idm.

information & data manager

**EzeScan celebrates
a major milestone**

Why Ransomware remains the
most destructive cybercrime

Five signs your Data Governance
initiative is failing

Put Proof of Identity at the Head
of your Onboarding Process

What is M365 Operational Governance?

iCognition deploys EDRMS cloud for Treasury

Australia's Department of the Treasury has gone live with iCognition's secure Content Manager EDRMSaaS. cloud. The Treasury selected iCognition as its long-term partner to help it seamlessly transition the Department from its current on-premise solution to a future-proofed and highly secure IRAP-protected cloud-based EDRMS, EDRMSaaS.iCognition upgraded the on-premises EDRMS to Content Manager version 10.1 and transitioned it to the iCognition Cloud within 60 days. With the launch of Treasury's EDRMSaaS, Treasury's Content Manager environments have been migrated to the new service to ensure ongoing management in a highly secure service.

The iCognition solution manages the Department's information to the highest available level of security, with assessment at the PROTECTED level by Information Security Registered Assessor Program (IRAP) and ISO 27001 certification.

As a central policy agency, the Department provides advice to the Government and implements policies and programs to achieve strong and sustainable economic and fiscal outcomes for Australians. As such, records and content management are a critical asset for the Department.

Rohan Ahluwalia, CTO at iCognition, said "iCognition's EDRMSaaS Content Manager Cloud provides the Treasury with a proven and secure SaaS solution that is the most advanced in the market. EDRMSaaS will continuously evolve and provide the best protection from increasingly sophisticated cyber threats."

Treasury joins iCognition's other clients on the EDRMSaaS platform, including Australian Digital Health Agency, The Tasmanian Department of Natural Resources and Environment, University of New South Wales, and clients in the financial and regulated industries market.

Joe Mammoliti, Chief Executive Officer, said: "iCognition's long-term relationships and deep understanding of our client's people, systems and processes enabled us to seamlessly transition them from on-premise to our secure cloud. Our proven capability and advanced cyber security assessment is widely trusted by both Federal and State governments. Our secure cloud solution and expertise gives them confidence that their decision to upgrade will meet their compliance demands and increase organisational efficiency."

Shareholders approve Micro Focus buyout

Shareholders of Micro Focus International plc have approved the terms of the recommended all-cash offer by OpenText, with regulatory clearances the only possible remaining hurdle. Subject to satisfaction of such conditions, the Acquisition is expected to close in the first quarter of calendar year 2023.

"We are pleased that Micro Focus shareholders have approved the offer," said OpenText CEO & CTO Mark J. Barrenechea.

"We have achieved an important milestone in our path towards completing the Acquisition. Upon closing, OpenText will be one of the world's largest software and cloud businesses.

ProcessMaker Acquires Doculayer IDP

ProcessMaker has announced the acquisition of the intelligent document processing specialist Doculayer, based in Amsterdam. Through the application of machine learning and artificial intelligence, Doculayer can classify and extract meaning and data from documents. Doculayer's intelligence can handle not only structured data that resides in known forms and tables, but also completely unstructured data from images, chats, emails, and much more.

ProcessMaker will incorporate Doculayer into its business process management (BPM) platform.

https://www.processmaker.com

Kofax Appoints Head of APAC and Japan Business

Kofax has announced the appointment of Australian Matthew Thomson as Senior Vice President of its Asia Pacific and Japan business.

Based in Singapore, Matthew has previously held senior positions at IBM in both Australia and Singapore and, more recently, VMware Tanzu, driving growth across Southeast Asia and Korea.

"As Kofax expands across the Asia Pacific region, global experience and market knowledge uniquely position us to understand our customers' requirements," said Thomson.

"By adopting a people-focused, inclusive mindset and leveraging Kofax's deep market and technical experience will enable customers to continue to quickly transform their processes to driving efficiency."

Australia's FOI legal bill jumps in 2022

Despite a 2% reduction in the number of Freedom of Information (FOI) requests received by Australian Commonwealth Government agencies in 2021-2022 Financial Year, FOI processing costs jumped by 5%, driven largely by increased expenditure on legal advice and litigation. Total legal costs jumped by more than 50% over 2020-2021. At $3.2 million they made up the vast bulk of non-labour costs of FOI.

