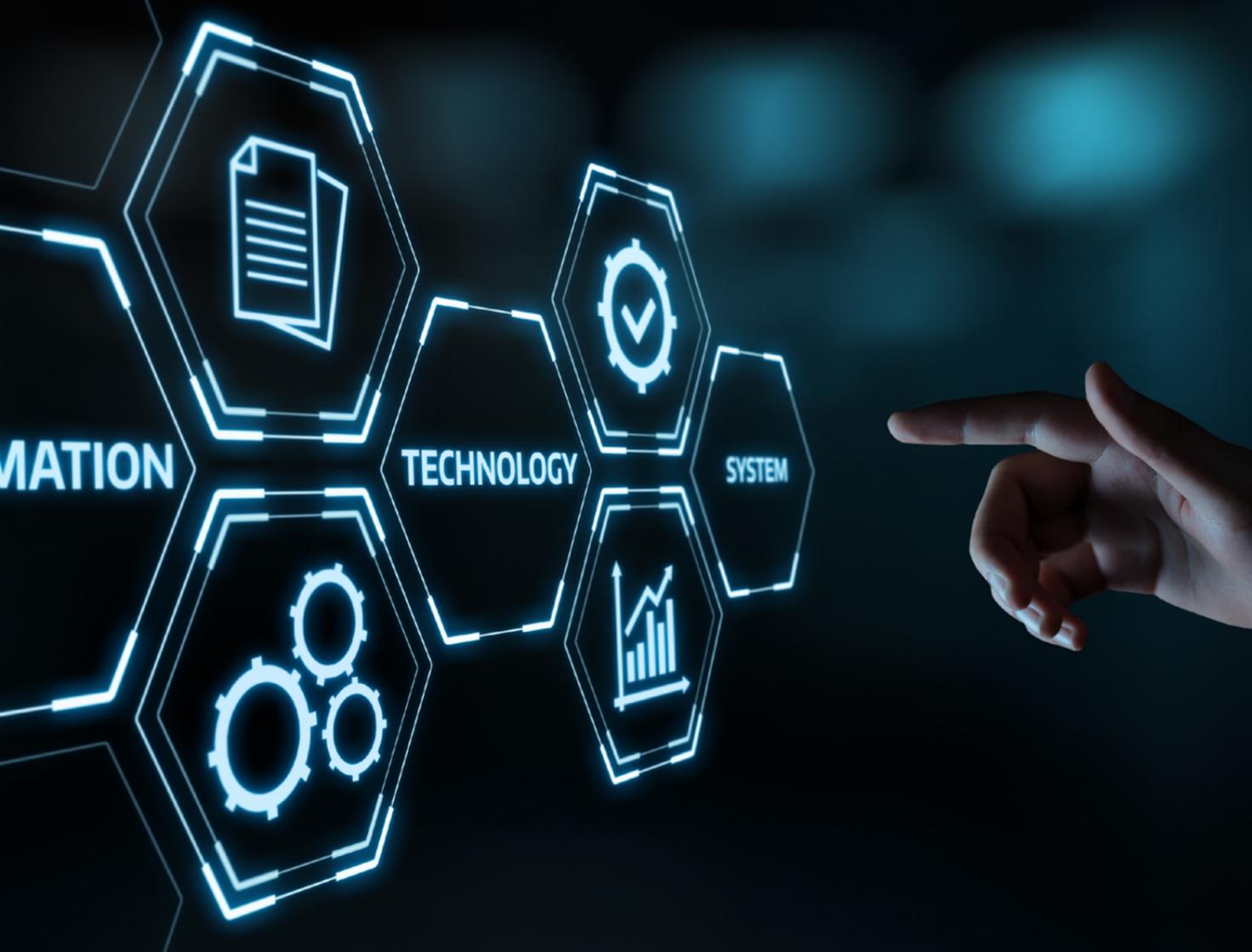
RM Workflow controls your records in Content Manager to ensure information security, audit and compliance while delivering ease of access and use.

Easily build new processes to supercharge your digital transformation using RM Workflow.



Request a demo

1300 426 400 | icognition.com.au



3 reasons companies shy away from automation

By **Torsten Malchow**

By now, we're all familiar with the promises of automation: efficiency gains, relief from talent shortages, greater efficiency, and increased margins. Sounds like a no-brainer, but if that were true, there wouldn't still be so many organizations that have not automated all or any of their processes. But why the ongoing hesitation?

Let's take a look at three common concerns that hold decision-makers back from implementing business process automation – and whether these concerns are still valid today.

Automation Barrier #1: Business Disruption

Will implementing automation cause delays that could impact your ability to meet SLAs? What happens when legacy software won't play nice with your new automation solution? Or when you have to adjust your existing processes to accommodate the solution? Delays that arise from mistakes are problem enough; delays that arise from a planned implementation are unacceptable for service providers.

Automation Barrier #2: Lackluster ROI

One of automation's biggest promises is cost reduction, which makes it all the more ironic that unforeseen cost explosion is one of the most common fears holding organizations back from automating. And there's a good reason for that fear. The ROI timeline for automation takes a hit any time the flow is interrupted by any of the examples given for Barrier #1. A recent [survey from Economist Impact](#) found that 50% of businesses feel they aren't achieving significant value from their technology investments.

The reality of designing an automation solution for an organization, then quickly deploying it and leading the needed organizational change management – all while maintaining data privacy and top-notch customer service can be a difficult balancing act. If any part of this balancing act stalls, ROI quickly evaporates, and that's why investment proposals for automation draw understandable scrutiny.

Automation Barrier #3: Data Privacy

Nothing can halt a project faster than a potential data leak or security breach. Any loss of control or transparency is paired with the genuine fear of

reputational harm or a hit to customer retention.

Picture, for example, a healthcare file. One file can carry the entirety of someone's personal data; if this complete data set is then visible to one individual, the risk for potential misuse is high. Or consider the potential for downstream mayhem if customer service reps respond to a claim incorrectly on account of inaccurate system data.

Even traditional automation solutions with higher-than-average 95% accuracy rates can introduce huge risks when cross-referencing a record in error, exposing additional personal data.

Are these automation fears valid today?

The truth of the matter is that these fears are all still valid to some degree. Automation solutions like intelligent document processing have improved over the years, but important gaps remain around continuity of service, disaster preparedness, skilled resources, and data security to name a few. Until now, there hasn't been a viable solution for covering these gaps in automation.

Collective intelligence offers a solution. By combining human and artificial intelligence, we're able to optimize the solution to improve the way people interact with the data entry tasks previously considered impossible to automate. Let's revisit the three automation fears with a collective intelligence approach:

Business disruption is the biggest fear when introducing new ways of working. With an on-demand

option to support document and data processing, organizations need not fear those dreaded automation gaps. Collective intelligence can and should be tapped whenever it doesn't make commercial sense to try to tweak an automation solution to cover difficult to automate tasks.

As far as ROI is concerned, transactional access to any number of skilled workers means processing volume spikes no longer pose a threat to the bottom line, and with collective intelligence, you know up front exactly what scaling up or down will cost. Not to mention lessening the financial impact of bad data feeding and training your algorithms.

With access to 2.3 million crowd contributors who can simultaneously label data at an accuracy rate of 99%, you can build a solid and accurate foundation for AI and machine learning at unprecedented volumes and speeds.

Lastly, while crowdsourcing in name alone may not imply high levels of data security, collective intelligence solutions like ScaleHub can offer foolproof data privacy with techniques such as snippeting and scrambling sensitive data. When a particular process requires that a document be viewed in its entirety, ScaleHub can be easily configured to access a select group of crowd contributors.

A webinar on this topic can be viewed [here](#).

Now based in Australia, **Torsten Malchow** is Chief Revenue Officer at [ScaleHub](#). Email him at torsten.malchow@scalehub.com

UPFLOW

Driving Digital Transformation in the workplace

Discover why your business should chose our products for Digital Transformation

upflow.com.au



How to identify Data Owners, where multiple areas use the same data?



By Nicola Askham, The Data Governance Coach
Identifying Data Owners is something that many people struggle with when they are starting out in Data Governance. When multiple different teams use that data it can often confuse matters, which is why I think this is a good question to answer.

It is something I come across an awful lot when helping my clients do data governance and I'm sure you will too, because unless the data is only used by one area, it's often not clear-cut who the data owners should be.

If you have read any of my other articles about data ownership you will know that in my experience, it really is important that you only have one data owner per data set, because if you have any more you end up with a situation where a number of people get together and they discuss and debate the data, but they rarely come to any conclusions and they just totally derail your data governance initiative. Simply, it doesn't work.

I believe very strongly that you should have just one data owner per data set and, yes, it can be challenging if you have multiple people using the same data and even more challenging when they all want to own the data but there are a number of different ways of dealing with this.

My preferred way is to see if I can break down the data and identify different chunks of it that can be split across multiple data owners. For example, for one organisation, which was an insurer, we had a big debate over who owned the customer data and the head of underwriting believed quite strongly that they owned it, but the head of marketing also believed that they owned customer data and when we sat and talked to them we actually agreed that they owned different subsets of it.

We broke it down and we had customer risk details owned by the underwriting area and customer contact details were owned by the marketing team and that worked very well... for a few months.

They got on and did everything we asked them to do

as part of doing data governance until we got to the day when somebody reported a data quality issue with postcode data and my heart sank because I had this horrible feeling that I knew what was going to happen.

I was right, when we asked them both who owned the postcode, they both said they did, and they both believed it was them.

Interestingly, because we had split the data out, they'd both been doing the role and got their head around it for a few months. We got them back together and discussed it and at that point, the head of marketing said "You know what, I actually don't think I am the data owner. I think I'm a key consumer of the data and I want my needs and requirements of that data to be considered, but I don't think I am the right person to be the data owner." We then put all customer details back into one data set and had one data owner.

The moral of that story is... splitting it sometimes works, and sometimes it doesn't.

Simply, you have to be flexible and understand that you may need to change it again further down the line, but it doesn't stop you from trying.

The other way of doing it if splitting the data into subsets it isn't an option, is to look which area or team really dictates the standards by which that data is captured. Do you have somebody that is setting the rules and saying this is how we do this? Because in which case they should be the data owner.

If you've got a number of other teams elsewhere in your organisation that are allowed to set the rules around that data (and that is a very rare circumstance) I sometimes come up with a two-level data owner model, but I prefer to use that as an absolute last resort because adding any complexity to your data governance framework makes it harder to embed and harder to make it successful.

Don't forget if you have any questions you'd like covered in future videos or articles please email me - questions@nicolaaskham.com

Originally published on www.nicolaaskham.com

Kapish

Empowering Secure Technology Solutions



Talk to us today to find out how our suite of products and services can help you get the most out of Content Manager.



Call 1300 KAPISH | info@kapish.com.au | kapish.com.au

Employees at largest Companies use Easy-to-crack Passwords

Even employees at the world's richest companies' have unbelievably poor password habits, reveals new research by NordPass. Despite cybersecurity experts repeatedly urging businesses to take better care of corporate passwords, the wealthiest companies worldwide still find the world's worst passwords - "123456" and "password" - good enough to secure corporate digital assets.

"On the one hand, it is a paradox that the wealthiest companies on the planet with financial resources to invest in cybersecurity fall into the poor password trap. On the other hand, it is only natural because internet users have deep-rooted, unhealthy password habits.

"This research once again proves that we should all speed up transitioning to alternative online authentication solutions," says Jonas Karklys, CEO of NordPass.

Though NordPass looks at the change in internet users' password habits year-round, this year the company specifically investigated passwords that employees of the world's biggest companies from 31 countries use to secure business accounts. The researchers compiled 20 industry-specific passwords lists.

According to the study, the passwords "password" and "123456," which shared the first two spots in last year's list of the world's most common passwords, are also popular among the largest companies' employees.

Across all 20 analysed industries, both passwords were found among the seven most commonly used passwords.

Some industries were more creative than others. The password "dummies" ranks 6th among consumer goods sector employees, "sexy4sho" 16th among real estate employees, and "snowman" 11th in the energy field. Interestingly, people working for corporations in the finance field seem to be in a serious need of a vacation, with the passwords "ready2go," "vacation," and "summer" as their top picks for passwords.

Common Inspiration for Passwords

Same as among ordinary internet users, dictionary words, names of people and countries, and simple combinations of numbers, letters, and symbols make up most passwords presented in the research.

However, the remaining 32% indicate another interesting trend. The world's wealthiest companies' employees love passwords that directly reference or hint at the name of a specific company.

The full company name, the company's email domain, part of the company's name, an abbreviation of the company name, and the company product or subsidiary name are the common sources of inspiration.

"These types of passwords are both poor and dangerous to use. When breaking into company accounts, hackers try all password combinations referencing a company because they are aware of how common they are.

The employees often avoid creating complicated passwords, especially for shared accounts. Therefore,

they end up choosing something radically basic such as the company's name," says Karklys.

Wide Representation of Countries and Industries

The password analysis was conducted in partnership with independent third-party researchers specializing in research about cybersecurity incidents.

They examined the world's 500 largest companies by market capitalization, which represented 31 countries and 20 industries.

The United States (46.2%), China (9.6%), Japan (5.8%), India (4.2%), the United Kingdom (4%), France (3.8%), and Canada (3.6%) are the countries most represented in this research. Also, most of the companies analysed fell under the finance, technology and IT, and healthcare sectors.

"Although password trends slightly vary each year across different audiences, the general take is that people continuously fail with their password management, and the world desperately needs to switch to new online authentication solutions such as passkeys," says Karklys.

Various progressive businesses such as Google, Microsoft, Apple, PayPal, KAYAK, and eBay have already adopted passkey technology and are offering passwordless log in to their users.

According to Karklys, in no time, other online companies will follow this trend. NordPass has developed a solution to store clients' passkeys and is developing a tool for businesses to easily integrate passkey support to their websites.

Tips to Secure Business Accounts

According to an IBM report, in 2022, stolen or compromised credentials remained the most common cause of a data breach in companies, accounting for 19%. Karklys says that by implementing a few cybersecurity measures, businesses could avoid many cybersecurity incidents.

Ensure company passwords are strong.

They should consist of random combinations of at least 20 upper- and lower-case letters, numbers, and special characters.

Enable multifactor authentication or single sign-on.

Although MFA set up on another device, connected with email or SMS codes, guarantees an additional layer of security, single sign-on functionality helps reduce the number of passwords people have to manage.

Critically evaluate who is granted account credentials.

Access privileges should be removed from people leaving the company and passed on only to those who need certain access.

Deploy a password manager.

With a business solution, companies can safely store all their passwords in one place, share them within the organization, ensure their strength, and effectively manage access privileges.

View the study at <https://nordpass.com/poor-company-passwords/>

Manufacturers urged to Prioritise Cybersecurity

The Australian Cyber Security Centre (ACSC), Computer Emergency Response Team New Zealand (CERT NZ) and New Zealand's National Cyber Security Centre (NCSC-NZ) have joined an international push urging technology manufacturers to take urgent steps necessary to ship products that are "secure-by-design and default."

A joint document was developed by the agencies in partnership with U.S. Cybersecurity and Infrastructure Security Agency (CISA), the US National Security Agency (NSA), the FBI, and the cybersecurity authorities of Canada, the UK, Germany and the Netherlands.

It states, "The authoring agencies strongly encourage every technology manufacturer to build their products in a way that prevents customers from having to constantly perform monitoring, routine updates, and damage control on their systems to mitigate cyber intrusions. Manufacturers are encouraged to take ownership of improving the security outcomes of their customers.

"Historically, technology manufacturers have relied on fixing vulnerabilities found after the customers have deployed the products, requiring the customers to apply those patches at their own expense. Only by incorporating Secure-by-Design practices will we break the vicious cycle of creating and applying fixes."

The authoring agencies urge manufacturers to revamp their design and development programs to permit only Secure-by-Design and -Default products to be

shipped to customers.

"Products that are Secure-by-Design are those where the security of the customers is a core business goal, not just a technical feature. Secure-by-Design products start with that goal before development starts. Secure-by-Default products are those that are secure to use "out of the box" with little to no configuration changes necessary and security features available without additional cost. Together, these two principles move much of the burden of staying secure to manufacturers and reduce the chances that customers will fall victim to security incidents resulting from misconfigurations, insufficiently fast patching, or many other common issues."

The Guide provides a list of software development best practices as well as specific recommendations such as eliminating default passwords.

"Organizational decisions to accept the risks associated with specific technology products should be formally documented, approved by a senior business executive, and regularly presented to the Board of Directors," is another recommendation.

The partners also call for "radical transparency and accountability": not only should vendors take part in vulnerability disclosure programs, "advisories and associated common vulnerability and exposure (CVE) records" should be "complete and accurate."

View the Guide [HERE](#).

FileBound Solutions

Drive Success with FileBound Solutions

Amanda & Sean are leading their organisation to success

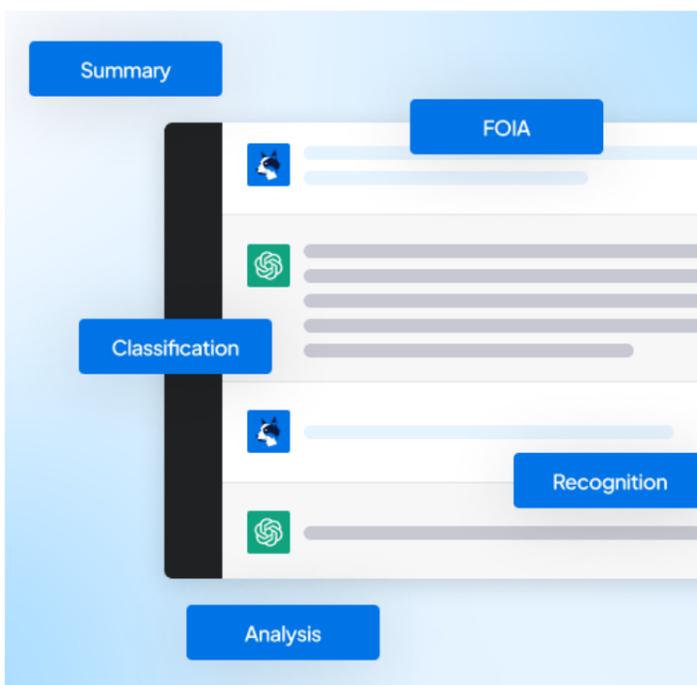
FileBound's digital work processing solutions save time, increase productivity, enhance transparency and provide control over their business.

Let's Talk Solutions

filebound.solutions
1300 375 565



Can ChatGPT and large language models streamline records management?



By Jason Franks, RecordPoint

In the few months since OpenAI's ChatGPT language model has roused public attention, there has been enormous interest and speculation about what they can do and how valuable they might become. In the records domain, where practitioners have long been overwhelmed by the exponentially growing volumes of born-digital data that they are expected to manage, these large language models (LLMs) could become a real game changer.

LLMs are astonishingly good at generating text. They can hold a conversation, write an essay, answer questions, or summarize text in coherent, grammatically correct English, or in many other languages. It's convincing enough that one of Google's own engineers came to believe that LaMDA, one of their own language models, [had become sentient](#).

The hype cycle has raised some unrealistic ideas about what LLMs can do, but vendors have done a poor job of communicating what they cannot. As we have quickly seen, LLMs are prone to bias, hallucination, or to outright lying. The popular technology review website [CNET has been forced to retract articles written by AI](#) because they are factually inaccurate. Meta's Galactica--an LLM similar to ChatGPT--[had to be taken offline after only three days](#) because it was spouting racist content.

There is a growing body of skeptics who maintain that they are only useful for generating throw-away SEO content or for cheating on homework. But there is also rising concern that these LLMs can be used to automate criminal activities to an industrial level, [generating disinformation, drowning out discourse](#), or even [tricking people into enabling cyber-crimes](#).

The truth lies somewhere in the middle. LLMs have

capabilities and they could be transformative for the management of records and archives, but only if they can be employed in ways that are credible and accurate. This requires a basic understanding of the way LLMs operate.

How Large Language Models work

Language models are built on neural networks--a type of machine learning algorithm that crudely approximates the workings of the human brain, in which input data is passed through layers of heavily inter-connected 'neurons' until they reach an output layer. The 'knowledge' of a neural network is entirely in the connections between neurons, which are weighted to [transform](#) the input data into the desired output as it flows between them.

The training process for a neural network is the same as for any machine learning algorithm. Example data is fed through the network and the weights of the connections are adjusted using a mathematical process that minimizes error.

Machine learning training follows one of two modes: **supervised** and **unsupervised learning**. In supervised learning, we are training the network to perform a certain task. The training data includes the results we want to output, and we can train the network to do very specific tasks. During unsupervised learning, on the other hand, we have no target output. The training process allows the neural network to discover statistical patterns and relationships in the input data that are too difficult to find using declarative logic.

LLMs employ what is called **semi-supervised learning**. They are pre-trained in an unsupervised mode by feeding them massive quantities of text data, which allows them to encode statistical information about language: which tokens (words or parts of words) are likely to be followed or preceded by which other tokens. The pre-trained models can then be 'fine-tuned' in a supervised mode to perform tasks where we do have a target output, such as classification or answering

questions. This process is called **transfer learning**: the knowledge gained by unsupervised learning can then be transferred to specific tasks.

When an LLM is asked to generate text, it takes the input data and figures out how to transform it, using an incredibly complex statistical process, into the output it thinks you want. This could be a summary of an article, the answer to a question, an essay, a movie script, an entity recognition task, or a sonnet. Or, as author Cory Doctorow puts it--LLMs are a very powerful form of the autocomplete functionality we see in smartphones and search engines.

What language models cannot do

LLMs don't actually know anything. They write coherently and convincingly, but they are not databases or search engines. LLMs are very good at manipulating language, but they cannot be trusted to deliver factual data, much less to make decisions. At best they will regurgitate unverified facts from the data used to train them. At worst, they will synthesize convincing sounding lies. The output is too coherent to be easily discounted as nonsense.

Not only are LLMs untrustworthy with facts, but they cannot actually reason. They can't process logic; they can only give the semblance of it by parroting the forms they have seen humans employ to argue. LLMs cannot add; they only recognize that when humans write "1+1", the answer is usually "2".

LLMs will never be able to do your book-keeping, plan your finances, or manage the data flowing through your network. All they can do is sit there waiting for you to give them a string of words--and give you the answer they think you want to hear.

How can language models be useful and trustworthy for records managers?

LLMs are not a good source of information, reasoning, or calculation, but they are powerful tools for manipulating text, and this is where we find applications where they can be invaluable. The common theme for these scenarios is that we must provide trusted data as input to the LLM to process, rather than relying on whatever questionable information has been used to teach it how language behaves.

Text Classification

LLMs can be trained using your own classified records, to categorize records to a disposal schedule, or to any other taxonomy you might require. This LLMs provide superior skill at these text classification tasks, outperforming older statistical models and non-pretrained neural networks by some margin.

Because the LLMs will be fine-tuned using trusted data, we find they are an accurate and reliable way to classify records that cannot be classified using their metadata.

Text Summarization

LLMs provide a powerful technology for rendering digests of record text, which can be used to help record managers more quickly understand what vast quantities of records are about without needing to open every one of them. This will be invaluable for identifying records that are relevant to FOI requests or other investigative tasks where record managers and archivists need to find which records are relevant or interesting. It may also help expedite the disposal process, giving record managers a quick way to spot check records before they are approved for destruction.

LLMs are trustworthy on these tasks because we have provided them with text to process as input.

Question Answering

LLMs can synthesize answers to sophisticated questions about the text in a record or corpus of records yielding robust results. The power of this application is that it is free form. Where text summarization will try to extract the most important information in a general sense, question-answering allows users to make targeted and specific queries against large amounts of text content. LLMs have the capability to interpret those questions contextually when seeking answers, considering synonyms and phrasing across paragraphs that goes well beyond the capabilities of common text search technology.

Because the questions are directed at the text of the records, LLMs are generally truthful on this task. ChatGPT is likely to tell you there is no relevant information if it can't find any. But of course, it's always worth fact checking the answers.

Entity Recognition

LLMs are very good at **entity recognition** tasks, identifying people, places, organizations, and other named objects referenced within a body of text. While there are other technologies that can do these tasks well, in many cases we do not wish to index this information due to the risk of exposing personal information. An LLM like ChatGPT can give us an easy way to discover this information on-the-fly, once we have identified relevant records.

Sentiment Analysis

ChatGPT and similar LLMs are also skilled at sentiment analysis--detecting the sentiment, or tone, of a document. This type of application is commonly used in the analysis of informal communications data: social media, email, and chat messages. With the growing volume of these types of records under management, this is likely to be of increasing interest to the records and archives community. One use case might be tracing social media posts generated by a disinformation campaign targeted at a political candidate or a public health issue. Identifying which messages promote positive or negative sentiment can help to aggregate these messages and attribute them to a bot farm or a bad actor.

In Summary

While LLMs are not useful or trustworthy replacements for search engines or suitable for broad analysis tasks, they have excellent applications beyond generating throwaway content. LLMs can help us to refine records into categories for disposal sentencing. They can be leveraged to enrich record metadata by mining a record's content for sentiment, named entities and other properties. They can summarize records, allowing record managers to more easily grasp their content, and they can allow record managers to assess text for specific answers. LLMs can help us enrich and refine records so they are easier to search, discover, aggregate, or interrogate, either for routine compliance purposes or to assist in forensic activities.

Language models like ChatGPT offer powerful new ways of understanding and interacting with digital records. Once they hype has died off this technology is likely to become an intrinsic part of our computing technology, unnoticed and unremarked upon, in much the same way that autocomplete is now something we take for granted. Here at RecordPoint, we'll be taking a close look to see how the technology may enhance our products and deliver better outcomes for customers.

Jason Franks is Engineering Team Lead and Data Scientist at RecordPoint. Originally published [HERE](#)

Legacy fix adds up for Dept. of Communities and Justice NSW

The NSW Department of Communities and Justice is underway with a major Legacy Data Migration Program which is retiring numerous historical platforms after extracting and transitioning critical legacy data to a modern, cloud-based analytics & reporting solution.

The Department of Communities and Justice (DCJ) was formed on 1 July 2019 when the NSW Government brought together the departments of Family and Community Services, and Justice. It incorporates NSW Courts and Tribunals, Corrective Services NSW, Family and Community Services and the NSW Trustee and Guardian as well as other agencies.

Legacy or "historical" data is found in virtually every organisation that has been operating for more than a few years. A large percentage of legacy data has ongoing business value and is commonly subject to laws governing its retention and treatment.

Even when a system ceases its daily operational role,

the lifespan of the data it holds can be measured at a minimum in years and more often in decades.

The significant operational costs of managing the platforms and applications that are associated with legacy data presents a vexing challenge for many executives today.

Australian company Datalynx claims to have the answer with its innovative solution for retiring expensive legacy platforms and replacing them with modern reporting solutions that maintain data compliance and support any ongoing querying and reporting requirements.

With over 4 billion transactions and millions of files already successfully migrated for Communities and Justice, Datalynx says it delivered outcomes up to 60% faster and at 50% less cost than traditional options.

The work completed to date as part of this ongoing initiative will result in millions of dollars saved in operational budgets over the lifetime of the data, while enhancing the usability and security of valuable data assets.

In addition, the solution provides the Department with the assurance that it has addressed its record-keeping compliance obligations via an approach that has been endorsed by the NSW State Archives & Records Authority.

"The DMS Phoenix solution is unlike anything else seen in the market today. 20 years of experience in data migration and transformation has enabled Datalynx to build a solution that takes data platform modernisation and the subsequent retirement of the legacy applications to a new level." says Brian Clark, Sales and Marketing director at Datalynx.

The challenges with Legacy Platforms, Applications and Data

Modernisation initiatives seek to achieve enhanced efficiency and cost reduction. IT management faces the ongoing challenge of enabling new technology while ensuring legacy applications remain accessible after cloud migration or application transition. However, there are challenges in maintaining the availability of legacy platforms which include:

Escalating support costs

Approximately 30 percent of the average organisation's technology footprint is comprised of legacy platforms. Those older technologies commonly consume a disproportionately large percentage of IT budgets.

Ongoing legacy platform support and licensing costs are significant, as are the rising expenses for skilled resources needed to support older technology.

Cyber risk

In comparison to modern technologies, legacy platforms present a higher level of security risk, that only increases over.

Ageing technology often operates out of vendor support and may even be "end-of-life." It rarely integrates easily with modern platforms and struggles to adapt to a rapidly evolving threat landscape. Older platforms are also less viable for implementing modern security models.

Compliance

There are no exemptions to a growing number of global regulatory requirements governing data handling and security, including GDPR, CCPA, and PIPL.

Across Australia, compliance considerations include the Freedom of Information Act, Information Security Manual (ISM), Privacy Acts, as well as specific laws regulating data in various domains such as health, insurance, finance, etc.

Legacy platforms and applications tend to have limited capacity to address evolving compliance requirements for data discovery, control, handling, and reporting.

Data protection

The Australian government requires organisations, via Information Security Manual (ISM) mandates, to ensure protection of data in the cloud or in conventional environments. Legacy applications rarely meet all the key ISM controls specified for data protection.

Record-keeping

Corporate record-keeping obligations include the retention of historical content for extended periods (sometimes decades or indefinitely) requiring ongoing maintenance of legacy systems, applications and data at significant cost.