The high litigation costs were incurred primarily by Services Australia, Home Affairs, the, the ATO, PM&C, Department of Agriculture, Water and the Environment (DAWE) and the Attorney General's Department.

In its 2021-22 Annual Report, the Office of the Australian Information Commissioner (OAIC) reported the total staff hours devoted to FOI was very much the same in 2021–22 (851,290 hours) as it was in 2020–21 (855,498 hours). There were 33% more notifications and applications for extensions of time (EOTs) for FOI processing during this financial year compared to 2020–21.

"When applying for EOTs, agencies continued to provide reasons relating to the COVID-19 pandemic as a cause for delay in processing FOI requests, particularly during the various lockdown periods. Reasons included redeployment of staff to frontline services and an inability to access hard copy files at offsite storage facilities."

The agencies that received the largest numbers of FOI requests in 2021–22 were: Home Affairs, Services Australia, the National Disability Insurance Agency (NDIA), Veterans' Affairs, the AAT, and the Department of Health (Health). Together, these 6 agencies received 75% of FOI requests received by Australian Government agencies and ministers, and 87% of all requests for access to personal information.

The OIC reports that agencies are blaming the increased complexity and volume in the FOI request caseload for processing delays. The number of applications for review by the Information Commissioner jumped markedly in 2022 to nearly 2000, up 63% from 2021.

"One of the causes of this significant increase was a large increase in IC review applications relating to decisions deemed to have been refused by Home Affairs because statutory timeframes had not been met. Of the 1,022 review applications made in which Home Affairs was the respondent in 2021–22, 885 involved deemed access refusals."

The average time taken to finalise an IC review was 6.3 months, although almost 20% of applications are still not finalised within 12 months. The OAIC has 135 staff, with 40% from non-English speaking background.

The OAIC Annual Report is available HERE

WWI diaries get new life online

Eyewitness accounts of the end of the First World War, as recorded in diaries and letters, are now available online as part of a major digitisation project led by the Australian War Memorial.

 These diaries and letters give an intimate insight to this globally significant day, as Australians gather to mark

Remembrance Day and commemorate the Armistice of the First World War, which was signed at 11 am on 11 November 1918.

"The Memorial has a multitude of original letters and diaries that express how people felt about the signing of the Armistice and the war coming to an end," Australian War Memorial Research Centre head Robyn Van Dyk said.

"Many of the letters and diaries on the Memorial's website record how people reacted to hearing of the end of a very long and horrific war. Some also took part in and recorded various celebrations.

"Many wrote about their relief of not having to fight anymore, for others there was a hint of disbelief.

"Others reflected on the loss of friends and family."
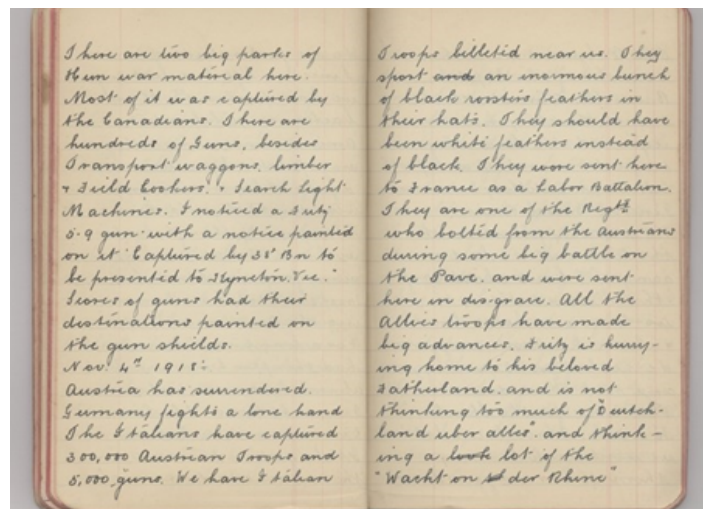
In one example, Lieutenant Sydney Traill wrote on the 11 November 1918: "It was officially announced late tonight that hostilities have ceased as from 11 o'c a.m. today. We knew early in the morning, though. No one displayed the slightest enthusiasm and it doesn't matter a tuppeny dump to me now, whether it goes on or not, the war has done its worst for our family."

Another example includes 18-year-old Australian Private Gallwey who wrote: "London has gone mad and I am intoxicated with joy."

The First World War collections of diaries and letters are part of the Memorial's four-year digitisation project.

"Digitisation makes these collections so much more accessible to everyone," Ms Van Dyk said.

"There are over 14,000 collections that have been digitised including archival records, photographs, film, maps, art posters and objects, all now being progressively published.

"In the past, people had to travel to Canberra and request to view these items which were only able to be viewed from the Reading Room but now you can access these historic records from home and unlike paper you can zoom into the text and bring up the content in detail.

"Personal collections such as letters and diaries give us a deep insight into how many Australians felt, you get a sense of what it was like for those individuals.

"Thanks to this project more and more of these collections can now be accessed online."

To find more historical gems use collection search to discover them online.

ABBYY puts Proof of Identity at the Head of your Onboarding Process

With the Optus hack recently dominating headlines in Australia, ABBYY has announced the timely release of a new all-in-one solution that offers instant identity proofing and affirmation. ABBYY Proof of Identity simplifies document-centric digital onboarding processes while promising to give organisations confidence that customers, constituents, employees, and partners are who they say they are.

As more consumers go online to conduct business, the challenge of verifying identities to prevent fraud has become increasingly critical.

One of the critical steps in completing online and mobile forms involves providing personal identification data, however more than half of consumers (68%) abandon an online onboarding process.

Additionally, there is concern for fraud with the US Federal Trade Commission reporting more than 2.8 million US consumers lost $US5.9 billion to fraud in 2021, including identity theft and imposter scams, an increase of more than 70 percent over 2020.

According to the Australian Bureau of Statistics, an estimated 0.8% of Australians aged 15 years and over (154,300) experienced identity theft in 2020-21. This was similar to the rate in 2014-15 (0.7%).

Of those who experienced identity theft, the stolen personal information was most commonly used to obtain money from a bank account, superannuation, or investments or shares (57% or 324,800).

To avoid risks and expedite the onboarding process, more organizations are turning to document-centric identity proofing methods where an image or video of the user's identity document is compared with an image or video of the user's face.

Gartner predicts that by 2023, 85 percent of organizations will be using document-centric identity proofing as part of their onboarding processes.

Bruce Orcutt, SVP of Product Marketing at ABBYY, said, "More high-risk interactions are transacted online especially in banking, healthcare, and government that require balancing trust in a person's real-world identity with the customer's expectation for a smooth user experience – and there needs to be a better way of doing it.

"ABBYY Proof of Identity accomplishes this by leveraging the company's intelligent process automation technology into identify proofing and identity affirmation capabilities that are easy for customers and secure for businesses.

"By using ABBYY Proof of Identity as part of their onboarding platforms, organizations will have significantly lower abandonment rates, and customers will benefit from a positive experience."

ABBYY Proof of Identity is built on ABBYY Vantage intelligent document processing and ABBYY Timeline process intelligence to seamlessly deliver all the capabilities to match a user's claimed identity with their actual identity, including:

■ ID reading, including mobile capture and document classification;

■ ID verification, including image-tampering fraud detection;

■ Facial matching based on a top rated NIST-rated algorithm with extremely low bias;

■ Trailing documents (document-centric identity affirmation);

■ Exception handling (optional human auditing of certain transactions); and

■ Process intelligence and mining to identify opportunities for process improvement.

Organisations interested in improving their onboarding experiences and reducing fraud risk can request a demo.

To learn more visit ABBYY Proof of Identity.