Declining talent

Few IT practitioners are excited to learn yesterday's technology. With the passage of time there is a diminishing pool of professionals available to support ageing technology. In contrast, the costs of the specialist support services required for legacy systems continue to rise.

Traditional solutions for managing legacy data

Unlike unstructured data, databases or structured data in large business systems is for the most part unusable without its associated application or system.

This complex data needs the application to make sense of it and its relationships which can span across hundreds to thousands of individual tables and at times billions of transactions.

This makes ongoing use and retirement of these systems challenging with three main approaches typically being employed today,

- Lift and shift – move the application and data to new or cloud-based infrastructure, this only solves stability issues.
- Retire the application and archive the database – without the application the data is mostly unusable, the application would have to be reinstalled to regain access.
- Migrate the data to an open standards format.

Datalynx Solution

DMS Phoenix solves the challenges of ongoing legacy data utilisation by incorporating each application's business and functional logic into the solution.

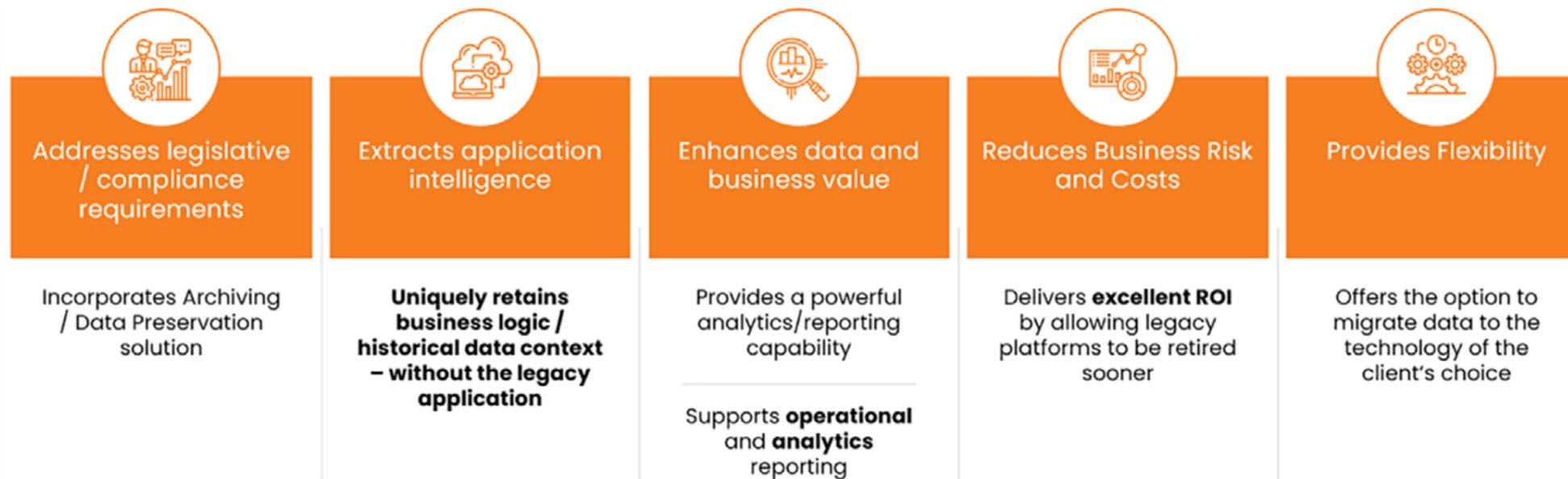
This enables the data to be preserved in its entirety and for existing reports and data querying capability to be reproduced within the new solution.

This helps deliver cost-effective data modernisation capabilities for transitioning any legacy data to the latest cloud-based technologies with options for record-keeping compliance, historical reporting, as well as modern data querying and analytics.

Once a system has been through the Phoenix process it can confidently be retired, delivering cost savings to fund the retirement of additional legacy platforms or undertaking further modernisation initiatives.

"DMS Phoenix provides clients with the assurance they need to confidently retire legacy platforms (infrastructure, operating systems and applications) to significantly reduce risk and achieve an outstanding ROI," said Clark.

For more information, visit <https://www.datalynx.com.au/>



Datalynx has drawn on 20 years of experience with complex, large-scale data migration and transformation projects to create its DMS Phoenix solution for data platform modernisation to the cloud.

What is enterprise application integration?

By Lindsay Sterrett, Micro Focus

Did you know that the volume of enterprise content is expected to [increase by 4.5x over the next two years](#)? If you're facing information management challenges such as siloed data, content sprawl, disjointed workflows and multiple disparate systems, strong and reliable integrations can help!

When done right, enterprise application integration can play a significant role in an organization's ability to manage the high volumes of information required to keep business moving.

Broadly speaking, **enterprise application integration (EAI) is the process of connecting and integrating business applications and systems** – such as enterprise resource planning (ERP), customer relationship management (CRM), human capital management (HCM) and supply chain management (SCM) solutions – so they can exchange data and interact with each other.

EAI can help organizations [streamline and automate their business processes](#), improve efficiency, overcome siloes, shore up security and compliance, and make better use of the data they generate.

For example, an organization may use one system to generate customer invoices, and another to create and share customer communications. But staff need information from both systems to have a full picture of a customer's situation (especially if that person is calling in with a complaint). Without integrating these systems, staff are left switching back and forth between applications, wasting time and creating friction throughout the process – a problem for both employee engagement and customer satisfaction.

What are some challenges of integrating enterprise applications?

"When information must flow across multiple departments, systems, and lines of business, it leads to fractured information contained in each of the individual applications. And if you don't establish a way to overcome these silos of information, then you end up with decision-making that's incomplete and based on a very limited view of the business process," says Wolfgang Schmidhuber-Tindle, an information management expert at OpenText.

Implementing EAI solutions comes with a range of challenges, including:

Complexity: Integrating multiple applications and systems can be technically challenging and time-consuming, especially when those systems use different technologies or data formats, which is often the case. However, using EAI to deliver content into lead applications is a critical requirement for large businesses looking to automate key workflows.

Security: Protecting the data being exchanged between systems is critical, so organizations need to ensure that their EAI solutions include strong security measures and data privacy protections.

Scalability: As organizations grow and change, their EAI solutions need to be able to adapt to meet their changing needs.

Usability: "In the end, it's always about the end user,"



says Bernd Hennieke, an EAI expert with OpenText. "If it's not usable, seamless and easy for the end user then it's pretty much worth nothing. You can protect all kinds of content and fulfill all kinds of regulations. But if the end user can't work with that content and do their job more efficiently, you've got a problem."

How does enterprise application integration work?

Enabling EAI usually involves many [enterprise application integration technologies](#) and approaches, including APIs, middleware, integration platforms, highly customized solutions and more. The specific technologies and approaches depend on the unique needs and requirements of the organization or use case.

"For us, it's not about a generic capability of connecting anything to anything. It's about bringing relevant Information Management solutions into all sorts of lead business applications, and by virtue of that, we need to be very good at integrating," says Schmidhuber-Tindle.

[Integrating with lead applications](#) is one critical way organizations can solve information management challenges in the context of a user's workflow – whether they're working in SAP S/4HANA or SuccessFactors, Microsoft 365 or Dynamics, Salesforce Sales Cloud or Service Cloud, IBM Maximo, or AutoCAD, to name a few.

How does integrating enterprise applications support business growth?

By streamlining processes, improving data accessibility, increasing agility, and enhancing customer service, EAI can help organizations operate more efficiently and effectively, and stay competitive in fast-changing markets. Let's break that down in more detail:

Enhanced data accessibility: EAI allows both organizations and end-users to access and share data across different systems and departments, regardless of which application users are working in or where they are in the business process. These insights drive more informed decision-making and business planning.

Greater agility: With EAI, organizations can more easily respond to changing business needs and adapt to new technologies or processes. That's helpful when it comes to staying competitive in fast-changing markets (including downturns/recessions) and capitalizing on growth opportunities.

Better customer service: By integrating customer management information across systems, organizations can provide a more seamless and personalized experience for customers. Boosting customer

satisfaction and loyalty, of course, can drive business growth.

Improved efficiency: By automating information management and business processes, and reducing the need for manual data entry and reconciliation, EAI can help boost operational efficiency. That efficiency can lead to cost savings, increased productivity, and higher employee satisfaction.

Why is governance critical to successful enterprise application integration?

Organizations need to automate and optimize their information management processes while being careful to [meet and exceed internal and regulatory data privacy and compliance requirements](#).

"Any industry that operates in a highly regulated environment – financial services, government and energy utilities, healthcare and so on – is very much in need of governance and security when it comes to integration with lead business applications," says Hennieke. "It's never simply a question of technical integration, but also business logic integration, and governance around that."

It's also a matter of integration – or strategic partnership – at a company level. "We have unique partnerships with the lead application providers that drive business – Microsoft, SAP, IBM, Salesforce and many more," says Schmidhuber-Tindle. "As a result, we're often involved in not just addressing integration requirements down the line, but in defining specifications for APIs and interfaces from the very beginning. Working this way means we can attend to governance issues throughout the process."

For example, a European customer, FARYS, in the highly regulated energy sector needed a consolidated platform for processing and sharing 2M+ communications each year. "Now, every document that is generated in SAP, be it a bill, purchase order, or letter to personnel, is done by one system," Hennieke explains.

FARYS CIO, Inge Opreel, says that "the upgrade has enabled us to use APIs so we can connect more easily to SAP and to other systems. The connection between SAP and OpenText is a huge benefit for us." Read [the full case study](#).

What does the future of enterprise application integration look like?

"What I think is next is to make integration more intelligent, more automated and more seamless for the end user, delivering an increasingly differentiated experience," says Schmidhuber-Tindle. "We're on a continuous journey – internally, with our partners, and with our customers – moving from multiple, siloed enterprise integration points to a unified cloud platform that integrates entire ecosystems."

The main objectives of this kind of innovation, says Hennieke, are cloud-to-cloud application integration, API stability and security, and the ability to get things done through configuration rather than complex customization.

"When solutions are integrated seamlessly into the front-end of lead business applications, customers connect business processes, end-user and backend systems in a transparent and organic way," he concludes. "That transforms optimal user experience, process efficiencies and holistic information governance into a high-value information ecosystem."

Originally published [HERE](#)



ENCOMPAAAS

PRESENTED BY
PLATINUM PARTNER

INFORMATION

Race ahead with next-gen AI

EncompaaS information management platform helps enterprises harness the full value of their information and reduce risk.

encompaaS.cloud

The Importance of Capture in Document-Based Process Automation



By **Arnold von Büren**

Capture is dead, long live capture! 25 years ago, turning a paper document into a digital image was a rather big challenge. One needed these unwieldy devices called scanners and document capture application software.

The capture software would create an image, and typically store it in a .tiff format. Then, before these captured images could be put into an electronic archive, a person would need to manually add some index data.

This was known as 'late' capture. 'Late' because paper documents are only captured and electronically archived at the very end of an entirely paper-based (manual) process -- the whole purpose was simply to replace paper-based filing systems with an electronic archive for easy storage and retrieval. Such were the times!

Capturing forms and data developed relatively early in the 1990s and was initially called data capture to differentiate from document capture, as only the data is of interest and the images often get discarded. Different technologies existed, each focused on handling to deal with either machine- or hand-written content and special information (e.g., checkboxes).

Around 15 years ago 'early' capture began to surface, which means that documents are being captured (scanned) immediately upon arrival at the organization. Again, an image is produced but advances mean that OCR technology is applied to obtain textual (content) data. The normalization standard is typically PDF/A, which allows to keep the image information and its text data in a separate layer. 'Early' capture nowadays is widespread. It is called digitization and is the important first step for complete digital processing.

From digitization to intelligent document processing (IDP)

With the arrival of the internet, it became possible to scan documents from any office with so-called desktop scanners, and the most prevalent 'documents' became emails. Capturing the body of an email is

straightforward, however email attachments are an entirely different matter – the variety of attachment formats is mind boggling, and that's before we even get into the topic of emails attached to other emails, and/or containing archive media (of which there are again multiple types - .zip, .rar, etc.) Recognizing the formats and normalizing them into one single standard is the first challenge.

With a personal scanner in everyone's pocket and data entering organizations in increasingly various formats, organizations needed to be able to extract data from a wide range of sources, turn that data into information and gather insights.

The criticality of capture

Customers want the choice of communication (format, channel) with organizations, and organizations want to remove friction from customer-centric processes. To achieve this, organizations must have a system and process in place that treats all document ingestions in the same manner. Only this centralized, standardized normalization approach to capture guarantees the least amount of processing errors downstream.

Of course, I would not write this if the products and solutions provided by TCG Process could not fully provide the necessary functionality.

Capture is neither a thing of the past nor getting less important – quite the contrary. Capture remains a critical aspect of intelligent document processing (IDP) and digitization efforts, serving as the foundation for automating and optimizing business processes in organizations that are driven by document-based information flow.

By implementing effective capture strategies, businesses can unlock the full potential of their data and leverage it to drive digital transformation.

Pay attention to proper capture. TCG Process' strong roots in capture and IDP mean we know how important this is to get right so you don't pay for it somewhere downstream, where correction costs explode, process times increase dramatically, and customer satisfaction is impacted. Long live capture!

Arnold von Büren is CEO, TCG Process.

INTRODUCING RIGHT-SPEED™ SCANNING

Traditional high-speed scanning requires extensive prep and lots of labour, especially as jobs get messier and messier. High-speed scanners sometimes require multiple operators to keep them in continuous operation. This leads to additional labour hours driving up cost per image and driving down profitability.

The OPEX® Gemini™ scanner is designed for maximum versatility and configurability and handles documents at the right speed while requiring minimal prep and controlling costs.



Visit us on stand G19 at



25-27 JULY 2023
The Dome, Sydney Olympic Park



Visit digitiseyourdocuments.com.au to learn more or contact info@opex.com to schedule a demo today.

OPEX®

47 percent of Digital Workers Struggle to Find Information: Gartner

A recent survey by Gartner, Inc. found that 47% of digital workers struggle to find information or data needed to effectively perform their jobs.

“Employees struggle to stay afloat as information and applications flood their digital workplace. Although digital workers are putting in effort to try to efficiently manage this content to try reduce duplication and/or improve knowledge sharing and retention, finding the information needed to do their jobs can often be a challenge,” said Tori Paulman, Sr Director Analyst at Gartner.

“Digital workplace leaders need to create a process for their employees that enables them to agree on applications they use to accomplish work.” According to the survey, the average number of applications a desk worker, also referred to as a “knowledge worker,” uses is 11, compared to six applications in 2019. Forty percent of digital workers are using more than the average number of applications and 5% of workers use 26 or more applications at work.