Five signs your Data Governance initiative is failing

By Nicola Askham

One: There are different understandings of the terminology within the same organisation

Most organisations are full of lots of jargon and terminology which can mean different things to different people. It's all very subjective and this is usually because of the culture within a particular organisation. The way the various terms are applied within organisations can vary their meaning. And that's ok - but you should also be wary of it. Data Governance takes a long time, and particularly in the early phases, it takes quite a lot of effort. Therefore, it is understandable that people look for ways to quicken this process up. One of the ways I am often asked if this can be done is by fast-tracking the creation of items like a data glossary by using standard definitions.

However, it's not a part of the process that can be skipped or glossed over, so to speak. Part of the reason for this that organisations, even those within the same industry, very rarely use the same terminologies in exactly the same way. This means there is no bank of standard definitions to pick and choose from; what works for one client, will very rarely work for the next. Only by creating your own data glossary can you be sure that everyone fully understands the definitions within it.

Two: Disengaged stakeholders and a lack of budget

Another reason many data governance initiatives fail is a lack of support at a management level. If senior management does not buy into the benefits of data governance and only sees the associated costs, an initiative will almost never succeed.

First, there is a danger that the required processes won't be executed correctly. Additionally, because of costs, critical improvements may not be implemented, or the initiative may need to end prematurely.

Sourcing the budget needed for an initial data governance initiative is easier today than ever before because there are regulations that justify it, for example the GDPR. However, it is crucial that management also makes sufficient long-term resources available to finance all roles and functions required for robust data governance on an ongoing basis.

If your stakeholders aren't prepared to put their money where their mouths are, this would indicate that the initiative is not being taken seriously enough and its value is not understood.

Three: Only implementing Data Governance because of regulations

If the pressure to implement data governance comes from a regulator, then it is very tempting for organisations to look at satisfying the absolute minimum required to keep the regulator happy. This is a big mistake, as in the long run, these organisations end up doing more work than if they properly implemented data governance in the first place. They also miss out on all the business benefits that come from improving their data management practices.

The tick-box approach to data governance is normally task-focused and completely ignores the people involved. They issue a checklist of things that need to be accomplished and issue threats if the tasks are not completed. As a result, people go through the motions because they must, and they see no real benefit to their day-to-day job. As a consequence, it's going to be hard to embed your data governance framework within your organisation and you will always be chasing people to make sure that they have complied with the regulations.

Regulators are notorious for moving the goal posts, so if you have not embedded data governance into your organisation, every time they change the regulations and update the checklist you will probably move back to square one, which means implementing the new checklist.

Four: No data quality issues being reported

If data users aren't reporting data quality issues, this indicates that either people don't know about your process to investigate and fix issues, they don't think you will be able to make a difference (maybe based on years of no-one being interested in making data better) or perhaps they don't understand that the manual workarounds they have to do every day/week/month are the result of poor data quality and everything could be improved and streamlined if the underlying issues were addressed.

Whatever reason, it all boils down to communication. And if you're failing to communicate with your data users your data governance initiative is sure to fail.

Five: It's not being talked about outside of IT

The key to data governance success is getting stakeholders to take ownership of their data and take the lead in data governance initiatives. When I perform a data governance health check for companies that are running into trouble, it is fairly common for IT to be leading the data governance initiative. This is always for the best of intentions. Even though IT does not own the data, they understand the implications of not managing data properly, and therefore they are often the first people in any organisation to realise that proper data governance is needed.

Businesses often leave IT to deal with data governance because they confuse the infrastructure with the data. If you work for an organisation that still believes that IT owns the data, then assigning IT to run the data governance initiative may seem logical. However, an IT-led data governance initiative can be fraught with problems. True data governance will only really happen once the business has taken ownership of their data, and an IT-led data governance initiative makes that more difficult.

In my experience, IT-led initiatives are too focused on tools that do things like cleansing data. This is understandable, as companies tend to get their advice from IT vendors who are in the business of selling tools. The problem is that unless a business changes the way that data is captured at the point of entry, the quality of the data will never improve.

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 https://www.nicolaaskham.com/

EzeScan 20th Anniversary 2022

At a function held this month near its company HQ in Brisbane, Australia's EzeScan celebrated 20 years since the business was founded in 2002.