On an average, 66% of the respondents agreed that better business outcomes could be achieved if IT provided universally accepted and supported applications and devices to get work done. When a digital workplace applications strategy attempts to solve every challenge with a new application, the result is that digital workers struggle to find information, make the wrong decisions due to lack of awareness, get irrelevant notifications and miss important updates amid the noise (see Figure 1).

Workers Would Accept Monitoring That Helps Them Be More Productive

Interest in employee productivity monitoring has grown since the pandemic. These systems are used to see whether employees are active on devices and in applications, or which employees are most productive and whether business outcomes are being met.

While employee productivity monitoring for the purposes at the lowest end of the spectrum is widely

distrusted and disliked, 96% of digital workers indicated that they would be willing to accept monitoring in return for assistance in at least one of the options provided.

Of the top three options, 34% of digital workers surveyed indicated they would accept monitoring in exchange for awareness of training classes and/or career development opportunities, 33% would accept monitoring for support in finding information to do their job, and 30% would accept monitoring in exchange for proactive outreach from IT support when facing problems with their computer or applications.

Workers Want Their Technology Problems Solved Proactively

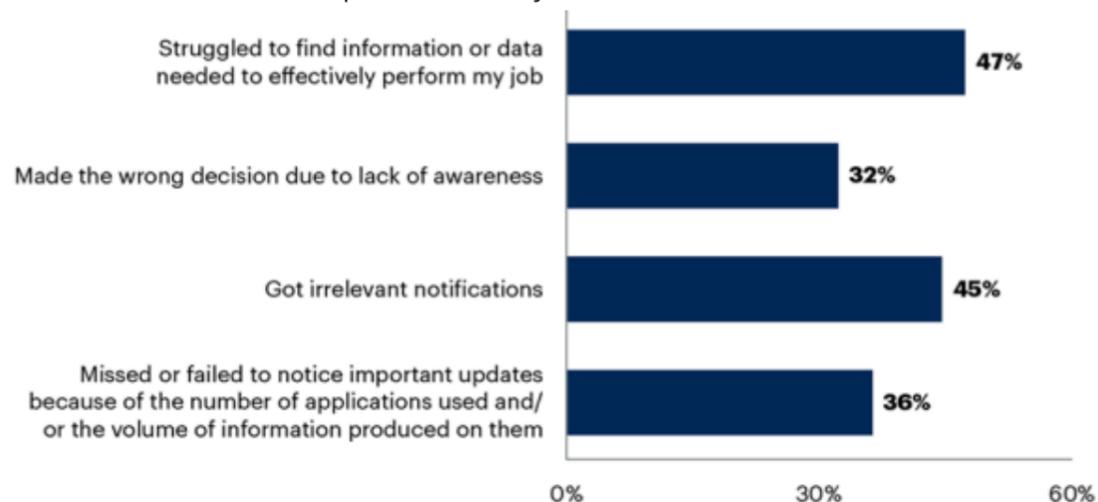
The survey found that digital workers’ top six preferred methods for solving issues with the technology they use for work are all through internal IT support, with the top three methods being live phone, chat and email conversations.

When asked why, workers stated their top reasons were the expertise of the person solving their issue and the speed of resolution. These findings shifted from 2020, when workers also preferred other methods to solve their issues with digital technology, such as receiving answers on the internet and asking a co-worker.

“Digital workers are now demanding IT support be more proactive, solving problems with computers and applications before they are reported or even noticed,” said Paulman. “Digital employee experience (DEX) tools can help IT teams achieve this by continuously improving device and application performance.

“Digital workplace leaders must step up to lead DEX, and recognize they are an experience leader with a technology toolkit. They should focus on developing the qualities and practices of an employee experience leader, such as building connections across the business and increasing empathy for the way employees experience technology change.”

The Gartner survey was conducted among 4,861 full-time employees that use digital technology for work purposes, at organizations with 100 or more employees in the U.S., U.K., India and China.



n = 4734-4802; All Digital Workers excluding Not sure/Not applicable

Q. Select how often you have encountered the following situations in your organization

Figure 1. Impact of Application Sprawl (Percentage of Respondents) Source: Gartner (May 2023)



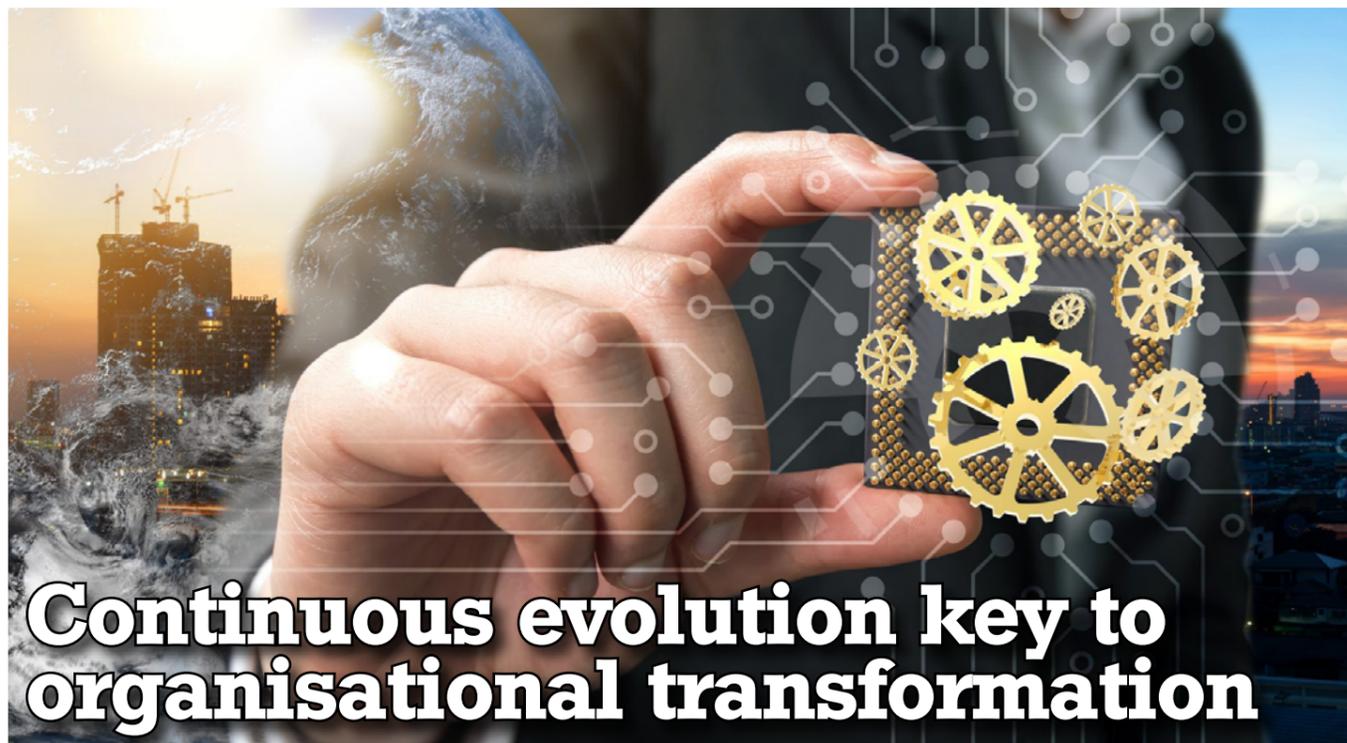
PRESENTED BY PLATINUM PARTNER



Turn information management into information opportunity

EncompaaS information management platform helps enterprises harness the full value of their information and reduce risk.

encompaaas.cloud



Continuous evolution key to organisational transformation

A new report by MIT Technology Review Insights seeks to understand how organisations approach transformation and the obstacles they encounter in adapting to a continually changing business and technology environment.

The report, “*Evolutionary organisations reimagine the future*,” is produced in partnership with Thoughtworks and draws on a survey of 275 executives and business leaders along with in-depth interviews with digital transformation, business strategy, and emerging technology experts from organisations including Prudential Financial, PEXA, and INSEAD.

The findings are as follows:

Digital transformation is not solely a technology issue. Adopting new technology for its own sake does not set the organisation up to continue to adapt to changing circumstances. Among survey respondents, however, transformation is still synonymous with tech, with 70% planning a new technology adoption in the next year, but only 41% pursuing changes to their business model.

The business environment is changing faster than many leaders think. Most survey respondents (81%) believe their organisation is more adaptable than average and nearly all (89%) say that they’re keeping up with or ahead of their competitors - suggesting a wide gap between the rapidly evolving reality and executives’ perceptions of their preparedness.

All organisations must build capabilities for continuous reinvention. The only way to keep up is for organisations to continually change and evolve, but most traditional businesses lack the strategic flexibility necessary to do this. Nearly half of business leaders outside the C-suite (44%), for example, say organisational structure, silos, or hierarchy are the number-one obstacle to transformation at their firm.

Focusing on customer value and empowering employees are keys to organisational evolution.

The most successful transformations prioritise creating customer value and enhancing customer and employee experience. Meeting evolving customer needs is the constant source of value in a world where everything is changing. However, many traditional organisations fail to take this long view, with only 15% of respondents most concerned about failing to meet customer expectations if they fail to transform.

Rapid experimentation requires the mindset to accept failure and the ability to recover quickly. Organisations agree that iterative, experimental processes are essential to finding the right solutions, with 81% saying they have adopted agile practices. Fewer are confident, however, in their ability to execute decisions quickly (76%) - or to shut down initiatives that aren’t working (60%).

Evolutionary organisations will succeed in the future. Companies that develop the capability to repeatedly reinvent what they do - not just the technology they use to do it - will be most prepared to respond to future disruptive technologies, market ecosystem changes, and societal shifts. When adaptive structures and mindsets are woven into strategies and operating models, organisational value is created and extends beyond that of a single digital transformation initiative.

“Successful transformation requires more than just adopting new technology - it demands a focus on building an organisation’s capability for continual evolution,” says Laurel Ruma, global director of custom content for MIT Technology Review. “Enterprises that develop the ability to repeatedly reinvent themselves will be the ones to succeed in the future.”

“Transformation suggests there’s a beginning and an end. Yet this research shows that organisations must constantly evolve and adapt to changing market dynamics and customer needs,” said Marcelo De Santis, Chief Digital Officer, Thoughtworks.

“For the modern digital business, transformation is a continuous series of ‘experiments’ in pursuit of building an ‘evolutionary mindset’ organically throughout all levels of the organisation - one shift at a time.”

5 FEATURES

That Make AI-Driven Order Management the Ideal Complement to RPA

Robotic Process Automation (RPA) has firmly established its place in today’s business world. However, RPA alone cannot streamline the end-to-end order management process. Because while bots are great for performing rules-based, data-centric and repeatable tasks, there are still many document-based processes awash in inefficiencies that RPA tools simply cannot address – order management being a prime example.

Here are five features that make AI-driven order management the ideal complement to RPA ...

Artificial Intelligence (AI) can seamlessly pick up where RPA leaves off.

01 DATA EXTRACTION & FIRST-TIME RECOGNITION

Managing the variance and complexity of customer orders manually – even if a robust RPA solution is already in place – can be a burden for any business. For starters, it keeps CSRs mired in repetitive, low-value tasks. Fortunately, AI-powered automation is specifically designed to bridge this manual gap. Best-in-class solutions embed intelligent data recognition technology on top of leading OCR engines to automatically extract relevant information from sales orders.

02 AUTO-LEARNING

Another powerful AI technology is a type of machine learning known as auto-learning that allows the system to automatically learn from the corrections of its users. Teaching capabilities are also available when it’s necessary to explicitly train the solution on top customers’ orders to ensure perfect data extraction. But unlike many RPA solutions that accomplish this through dev tools, AI-driven solutions enable teaching to be done directly through the interface.

03 MOBILE CAPABILITIES

Automated order management solutions enable users to perform the critical duties of their job while on the go via an online mobile app. For example, Esker Anywhere™ can be used to place a variety of customer orders, access status updates and links to the carrier’s website or app or even create an inventory report, starting from the items that are supposed to be in stock and instantly match them.

04 ANALYTICS & REPORTING

AI-driven automation solutions seamlessly equip users with intelligent dashboards that display live, visual metrics – making every action smarter and more strategic.

“Esker’s reporting capabilities were the biggest differentiator.

The opportunities for data mining are limitless, as WE CAN TRACK METRICS FOR BASICALLY ANYTHING.”

Supervisor of Customer Service | Global Paint Company

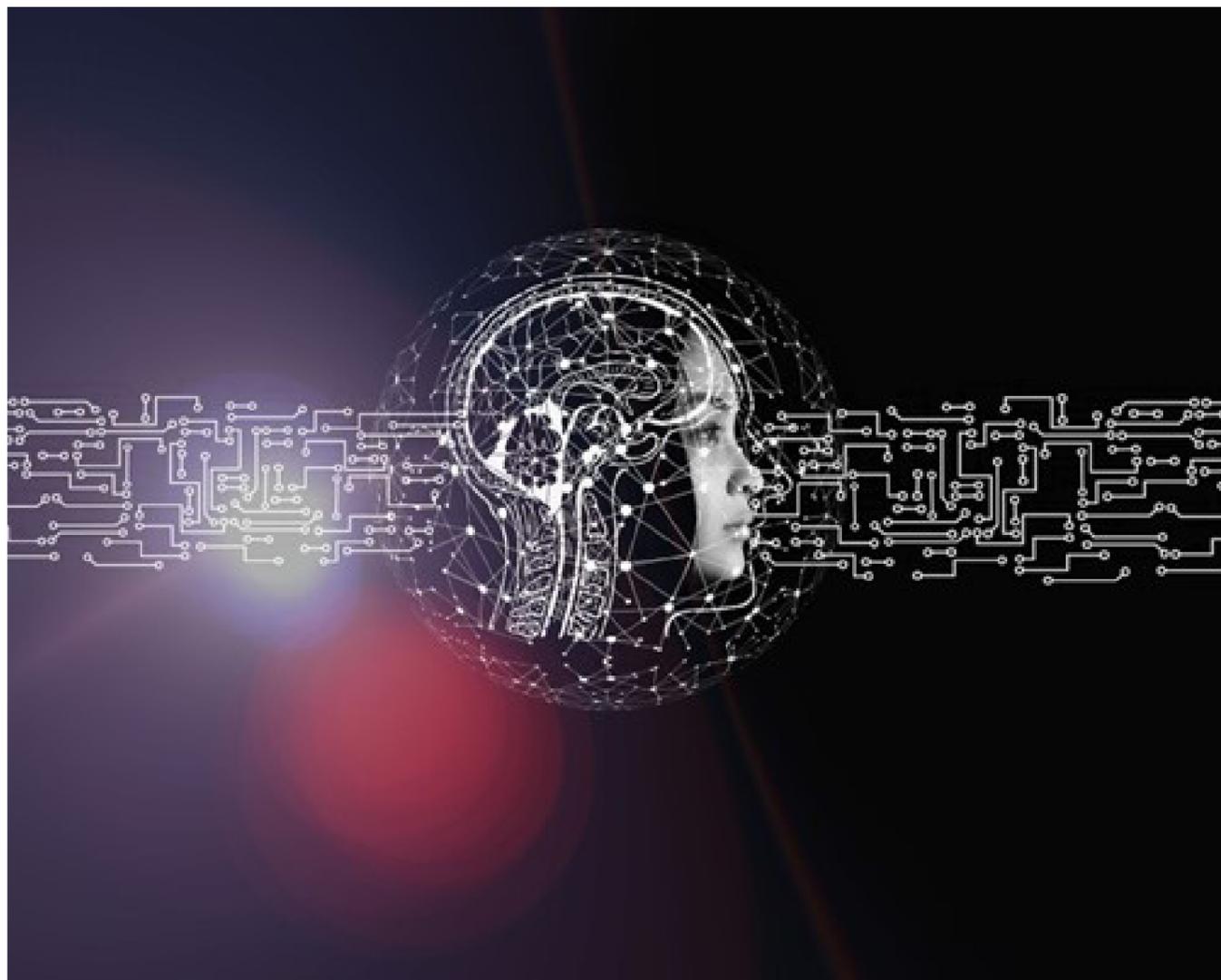
05 EXCEPTION HANDLING

Another significant challenge in a manual order management environment is the absence of collaborative tools – both for inter-department communication and customer interactions. For example, when data exceptions occur (e.g., price mismatches) or approvals are necessary, RPA solutions do not provide an effective path for a rapid resolution. Fortunately, AI-driven solutions do. In the scenarios described above, the order is automatically put into a separate workflow while waiting for feedback from an internal user until the exception can be lifted.



Scan the code to get in touch today

www.esker.com.au



The Potential Impact of AI Solutions on IDP Platforms

By Bruno Zampaglione, TCG Process

As a professional immersed in the ever-evolving landscape of technological advancements, I find myself increasingly fielding customer inquiries regarding the potential impact of new AI solutions, such as ChatGPT & BARD, on IDP platforms.

Well, I think we'll face a huge increase in the automation rates and reduction in processing times of the standard processes and other processes that apparently are impossible to improve will be 100% automated in a very short time.

Let's start from the beginning and explore the transformative power of AI and its implications for IDP platforms.

An AI solution refers to a technology or system that incorporates artificial intelligence (AI) capabilities to address specific problems or tasks. It typically involves the use of machine learning algorithms, deep learning models, natural language processing, or other AI techniques to perform complex tasks, make predictions, or generate insights.

One notable breakthrough in AI technology is ChatGPT, an advanced language model created by OpenAI. With its exceptional natural language processing capabilities and coherent response generation, ChatGPT represents a remarkable milestone in the field of AI.

What's IDP?

An IDP platform, or Intelligent Document Processing platform, is an incredible software application that uses different components to automate the extraction of data from documents.

IDP platforms typically work by first identifying the type of document being processed. Once the type of document is known, the IDP platform will use different engines to extract the relevant data from the document. The extracted data can then be used to automate business processes, such as billing, compliance, and customer service.

As a professional who has worked closely with IDP projects, I've witnessed the transformative impact they have had in various sectors.

Banking & Finance

Within the financial industry, IDP platforms have

revolutionized the processing of invoices and payments. By automating these tasks, businesses can now experience improved cash flow management, reduced manual errors, and enhanced fraud detection capabilities. This not only streamlines financial operations but also safeguards the financial well-being of organizations.

Retail

In the dynamic realm of retail, IDP platforms have become indispensable in automating the processing of customer orders. This seamless integration has yielded multiple benefits, including enhanced customer satisfaction through faster order fulfillment and accurate tracking. By reducing manual intervention and associated errors, IDP platforms also contribute to cost savings and increased operational efficiency for retail businesses.

Healthcare

In the healthcare industry, for instance, IDP platforms have proven invaluable in automating the extraction of data from medical records. This breakthrough has significantly enhanced patient care by enabling doctors and nurses to effortlessly access vital information, leading to more informed decision-making and improved treatment outcomes.

What is the point of convergence between IDP platforms & AI solutions?

In my professional perspective, the synergy between IDP & AI is paramount for achieving optimal process automation outcomes. By harnessing the combined capabilities of these solutions, it becomes possible to automate a wide range of human tasks within a business, effectively eliminating the need for human intervention in the loop (HITL).

This collaborative approach not only reduces processing times but also enhances customer satisfaction through streamlined operations. Using the power of IDP and AI together enables organizations to achieve heightened levels of efficiency, productivity, and overall business success.

By leveraging a robust IDP platform to orchestrate business processes and intelligently determine the

optimal routing of each transaction to be processed by the most suitable AI engine, we can harness the combined power of these solutions to achieve superior outcomes. This seamless integration allows for a synergistic collaboration that enhances overall performance and delivers optimal results.

The scope of document processing goes beyond the mere classification and extraction of various types of documents, including those that are completely unstructured, such as legal documents & contracts. Using knowledge acquired from years of processed documents and training within a learning model, AI solutions can effectively address an old IDP challenge: **Take decisions based on document context.**

Which means that with the correct training model an AI solution can take different decisions (or generate different results) by analyzing the whole document's context in a transaction not only cross-checking extracted data against business rules like IDP platforms generally does.

Conclusion

It is truly fascinating to witness the profound interest and curiosity surrounding the convergence of these cutting-edge technologies and how they may shape the future of IDP. The evolving relationship between AI and IDP holds tremendous promise, and I am excited to explore the potential implications and possibilities that lie ahead for this dynamic intersection.

If your business permits, do not be afraid to consider AI solutions on your processes automation, I believe with right approach using AI & IDP platforms we can have an unbelievable automation rate in some of the most complex business processes!

Bruno Zampaglione is a Process Automation and Information Capture Expert at TCG Process.

Contact TCG Process

Tel: +61 2 9060 3727

Email: info.aus@tcgprocess.com

<https://www.tcgprocess.com/en-en/australia/>

Insurance tech provider takes on TCG Process

Duck Creek Technologies, a solutions provider for the property and casualty (P&C) and general insurance market, has announced an intelligent document processing (IDP) partnership with TCG Process.

The partnership allows IT and business units to model and orchestrate insurance business processes to collect, understand and act on unstructured content for applications such as claims, underwriting, regulatory compliance, onboarding, and digital mailroom, rapidly eliminating data bottlenecks across the enterprise with a low code, no code solution.

Moving IDP beyond its traditional role as a preliminary step in a process, the integration also empowers businesses to meet their digital transformation goals while keeping humans in the loop.

"Our collaboration is driven by a shared commitment to providing exceptional document-driven automation for the insurance market, and we're excited to see the positive impact it will have for both Duck Creek's customers and stakeholders," said Bob Fresneda,

President, TCG Process US Operations.

"Our global team is confident that this partnership will create immense value and we look forward to forging a successful future together for not only insurance companies, but also third-party administrators (TPAs), business process outsourcers (BPOs), and shared service centers (SSCs)."

"We are thrilled to announce a solution partnership that will enhance the intelligent process automation landscape for document ingestion," said Robert Fletcher, Sr. Partner Manager at Duck Creek.

"We will not only amplify our process automation offerings, such as Duck Creek Turnstile, but by combining our solutions for customers, TCG Process provides unparalleled document classification, data extraction and validation exception handling, and cost-efficiency for even the most complex document-driven workflows across the rest of the Duck Creek Suite of products."

The Top 5 Cloud Security Risks of 2023 (so far)

By Bar Kaduri and Jason Silberman, Orca Security

As we approach the middle of 2023, we thought it an appropriate time to reflect on the cloud security risks and threats that we have seen so far this year, as observed by the Orca Cloud Security Platform that continuously scans billions of cloud assets on major cloud service provider platforms. After careful analysis of aggregated scan results from January-May this year, the [Orca Research Pod](#) has identified the top five most common, yet severe, cloud security risks that are ubiquitous in many cloud environments.

In addition to revealing the risks and presenting the data we found, we also provide background information on each risk, as well as [key recommendations](#) on how to avoid these risks from occurring in the first place.

We hope that this research will help organizations understand which areas can provide the greatest improvement in cloud security posture so they know where to focus their efforts.

Executive Summary

The Orca Research Pod found that the five most common as well as severe cloud security risks of 2023 so far are, in order of severity: (1) unpatched exposed web services, (2) sensitive information in Git repositories, (3) unsecure sensitive AWS keys, (4) overprivileged IAM roles, and (5) overprivileged AWS Lambda functions.

Each of these risks were found to be widespread in organizations of all sizes, even in those with a high maturity level in terms of cloud security.

Even though these are not the newest and most talked about issues, they are part of cybersecurity 101 (such as the need to patch vulnerable web services and enforcing policies that adhere to the Principle of Least Privilege (PoLP)), and further highlight what is commonly said in the industry: that we should first focus on the security basics to make the largest improvement in cloud security postures.

It is also important to acknowledge that many security teams are facing a huge backlog in open security alerts while being understaffed. This is hampering their ability to address risks in a timely manner, which is why prioritization of alerts, coupled with guided and automated remediation, are essential to overcome these challenges.

The Orca Research Pod compiled this research by analyzing workload, configuration, and identity data captured from billions of real-world production cloud assets on [Amazon Web Services \(AWS\)](#), [Microsoft Azure](#), [Google Cloud](#), [Kubernetes](#), and serverless functions, scanned by the [Orca Cloud Security Platform](#) from January 1st – May 1st, 2023.

Orca Cloud Security Research Results

Below we list the five most common and critical cloud security risks of 2023 so far, in order of importance:



Finding #1: Patching is lagging on exposed web services

Orca found that 36% of organizations have an [unpatched web service](#) in their cloud environment that is exposed to the Internet and therefore easily accessible by attackers. Unpatched services, with known vulnerabilities and bugs, can be one of the main attack vectors into cloud environments. In fact, the majority of [attack paths](#) that the Orca Security research team detects and analyzes [begin with an exploitation of a known vulnerability](#). The stakes are considerably higher if the service is web-facing, that is, accessible from outside the network.

Malicious actors can relatively easily exploit an unpatched vulnerability to cause service downtime, potential remote code execution, or more. In some cases, unauthorized remote access may also be a possibility.

All software has the potential to have vulnerabilities and bugs, including web services. Software vendors are responsible for discovering and fixing them before they are found and exploited by malicious actors. Software consumers are in turn responsible for immediately applying these fixes, released via updates or patches.



Finding #2: Sensitive information commonly stored in Git repository

Orca discovered that 50% of organizations have at least one [Git repository containing sensitive data](#). Sensitive

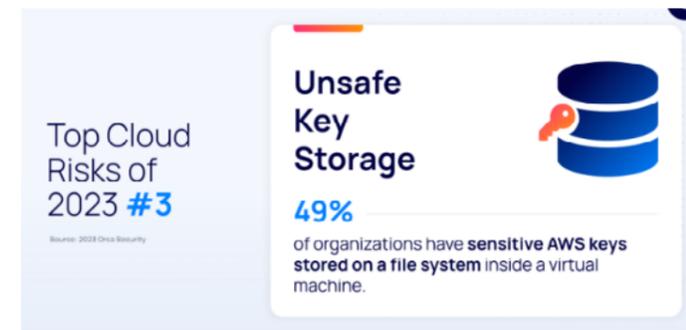


Attack path showing how an unpatched service vulnerability inside an Internet facing VM, combined with sensitive keys, can facilitate lateral movement to a high-privileged IAM role in AWS Lambda.

information such as database passwords, API keys, encryption keys, hash salts, and secrets, can mistakenly get pushed into a Git repository.

In addition to this being contradictory to security best practices, if they are part of the source code of your application, attackers can potentially extract them and compromise your systems.

Any pushed sensitive data must be detected and removed immediately, both from the repository and the history.



Finding #3: Sensitive AWS Keys often stored on file systems

49% of organizations have [sensitive AWS keys stored on a file system](#) inside a virtual machine. Think of AWS keys as literal keys to your system.

Anyone with your key has access to all your resources and can perform any operations that you can, like launch EC2 instances, delete S3 objects, etc. This is why you must always store your keys in a safe location, and never share them with anyone, especially not external parties.

By default, sensitive AWS keys are stored on the file system. If these keys are obtained by a malicious actor, they can use them to access sensitive resources and perform unauthorized operations. It's important to note that sensitive AWS keys are one of the main exploits for malicious lateral movement identified by Orca Security in [attack paths](#).

AWS keys provide indefinite access unless they are manually revoked. However, for many use cases, you don't need long-term access without an expiration date. This is why AWS recommends using temporary credentials (generated using the Security Token Service) instead of AWS keys.

In addition to the access key ID and secret access key, temporary credentials also have a security token that specifies the expiration date of the credentials.



Finding #4: Too many admin users per organization

Orca discovered that 33% of organizations grant [full administrative privileges](#) for more than 10% of Identity and Access Management (IAM) roles in their cloud environment, with 10% of the organizations even granting administrative permissions to more than 40% of their roles. This is way too many.

An IAM role in an AWS account is an identity with specific permissions that dictate what actions the identity can perform and which resources it can access.

Unlike IAM users, IAM roles are not bound to a single person and can be assumed by anyone that is authorized to do so.

There are no long-term or indefinite security credentials associated with a role. Instead, short-term credentials are issued whenever a user assumes a role.

Roles provide a great way to delegate access to users or applications that don't usually need access to your resources.

IAM privileges are an example of how sometimes security is less convenient, but is still the correct choice. While it's much faster, and easier, to grant many privileges to users - rather than restricting permissions and creating the need for more oversight - it's a case of short-term gain and (potentially) larger damage in the long-term.

As a golden rule, it's best to not, except in rare circumstances, define an IAM role with full administrative privileges, since anyone who assumes the role will have the ability to perform any action on any resource in the account. This violates the [Principle of Least Privilege \(PoLP\)](#), greatly increases the attack surface, and increases the risk of full account takeover.

(Continued over)

Finding #5: Majority don't use separated roles for Lambda functions

Orca discovered that 70% of organizations have at least two [Lambda functions that share the same IAM role](#). In addition, almost 86% of all Lambda functions are sharing their IAM role. When it comes to AWS Lambda, AWS recommends creating separate roles for each function, in order to promote the Principle of Least Privilege.

“By using one dedicated IAM role per function, you can control permissions more intentionally. Every Lambda function should have a 1:1 relationship with an IAM role. Even if some functions have the same policy initially, always separate the IAM roles to ensure least privilege policies.” This protects data from unauthorized access, and allows you to adhere to various security and compliance standards.

Key Recommendations

As mentioned, these risks are not new. The fact that they are so widespread, therefore, is preventable. By following the recommendations below, organizations can strengthen their cloud security risk posture and minimize the occurrence of these risks as much as possible:

Adhere to the Principle of Least Privilege – Ensure that administrator privileges are *only* given to those who really need them, and that regular users don't have the power to escalate their own privileges or create new accounts. Regularly [review user policies](#), to ensure that users are not given permissions they don't strictly need. If users [haven't used permissions in 90 days](#), they should ideally be revoked.

Never stop patching – Regardless of how rigorous your security controls are, if you don't regularly patch software, you are at serious risk of compromise. This is

because cyber criminals scan and target networks with known, unpatched vulnerabilities. Whenever possible, systems with known vulnerabilities should be patched. Since it is impossible to patch *all* vulnerabilities, it is important to understand which vulnerabilities enable dangerous [attack paths](#) and make sure those are patched first.

Utilize checklists and CIS benchmarks – To minimize human error, use checklists when creating and configuring cloud assets, entitlements, and resources. Additionally, we recommend implementing policies that follow the best practices of well-known [CIS benchmarks](#).

Perform continuous cloud scanning to identify risks – Continuously scan your cloud environments for these and other risks. You can really only do this effectively and keep pace with the speed at which cloud environments change by adopting a [cloud security platform](#) that has wide visibility across clouds, accounts, and workloads. Ideally, it will empower you to understand the full context of risks and recognize when seemingly unrelated issues can create dangerous attack paths.

Leverage prioritization to avoid alert fatigue – Risk prioritization is a foundational requirement for effective cloud security. Security tools typically generate many alerts. When you consider that security teams—often understaffed and overworked, and working under heavy pressure—are generally monitoring several tools simultaneously, that's a lot to handle. Although it will never be possible to fix all risks, it is important that you [focus on the ones that are most critical](#).

These risks, as well as over 2,000 others, are described in [Orca's Cloud Risk Encyclopedia](#), a free and public resource featuring cloud security and compliance risks.

Originally published [here](#)

Busting a CDR myth - why we need to talk about migration

By Stuart Low

In today's digital landscape, businesses find themselves needing to migrate their data to new systems for a myriad of reasons. Whether it is to save costs or to improve collaboration or to meet consumer data requirements, the process of migration must be thought out to ensure continuity of service and data security.

In February we found out ING's planned swap-out of its CDR solution could [place it in breach of its obligations](#), indeed the ACCC has since clarified it [expects data holders to avoid disrupting or breaking consents](#). Cutover to the new system would invalidate potentially thousands of customers' existing consents to share data and put the burden of reintegration costs on data recipients.

ING customers signed up to CDR were told their current data sharing arrangements would end on 21 February and that they won't be able to view data sharing arrangements set up prior to the platform upgrade in ING online banking. To re-establish data sharing arrangements, customers will need to complete the data sharing consent process in each provider's app. Something that could mean hard-won ADR customers are lost.

The industry is up in arms. But the thing is, data holders need to consider migration options when they sign on to any project as it was only a matter of time before a data holder wanted out of its existing vendor-supplied or in-house developed solution and needed to migrate its consent data as a result. So, why is this conversation only happening now?

Importantly, solutions to this problem do in fact exist. When a data holder is signing on for a project, whether it's a bank, energy company or (soon) telcos and non-bank lenders, they need to have the migration conversation upfront so they're not trapped by a vendor or their own in-house solution, whilst still ensuring continuity of service.

There is an urgent need to dispel the sentiment that data holders are locked in with one vendor because organisations are told it's too hard or even impossible to migrate. Propagating this idea will only hinder the progress of the CDR and stifle innovation.

So, what are the solutions?

A CDR infrastructure migration can go one of two ways. A “lift and shift”, or a concurrent transition.

A lift and shift involves the migration of consent metadata and data recipient registrations from the old system format to the new system format. While this requires concurrent metadata understanding of both systems this method allows for a “big bang” migration strategy that is completely transparent to participants.

In this way participants are essentially unaware of changes to the underlying systems. Once the migration is completed the new system operators can proceed with rotating cryptography elements to become exclusively authoritative for the holder in question.



The concurrent transition method involves placing the new system in front of the old while performing a conditional pass through where required. By using this mechanism implementers can place the old system in sustainment, essentially “waiting out” the existing arrangements while establishing the new arrangements in the new system.

Over time the new system becomes the exclusive owner of all arrangements with a final historical arrangement migration activity conducted. This method facilitates a gradual transition and rollback checkpoint separate from the go live checkpoint.

What should data holders be looking for in a CDR solution?

It's important to remember that the CDR is a highly complex ecosystem that requires multiple parties to work together for it to function. It won't work if we're only thinking about ourselves, and how to ‘lock out’ competitors.

When starting on your CDR journey, data holders should be looking for:

- High-level contingency plans for the future so you're not trapped with a solution that's not fit for purpose or leaves you unable to innovate or take advantage of new CDR capabilities.

- A vendor that positively contributes to the growth and success of the CDR. They should always have your back whilst still being willing to work with the wider ecosystem to overcome challenges.

- A vendor that understands both sides of CDR — the Data Recipient and Data Holder domains — so they can provide informed and accurate guidance.

- A solution that goes beyond primary functionality from Day 1. The ability to quickly analyse consents to support a migration or initiate customer contact are examples of this. Often these are viewed as secondary considerations and unlikely to fall within an MVP, these features can quickly become critical.

Stuart Low is Founder and CEO of Biza.io, developer of a Software-as-a-Service solution to meet the complex and rapidly changing Consumer Data Right specification.

Unleashing Human Potential in the New Zealand Workplace.

AP Automation
Health Records
Contract Management
HR Automation
Web Forms & Document Workflow
Document Archival



upsol.co.nz

 UpSol



Kodak Info Input Solution

Data Capture and Automation for Everyone, Anywhere

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



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.

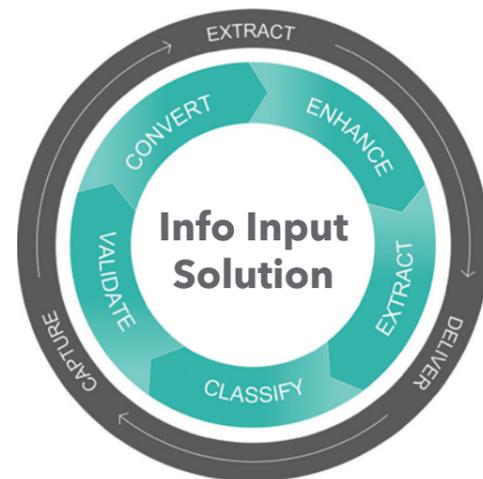
These locations will also have made investments in enterprise business applications requiring integration. Having downstream automation capabilities without automated capture capabilities means you are only automating half a process. In a mobile world, work happens everywhere. This is where web-based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

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.

Want to learn more?

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



Kodak Info Input Solution integrates with leading ECM, workflow solutions

"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



COMPANIES WITH ANSWERS AND SOLUTIONS FOR YOUR DIGITAL TRANSFORMATION INITIATIVES



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 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 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



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



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 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 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 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 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



Kodak Alaris is a leading provider of information capture solutions that simplify business processes. Digital Transformation is the need of the hour for many organisations, and it starts with information and data capture. We exist to help the world make sense of information with smart, connected solutions powered by decades of image science innovation. Alaris drives automation through every business process dependent on document and data capture so that you can get the right information to the right place at the right time. Our award-winning range of scanners, software and services are available worldwide, and through our network of channel partners.

www.alarisworld.com/en-au | Angelo.Krstevski@kodakalaris.com | 0419 559960



Information Management and Governance (IMG) specialist, iCognition Pty Ltd, helps our clients to maximise the value of their information assets, while minimising cost and risk. We use an integrated Information Management and Governance approach that combines the disciplines of data, records, and information management to value, manage, control and harness information across the enterprise. iCognition's Electronic Document and Records Management System-as-a-Service (EDRMSaaS) represents 20 years of iCognition experience. It is a proven, secure and trusted Software-as-a-Service offering for Content Manager. It can also include iCognition's award-winning RM Workspace for secure web-based end-user access and collaboration, Office365RMBot for fast and easy information governance of Office 365 information, RM Workflow to deliver easy-to-use Content Manager workflows, and RM Public View for publishing and sharing to non-Content Manager users.

www.icognition.com.au | info@icognition.com.au | 1300 00 4264



WyldLynx was originally established to provide content services for small to large organisations, and has quickly gained a reputation for being an innovative and service driven organisation with great people. Many small to large information management solutions have now been delivered by WyldLynx to a range of Queensland government organisations and councils, with many of the products coming from the MicroFocus Secure Content Management suite. WyldLynx will never rest on its laurels, however, and is always on the cutting edge with new technology and process innovations that can deliver better business solutions for our customers. WyldLynx has developed expertise in business products from multiple vendors, and is proud to be able to bring these products to our clients. We are also constantly developing our own software products in-house, with many most being specifically designed to enhance other vendor's products, or fill important gaps to make our client's time more efficient.

wyldlynx.com.au | contact@wyldlynx.com.au | 1300 WyldLynx



UpSol are experts in Digital Transformation and Business Process Re-engineering with strong domain expertise in Data Capture, Document Management, Organisational Workflow, Electronic Forms, Data Integration

upsol.co.nz | sales@upsol.co.nz | 0800 003 115

CyberCision adds real-time threat protection

Australian cybersecurity and network management software company FirstWave Cloud Technology Limited (FirstWave) has released a significant new upgrade to its cybersecurity-as-a-service platform CyberCision. The latest release includes a new standalone deployment system for Government platform installations and incorporates technology acquired as part of FirstWave's purchase of Opmantek Limited in early 2022.

Among other features, the release builds on CyberCision's Advanced Detection and Response (ADR) technology with a new layer of enterprise-level intelligence feeds sourced from Cisco Talos Intelligence Group, one of the largest commercial threat intelligence providers in the world.

CyberCision's ADR provides businesses with continuous realtime monitoring of email security services and automated threat visibility, detection and alerts in response to attacks and incidents. The new release also adds significant new security detectors and data classification features while enhancing the platform's "trace and threat hunting" capability to give CyberCision users deeper security knowledge and insight.

FirstWave Chief Executive Officer Danny Maher said, "CyberCision is the world's only open security management platform designed specifically to deliver enterprise-grade security to businesses of all sizes. With CyberCision service providers can build as-a-service cybersecurity packages of enterprise-grade, including a range of management and operational services such as multi-tenanting, billing, and provisioning that enable them to streamline the sales and delivery process at a minimal cost."

www.firstwavecloud.com/cybercision

Data analysis for SharePoint/OneDrive

The developer of the Aparavi Data Intelligence and Automation Platform has launched new connectors to bring these data management tools directly to Microsoft SharePoint Server and OneDrive

The Aparavi Platform delivers a deep dive into data and metadata to identify and provide insight into redundant files, aging files, files with sensitive information, and more. Aparavi easily scans and finds unstructured data by hundreds of criteria and can automate chores such as classifying, deleting, and moving data to offsite archive to reduce storage footprints.

Key to Aparavi's value for SharePoint and OneDrive is its ability to assess files and locate redundant, obsolete, and trivial (ROT) data - typically 25-80 percent of business files - to free up storage. Aparavi can also proactively identify files with regulated personal information such as SSNs or financial information, and confidential business

data, that might be vulnerable to data breaches and cyberattacks.

By performing "data hygiene" in SharePoint and OneDrive, and eliminating unnecessary files, Aparavi also helps groom data for better and faster results in data analytics and machine learning.

Aparavi has also added SharePoint Cloud to its compatible cloud targets, enabling organisations to automatically copy or move data to SharePoint Cloud for migration initiatives to streamline operations, gain elastic scaling, and maintain data access while containing the costs of cloud capacity.

The Aparavi platform can clean data and archive it to off-site targets, such as public cloud or object storage-compatible targets, reducing on-premises storage footprint by up to 40 percent and making data less vulnerable. Its advanced search works across all systems to provide insight into data and metadata by location, owner, content, events, creation, last access, extension type, or modification date, and eliminate ROT data.

<https://www.aparavi.com/>

Atakama partners with Panzura

A new partnership combines multifactor encryption from Atakama with the Panzura File Management System to offer a hybrid multi-cloud data management and protection solution. The integration between Atakama's [multifactor encryption solution](#) and [Panzura's CloudFS, Data Services \(PDS\)](#) seamlessly enforces a data-centric security model.

Atakama's [multifactor encryption](#) solution eliminates centralized points of attack and failure and provides data protection at the granular object level to fortify a data-centric security model. This dedicated security layer is policy based and achieved in accordance with each organization's specific use case.

With a zero-trust posture, every file access request is evaluated individually, in alignment with a complete data management lifecycle. Atakama removes the conventional trade-off between data security and accessibility through simplified administrative and end-user experience toward an air-tight data-centric security model.

"Even with strong access control policies, stringent audit practices, and the best of intentions, the threat of data exfiltration is significant," said Don Foster, Global Head of Sales Engineering, at Panzura.

"By pairing our industry-leading file management system and Atakama's pioneering multifactor encryption, we have created a compelling end-to-end data management and protection solution that puts companies back in control of their mission-critical data."

Panzura's [CloudFS](#) is a global file system that dynamically coordinates file storage location, edit and access rights, data management, and more.

<https://www.atakama.com/> <http://panzura.com/>

AvePoint Advances SaaS Management

AvePoint has unveiled updates to the AvePoint Confidence Platform that adds new SaaS management capabilities. Today, the AvePoint Confidence Platform supports the management and governance of Microsoft 365, Power Platform, and other Microsoft objects like Azure Active Directory and mail enabled distribution lists in the following ways:

Improved Operational Efficiency: Gain a comprehensive view across SaaS applications, automate repetitive processes with event or manual workflow triggers, quickly update licenses and entitlements to give users the right access and automate service requests with dynamic profiles.

Increased Visibility: Capture context for collaboration workspaces and objects to understand why and how they are being used, execute object or user-based security searches for insight into SharePoint, OneDrive, Groups and Teams permissions and aggregate highly exposed content with sensitive information types to present a heat map of at-risk data across Microsoft 365.

Proactive Security and Compliance: Create lifecycle management to empower users while ensuring they stay within organizational policies, review security concerns and quickly update access and security controls within Microsoft 365 objects, and identify orphaned objects in Microsoft 365 or Power Platform to rapidly take corrective action.

“Our customers need centralized visibility and control over their SaaS applications in order to mitigate risk and save themselves time,” said John Peluso, Chief Product Officer, AvePoint. “With multi-tenant views and policies that extend across cloud applications, we make it easy for IT teams to not only take stock of all tools they have in place but also to secure and optimize their use to power success in the digital workplace.”

<https://www.avepoint.com/solutions/saas-management>

Cognizant launches Neuro AI Platform

Cognizant has announced a new, enterprise-wide platform, Neuro AI, designed to provide enterprises with a comprehensive approach to accelerate the adoption of generative AI technology and harness its business value in a flexible, secure, scalable and responsible way.

The platform leverages Cognizant’s consulting, advisory, ecosystem partnership, digital studios, solutioning, and delivery capabilities, in conjunction with industry expertise, to help clients transition seamlessly into the era of generative AI.

The Cognizant Neuro AI platform will guide firms on this journey, from identifying company specific-use

cases and operationalising AI, to data engineering and continuous improvement. The platform enables AI and software engineering teams to build flexible, reusable, safe and secure solutions, and design conversational and generative user experiences, embedding AI models to create fully functioning apps – all supported across multi-platform, multi-cloud ecosystems.

Cognizant Neuro AI includes a library of reusable generative AI models and agents, development tooling and control components including API and access management, versioning and auditing. The platform is designed to provide meaningful business benefits for clients, including:

- Discovering new business innovation vectors,
- Creating pathways to differentiated customer and employee experiences,
- The ability to reimagine and digitise business processes,
- Reliable governance, visibility, control and compliance,
- Faster access to a holistic library of curated solutions, and
- Improved time to market at enterprise scale.

www.cognizant.com

One GIS to Bind Them All

To support users in the intelligence and national security community, Esri has released ArcGIS AllSource. The new desktop software turns raw data into decision support by combining data from multiple sources. Analysts can leverage built-in link analysis, 2D and 3D maps, timelines, imagery exploitation, graphs, and video to uncover patterns, trends, and relationships in data to inform decision-making.

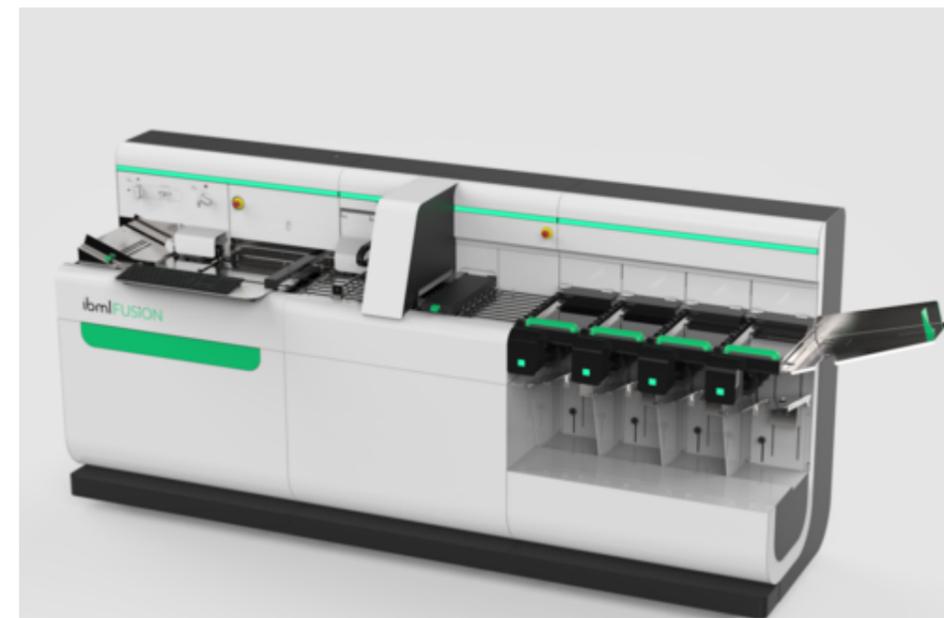
Globally, intelligence analysts and auditors in national security and public safety organizations must use multiple data sources for their analyses. Increasingly, organizations are turning to geographic information system (GIS) technology to provide the context of location for their data.

This geographic approach gives professionals the understanding they need in order to do everything from protecting assets, people, and property to addressing cyber threats and more.

ArcGIS AllSource is designed for intelligence professionals working in civilian intelligence agencies, commercial organizations, law enforcement, and the military. By integrating with existing organizational ArcGIS infrastructure, AllSource saves analysts time and reduces spending. The software is compliant with industry standards, allowing professionals to share and leverage data easily while working with other systems and applications.

<https://www.esri.com/en-us/arcgis/products/arcgis-allsource/overview>

ibml launches High Volume Scanner



ibml has announced its new FUSION HD High Volume Document Scanner designed to meet the US Federal Agencies Digital Guidelines Initiative (FADGI) 3 star imaging quality standards. The FUSION HD can quickly digitize high quality documents at scale so they can be easily archived, shared and utilized while still meeting these high standards.

“Our new 600 DPI System enables our customers to achieve high productivity while simultaneously having the intelligence to classify and extract data needed to drive immediate business decisions, and also meeting the most rigid Image Quality standards for archival storage,” said Pete Rudak, Chief Technology Officer for ibml.

“This enables complete digital transformations across any document types, and gives our customers peace of mind knowing that the FUSION will meet the most rigid archival Image Quality requirements, both now and into the future.”

Some new FUSION HD features include:

- 122ppm (industry’s fastest throughput) at 600DPI output enabling digitization at scale for all applications;
- New 400DPI and 600DPI output for high quality image output applications for complete digital transformation including specialized applications like fingerprint cards, photographs and other high value records;
- FADGI 3 Star standards met at 200DPI, 300DPI and 400DPI;
- High quality lossless PNG output for demanding imaging applications;
- ICC Color profile matching to meet stringent quality standards.

Integrated ibml Capture Suite (iCS) software offers FADGI Verification module designed to allow operators to have an integrated experience between

iCS and ISA’s Golden Thread software.

Operators can verify the image quality as often as needed from ibml scanners while maintaining an audit trail.

With this module, operators have an integrated single user experience in iCS allowing them to be productive while consuming the least amount of time in ensuring image quality consistency.

<https://www.ibml.com/>

Workflow in M365

Nintex has announced a transition plan for Nintex Workflow for Office 365 customers following Microsoft’s decision to retire the existing Microsoft SharePoint 2013 workflow engine in Microsoft Office 365.

Microsoft announced that SharePoint 2013 workflows will be turned off for new tenants as of 1 April 2024, and will be removed from existing tenants and fully retired as of 1 April 2026.

Nintex announced the Nintex Upgrade Program in September 2022 to provide a transition path to Nintex Automation Cloud, Nintex’s cloud-hosted workflow solution.

Holly Anderson, Nintex VP of Product Marketing, said that “while today’s news shouldn’t come as a surprise to customers, it is important for organisations to thoughtfully plan their migration.”

The Nintex Upgrade Program is designed to make the transition as simple as possible by providing migration tools, services, and dedicated support from Nintex process experts.

For more information about the program and to tailor a solution that ensures continuity for your processes, customers can visit the Nintex Upgrade Center.

Enterprise Recon 2.8 for Data Discovery

Ground Labs, a provider of critical data discovery solutions, has announced the general availability of Enterprise Recon 2.8, the latest version of its flagship solution. This release enhances support for additional high-scale, high-volume environments on more Microsoft platforms, including Teams and OneNote, and Salesforce Government Cloud.

The latest features extend the number of platforms Enterprise Recon supports for sensitive data scanning of any file type stored on endpoints, servers and cloud environments. As global regulations proliferate and become increasingly stringent, Ground Labs enables enterprises to meet these requirements and avoid heavy financial penalties for non-compliance.

Powered by the company's own GLASS Technology, Enterprise Recon allows customers to define their own custom data types while maintaining their systems' performance.

Other key features and benefits of Enterprise Recon 2.8 include the following:

New Global Data Types: The ability to scan and remediate locations that store unsecured Singapore telephone numbers and next-generation US passport numbers, supporting compliance with the PDPA, CCPA and other related data privacy regulations.

Data Classification: Support for the newest Microsoft Information Protection SDK version allows developers to classify and label sensitive content identified in local storage and Windows share locations.

Reducing False Positives: Other enhancements to existing capabilities supporting compressed files, Oracle databases and features to further reduce false positives in larger environments have also been added.

Enterprise Recon enables organizations to quickly discover, manage and remediate critical categories of data to meet privacy and compliance obligations. Enterprise Recon helps organizations comply with a wide range of international data protection regulations including GDPR, PCI DSS, CCPA, CPRA, HIPAA, PDPA, PIPEDA and CDPA.

As a result of customers' suggestions, in this release, Ground Labs will deliver early-stage functionality around Cloudera distribution for Apache Hive.

<http://www.groundlabs.com/>

Armis adds Cybersecurity insight

Armis has enhanced features of its Cybersecurity Asset Attack Surface Management (CAASM) Solution giving security teams' abilities to overcome asset visibility and exposure challenges. Security teams will be able to improve their overall security position by ensuring security controls, security posture, and asset exposure are understood and remediated.

The proliferation of assets across organisations has increased the need for better visibility but unfortunately, management of those assets is usually performed using multiple IT and security solutions. The "great silo-isation" of legacy tools means a fragmented landscape, with neither complete visibility nor a single source of trusted information.

And that means IT and security teams struggle to understand what assets they truly have and therefore the level of exposure and risk —and to ensure policies are properly enforced, risk is managed, and assets are protected.

Armis has enhanced the capabilities of its platform so that organisations can identify gaps in security controls, prepare compliance reporting and audits, identify technical debt and enhance their CMDBs. Customers have access to:

Accurate Inventory - Armis unified asset inventory enables data to be consolidated from multiple sources to reflect real life environments,

asset to asset. It also allows accurate classification of the different assets, so it can easily differentiate between servers, personal computers, mobiles, and others.

Deep Asset Context - Each asset has advanced information that is pulled from different tools, including the user of the asset, its business applications, any software applications running on it, dependency mapping, and much more.

Endless Integrations - Hundreds of integrations with existing tools - EDRs, vulnerability scanners, Cloud Services, CMDBs, MDMs, Identity Providers, and many more. Specifically, our partnership with ServiceNow allows rapid connection to the biggest CMDB, with capabilities of pulling and pushing data between the platforms.

Advanced Trending and Benchmarking Capabilities - The platform now allows organisations to set their own security standards and easily see over time trends, to make sure project goals are met.

Out of the box reporting and dashboarding - Pre-built reports and dashboards designed for the most critical needs can now be set in seconds, used for executive reporting as well as everyday consumption.

<https://www.armis.com/solutions/cybersecurity-asset-management/>

Data Governance with Deep Analytics

Komprise has announced new governance and self-service capabilities that simplify departmental use of Deep Analytics, a query-based way to find and tag file and object data across hybrid cloud storage silos.

IT organizations need to maintain data governance and data security while also making it easier for users to find, use and manage data. Often, these goals are in conflict and require significant IT overhead.

The latest Komprise Intelligent Data Management release minimizes administrative effort and improves unstructured data governance with new capabilities:

Share-Based Access for Groups: A recent Informatica survey revealed that data governance is the top priority among chief data officers and that 68% of data leaders will increase data management investments in 2023. But managing access control while enabling self-service unstructured data management for users often requires IT to spend considerable time provisioning each user's role-based file and object storage access.

Komprise simplifies this task by giving administrators the ability to assign group access to shares using Active Directory which automatically provisions data management access only to users in those groups.

Directory Explorer: A new Directory Explorer gives authorized line-of-business teams and departmental researchers the ability to augment the global search capabilities of Deep Analytics with a familiar browser interface. This means users can drill down into individual directories.

Users now have multiple ways to find what they need: either by searching for it using queries on metadata and tags through Deep Analytics or if they know exactly where the data is, using the Directory Explorer.

Exclusion Query Filters: The Global File Index search capabilities of Komprise Deep Analytics now includes the ability to filter data using exclusions (e.g., "all data except .log files" or "all data except in .dat directories") and then use these queries to create data management policies. This makes it easy to specify data management policies in situations where outliers can prevent data movement.

"Komprise is on a mission to change how enterprises manage unstructured data to deliver maximum cost savings and value," says Kumar Goswami, Komprise co-founder and CEO.

"Increasingly, line of business and research teams rely upon data that has been historically locked away in disparate storage systems to run analytics, AI and ML. Our latest release makes it dramatically easier for teams to find and manage their own data, while simplifying governance for IT."

<https://www.komprise.com/category/blog/whats-new/>

Newgen ECM in Azure & AWS

Newgen's Contextual Content Services Platform, OmniDocs, is now available in both the Microsoft Azure and AWS Marketplace.

The OmniDocs ECM platform enables the end-to-end management of enterprise content, from origination to disposition. The platform connects content and processes in a contextually accurate manner and enables organizations to go digital.

It comes integrated with smart tools to capture content from multiple sources, manage it in a secure centralized repository, and make information easily accessible for users. It offers flexibility to access or deliver content via mobile and the cloud, creating a highly connected and digital workplace.

Two other Newgen products - NewgenONE Digital Transformation Platform, and Loan Origination Software (LOS) / Digital Lending - are also available for purchase in the Amazon Web Services (AWS) Marketplace.

"By collaborating with Microsoft, we will be able to enhance our sales efforts and offer a top-notch solution to our customers that leverages the power of Azure's cloud-based infrastructure," said Rajvinder Singh Kohli, SVP at Newgen Software. "Our platform can be leveraged by users to create a boundaryless workplace with anytime-anywhere content access and document management."

To find Newgen's products in AWS Marketplace, visit <https://aws.amazon.com/marketplace/seller-profile?id=8598f4f2-d02b-477d-ab00-915261224d10> www.newgensoft.com

MSAB enhances forensic capabilities

The latest release of MSAB's flagship product, XRY, comes with the launch of XRY Pro, an advanced solution for locked and encrypted devices.

This new tool has cutting-edge level access capabilities, allowing forensic investigators to get into some of the most challenging and secure devices. XRY's extraction and decoding capabilities now include over 44,200 devices and 4,360 app versions.

Additionally, the new release includes an improved version of the companies' forensic analysis tool, XAMN. With case review tracking, Detego integration, and upgraded reporting capacities, XAMN is now an even more powerful solution to discover, analyze and share critical digital evidence faster and with unparalleled ease of use.

Other notable improvements were brought to XEC, MSAB's management tool, allowing customers to follow up and report their operations more productively and efficiently.

<https://www.msab.com/>

Ontotext metadata management & tagging

More than just an end-user UI for establishing a set of documents that represent a business' own version of the Ground Truth for tagging, Ontotext Metadata Studio 3.2 makes it easy for users to quickly determine whether a use case could be automated or not across any third-party text mining service.

It also simplifies orchestrating complex text analysis across various third-party services and evaluates their quality against internal benchmarks or against one another.

With version 3.2, Ontotext Metadata Studio enables non-technical end users to create, evaluate, and improve the quality of their text analytics service by tagging and linking against their own business domain model.

With extensive explainability and control features, users who are not proficient in text analytics techniques can understand the causal relationships between the underlying dataset, the specific text analytics service configuration, and the final output.

This enhancement enables efficient user intervention, making the human truly in the loop and completely in control of the whole extraction process.

Ontotext Metadata Studio is domain neutral and applicable for various domains and use cases, as the application is dependent on the underlying domain model and content to be processed.

<https://www.ontotext.com/products/ontotext-metadata-studio/>

GPT-4 Document Automation

Microsoft company Nuance Communications has announced Dragon Ambient eXperience (DAX) Express, a clinical documentation application that combines conversational and ambient AI with OpenAI's GPT-4.

Using a combination of conversational, ambient, and generative AI, DAX Express automatically and securely creates draft clinical notes in seconds for immediate clinical review and completion after each patient visit in the exam room or via telehealth patient conversations.

Dragon Medical One, DAX, and DAX Express are tightly integrated into the electronic medical record, beginning from pre-visit through post-encounter.

DAX Express will be included for users of DAX and available as an addition to Dragon Medical One.

To be added to the DAX Express interest list visit <https://www.nuance.com/healthcare/campaign/learn-more/express.html>.

ProcessMaker adds AI and Enhanced Functionality

ProcessMaker, a provider of low-code business process automation software, has announced new enhancements including Artificial Intelligence (AI), a decision engine, process templates, dependent select lists, modeler usability improvements, dynamic menu enhancements and autosave.

The decision engine implements intelligent decision tables as an independent asset to automate complex business rules without coding. Decision tables will significantly reduce the time needed to create or update decisions automated within a process.

ProcessMaker AI introduces new global search functionality that allows users to search their requests, tasks, and processes with natural language. Incorporating artificial intelligence optimizes workflows and empowers users to make informed decisions quickly.

Predefined process templates will provide a "create from template" feature for faster and easier workflow automation, which allows users to select from a list of available templates to use as a base when creating a new process. This feature is designed to expedite the development of new processes by allowing users to curate their list of developed processes as a starting point.

Process designers can also save their processes as templates to share across their organization. At the same time, autosave saves process models, screens, and scripts in a draft state, eliminating the need to save work manually.

Dependent select lists support no-code collections as a data source. They will allow for filtering based on other fields on the screen, providing no-code-dependent dropdowns for screen designers. The modeler usability improvements include extended keyboard shortcuts and enhanced copy-and-paste functionality.

www.processmaker.com

Reveille Agentless Monitoring Solutions

Reveille Software has announced new Hyland RPA and Kofax RPA support. The new Reveille solutions provide agentless management and monitoring capabilities to ensure the continued health and productivity of the Hyland RPA and Kofax RPA platforms.

This includes managing robots at scale, measuring platform operating performance, and triggering automatic recovery actions - enabling Hyland and Kofax users to understand RPA service levels through a single comprehensive dashboard view.

When using Hyland or Kofax platforms, most organizations need several third-party providers -

each using silo-native product management tools - to achieve the same productivity management and monitoring capabilities of a single Reveille RPA solution.

Reveille's automated RPA functionality allows organizations using Hyland RPA and Kofax RPA to simplify their platform's management by:

- Eliminating the manual observation of RPA platform health with active service level management.
- Automating recovery actions for RPA component errors and robot execution bottlenecks.
- Verifying target application availability and minimizing error recovery logic in robots.

Reveille's single RPA content management dashboard goes beyond product-specific dashboards by displaying suspicious administration transactions and ensuring RPA target applications are available and responsive before robot execution.

In addition, the new solution delivers direct severity-based event integration with SIEMs (Splunk, Azure Sentinel), incident management (ServiceNow), notification (PagerDuty), AIOps (Big Panda), and collaboration tools such as Slack and Microsoft Teams.

<https://www.reveillesoftware.com/>

IBM embeds Watson AI into SAP Solutions

SAP SE and IBM have announced that IBM Watson technology will be embedded into SAP solutions. SAP will use IBM Watson capabilities to power its digital assistant in SAP Start, which provides a unified entry point for cloud solutions from SAP.

With SAP Start, users can search for, launch and interactively engage with apps provided in cloud solutions from SAP and SAP S/4HANA Cloud.

New AI capabilities in SAP Start will be designed to help users boost productivity with both natural language capabilities and predictive insights using IBM Watson AI solutions built on IBM's trust and transparency and data privacy principles.

New digital assistant capabilities in SAP Start will be extended across SAP solutions to help answer diverse questions for managers and employees. By automating and speeding up common tasks, the capabilities are designed to help unlock employee productivity to focus on more strategic work.

SAP Start will allow customers to benefit from intelligence at the point of decision-making with the ability to use AI and machine learning to extract information from a variety of data sources and answer user questions across lines of business.

In addition to natively embedding IBM Watson AI capabilities into SAP solutions, SAP and IBM are collaborating on generative AI and large language models aimed to deliver consistent continuous learning and automation based on SAP's critical application suite.

Appian AI for Process Automation

Appian has announced the release of the latest version of the Appian Platform for process automation. The new release introduces AI Skill Designer, a low-code way to build, train, and deploy custom machine learning (ML) models. The release also features enhancements in automation and total experience, plus further-streamlined data management via the Appian [Data Fabric](#).

Appian AI Skill Designer enables developers at all levels to easily operationalize AI and automate repetitive tasks, freeing up their workforce and eliminating the risk of human error in data classification and extraction. The low-code design allows developers to quickly incorporate AI to optimize business functions while leveraging the Appian Platform's native AI/ML services to provide an integration of AI capabilities automatically.

The Appian Platform provides three out-of-the-box native AI Skills for content processing: document classification, email classification and document extraction.

This new release elevates total experience across all users with new features for Portals, Sites, and interfaces that make development faster and easier. New features include:

- Expanded page navigation on Sites and Portals. You can now add up to 10 pages to a Site or Portal, giving the flexibility to provide a robust and engaging experience to users. As more pages are added, the navigation is optimized for a simplified view.
- Customize Portals domains. Now you can configure your Portals with a custom domain to match existing web addresses.
- Build Portals for healthcare with HITRUST certification. Portals are now included under the Appian Platform's HITRUST certification and can be used to capture protected health information at industry standard.
- Appian Data Fabric stitches together data from any system into a single virtual data model, while keeping data where it is. This release includes Data Fabric enhancements to reduce the time and effort needed to build powerful applications, including:
 - Capture and display business events. Data and how users interact with it is the heart of the enterprise. Record events enable tracking that identifies who took action on a record and when. As events are captured, they are displayed in the event history list component to generate a timeline and snapshot of business operations.
 - Simplified record action security. This release wraps up Appian data security features with the introduction of codeless record action security. Now, you can use familiar low-code security rules to determine who can see your actions and when.

<https://appian.com/products/platform/overview.html/>

Unlocking the Future of e-Signatures with GPT-4

Sydney-based developer DoxAI has announced the integration of OpenAI's GPT-4 through Microsoft Azure OpenAI Service into its e-signature AI solution.

The company claims this collaboration is set to revolutionise the way users comprehend complex and lengthy documents, enabling them to ask specific questions and receive clear answers before digitally signing or witnessing documents.

Some of the key benefits promised by DoxAI's e-signature AI solution include:

- Improved document comprehension through GPT-4 integration, allowing users to ask specific questions and receive clear, concise answers before making crucial decisions.
- Streamlined digital transactions, making the process more accessible and user-friendly across a wide range of industries.
- Secure and seamless integration with Microsoft Azure Cloud Services, ensuring data protection and privacy for clients.
- Enhanced scalability and adaptability, with the potential to expand AI-driven solutions across various applications and industries through the DoxAI Virtual Assistant.

DoxAI offers a wide range of services and products, including e-Signature e-witnessing, Redact AI, Categorise AI, Extract AI, Data Exchange, Asset Verification and more.

Giuseppe Porcelli, CEO and Founder of Lakeba and Chairman of DoxAI said, "The integration of GPT-4, OpenAI's most advanced AI language model, through Microsoft's Azure OpenAI Service, will empower DoxAI's e-signature AI to transform the user experience. This powerful natural language technology can be helpful for tasks including content creation, conversation, document search and analysis."

www.doxai.co

Speech drives process with SnapGPT

SnapLogic has announced the release of SnapGPT, which leverages AI to quickly integrate and automate business processes using natural language prompts.

Business users simply specify their integration requirements in natural language and SnapGPT does the rest by creating all the necessary processing flows, expressions, or scripts needed to complete the task faster and more accurately than ever before.

"SnapLogic is making huge strides by incorporating AI to better serve our customers' application and data integration workflows," said Gaurav Dhillon,

CEO at SnapLogic. "Our launch of Iris a few years ago was an industry-first advancement that applied machine learning to enterprise integration – dramatically changing the economics of cloud, analytics, and digital transformation initiatives.

"SnapGPT is the next evolution, using AI to forever change the way integration is done and how businesses get the maximum benefits out of their enterprise automation. SnapLogic is dedicated to making it easy and intuitive for customers to remove complexities and be able to work better, faster, and smarter."

SnapGPT will deliver a specialised LLM (Large Language Model) trained against petabytes of integration and automation metadata, accumulated from over six years of usage.

With SnapGPT, IT and business users will be able to automate and integrate data flows and build integration pipelines with ease.

For example, a "Quote to Cash" product owner could specify their business intent in natural language to automatically create an invoice in NetSuite when an opportunity is marked "Closed Won" in Salesforce.com. SnapGPT can translate the intent into a complete pipeline with suggested filters, mapping, and transformation required to complete the task.

It's clear that generative AI will play a critical role in the future of integration, forever reshaping the technology landscape. Non-technical users will now be able to use natural language to execute complex IT tasks, thus lowering technical barriers and enabling them to work faster and more efficiently.

Going beyond no code/low code solutions to now natural language is a major advancement in the field of hyper-automation. Customers can now stitch together the apps that are specific to their business to create a custom view without the need for technical design.

<https://www.snaplogic.com/>

Newgen & Mambu Streamline Lending

Newgen Software is partnering with cloud banking platform, Mambu, as used by Commonwealth Bank of Australia. The partnership enables financial institutions to leverage Newgen's lending solutions, built on NewgenONE digital transformation platform along with Mambu's core banking systems, ensuring flexibility and adaptability.

"Newgen's solutions complement Mambu's core banking platform by streamlining lending functions across retail, commercial, SME, SBA, mortgage, and Islamic banking," said Rajvinder Singh Kohli, SVP, Sales, Newgen Software.

"The solutions align with Mambu's composable banking and lending approach to ensure faster market time and help financial institutions carve out their journey through customisation options. With this listing on the Mambu marketplace, Newgen will enable more financial institutions in their digital

journeys and impact more people and processes."

"Partnering with Newgen will bring value to customers by streamlining lending processes including onboarding, loan origination, and application management and underwriting. By combining the power of our cloud banking platform with Newgen's expertise in digital transformation, we can help more financial institutions offer modern lending experiences," said William Dale, Regional Vice President for Asia-Pacific at Mambu

Newgen's lending solutions, backed with AI-enabled underwriting, rule-driven decisioning, realtime dashboards, and document management capabilities, enable streamlined loan application management, portfolio management, instant disbursements on channels, and better collaboration. Mambu is a SaaS cloud banking platform. Launched in 2011, Mambu fast-tracks the design and build of nearly any type of financial offering for banks of all sizes, lenders, fintechs, retailers, telcos and more. Mambu has 900 employees that support 250 customers in over 65 countries - including Western Union, Commonwealth Bank of Australia, and ABN AMRO.

For more details, visit www.newgensoft.com

VIDIZMO adds Document Redaction

VIDIZMO has unveiled a new document redaction feature which allows organisations to quickly redact sensitive information from documents before sharing them with internal and external stakeholders. With a simple and intuitive interface, users can quickly identify and highlight sensitive information, such as personally identifiable information (PII), financial data, phone numbers, and confidential business information, and replace it with a black box, making it invisible to viewers.

The proprietary search algorithms employed by VIDIZMO go beyond simple keyword searches, delivering precision and efficiency in data redaction. It provides the convenience of automatic redaction of documents through searching for specific keywords, sentences and custom regular expression patterns to detect various types of sensitive information.

It also offers the flexibility of manual redaction with its line and text selection tools. Users can customise their redaction experience by manually selecting specific text areas or drawing a rectangular box to redact a particular section.

VIDIZMO also offers bulk redaction, allowing users to redact multiple documents simultaneously. Furthermore, VIDIZMO also integrates optical character recognition (OCR) capability with the new document redaction feature to ensure seamless redaction, even for scanned copies or various file types, making it a comprehensive solution for all redaction needs.

<https://vidizmo.com/>

Komprise Tiering for Azure Storage

Komprise, a specialist in analytics-driven unstructured data management and mobility, has extended its Microsoft collaboration with the availability of Komprise Intelligent Tiering for Azure.

Most organizations are spending 30% or more of their IT budgets on managing unstructured file data, which continues to grow rapidly. This Microsoft Azure Marketplace solution that gives customers access to file analysis and tiering to and within Azure. Customers can acquire this without purchasing the full Komprise Intelligent Data Management platform.

Organizations can accelerate their cloud journey and gain better ROI from cloud migrations by first transparently tiering data from any cold NAS that has not been accessed in months to Azure Blob Storage. This cuts an average of 70% of costs for storage, backup, and disaster recovery.

Second, an organization with file data in Azure Files or popular cloud NAS platforms can use Komprise Intelligent Tiering for Azure to tier data to lower-cost Azure Blob Storage automatically via easy-to-configure policies. Komprise Intelligent Tiering for Azure builds upon the success of the Azure File Migration program, which launched in February 2022 and gives customers access to Komprise at no cost to migrate data to Azure.

"More than 100 enterprises are already using Komprise through the Microsoft Azure Storage Migration Program because of its simplicity and convenience," says Krishna Subramanian, COO of Komprise.

"The new Komprise Intelligent Tiering for Azure extends this ease of use by allowing customers to use services such as Microsoft Purview, Microsoft Defender for Storage, Azure Synapse Analytics, and Azure AI with data copied or tiered from on premises. Azure customers can use their existing Azure contracts and utilize their Azure Consumption Commitments through this specially priced Komprise offer in the Azure Marketplace."

"Every organization in the current environment is looking to do more with less while reducing costs. The rising cost of on-premises storage is a pain point that we are pleased to tackle in collaboration with Komprise," says Jurgen Willis, VP Azure Specialized Workloads and Storage.

"Since Komprise tiers data to Microsoft Azure in native readable format and provides data workflows, customers can cut costs and leverage the full power of Azure services to address AI, big data, security, and compliance use cases."

Komprise Intelligent Tiering for Azure is priced at \$0.008/GB/month based on an annual subscription. The solution is available today on the Azure Marketplace. Customers can easily upgrade to the full Komprise Intelligent Data Management platform to gain Smart Data Workflows and the Global File Index with Deep Analytics.