Joining in the celebrations were (clockwise from top left below): Chris Ewers of reseller Infocentrik; Michael Redman of reseller Redman Solutions, Jessie Parker of Distributor TacoTechnologies; Director of Sales & Marketing Demos Gougoulas receiving the Outstanding Sales Award; and proud Dad Mike with son Justin, a software developer at EzeScan for the past 10 years, and daughter and Marketing Assistant Amanda.

Celebrating EzeScan's 20th anniversary with staff, clients and partners, CEO Mike Kirkby reflected on two decades since establishing parent company Outback Imaging in his home garage in suburban Brisbane.

Initially developed as a Windows-based Document Management application called ScanIT, the EzeScan software suite is now deployed across the APAC region and globally to aid in automated data capture and information processing solutions for unstructured, semi-structured, structured hardcopy and electronic documents including email and digital forms.

"2023 is going to a great year for us," said Kirkby. "Our products are now even more re-aligned to solving real world customer problems. EzeScan CLOUD on AWS is now past the startup phase. We are regularly on-boarding new customers in our target verticals.

"In 2023 we will be launching a new CLOUD offering for our resellers," he announced. "This cloud will allow our resellers to sell and implement their own vertical market solutions that are 'Powered by EzeScan'."

Kirkby expressed his thanks to "customers for their purchases and their ongoing use of our software, loyal relationships going back over 20 years. Without our customers we would not exist.

"Also, thanks to our resellers for their efforts they put into selling and supporting our solutions, here in Australia and the UK and USA.

"We know you have a choice to sell other products and we appreciate your ongoing relationship with us.

"Finally, thanks to our staff who turn up day after day, believing that they can make a difference to our customers.

"Continually going above and beyond to help people. There is no company without our people," said Kirkby.

The EzeScan software development team (Back row l-r) Anthony, Ryan, and Business partner and Head of Research & Development, Keith. (Front Row l-r) Rhys, Justin and Christian.

EzeScan 20th Anniversary 2022

Mike Kirkby with EzeScan International Sales Manager and Business Partner Kevin Blackely, who received an award acknowledging 15 years of service.

Nancy Taia, Records Solutions (l), Anne Cornish, RIMPA.

Below is a Timeline highlighting significant product and company landmarks that have been achieved over the past 20 years.

The EzeScan Admin team: (l-r) Jennifer, Sarah, Catherine, Janette, Meera and Jessica.

2002
- Bought ScanIt IP from alphawest
- Outback Imaging PTY LTD created
- Built home office in garage
- e-Quip (Demos) became a reseller
- TRIM Integration

2003
- Released EzeScan 3.0 Pro & LITE
- ProScan became resellers
- Xerox DocuShare Integration

2004
- Released first modules
- Rivetgroup became resellers
- Interwoven

2005
- Released EzeScan Version 4.0
- Fuji Xerox became a reseller
- Objective Integration

2006
- Infocentrik Objective
- Merido Integration

2007
- EzeScan SERVER as a product
- Moved into Carina office building
- Sharepoint Integration

2008
- Ricoh became resellers

2009
- Outback Imaging UK Limited created
- OBS, Kapish & Lanier
- InfoXpert Integration

2010
- Released EzeScan Authority Server
- IDR, ISIS, MICR & OMR Modules
- Extrados, CSG, OIA, Civica, FYB, Alloys & Clarity
- DocuVantage, Civica, DocuWare & Laserfiche

2011
- Trinogy, Phoenix & Imex
- InfoRouter, Alfresco & TechologyOne

2012
- Started renting shop front 1A
- Released Line Items module
- Proficiency & Quantario
- Infor Integration

2013
- Outback Imaging USA LLC created
- Barcode Coversheet Generator
- Genie & Shexie Integrations

2014
- EzeScan WebApps RIA, FUA & FAA
- Email Record Capture Module
- Blackbaud, Xero & Myob

2015
- Viatek & Vikings Office Systems
- Therefore Integration

2016
- Digital Forms Assistant Web App
- BBC & ITEC became resellers

2017
- Started renting Melbourne office
- Started Scanner Rentals
- Redmans Solutions became a reseller
- M-Files Integration

2018
- Informotion & Post Partner
- Redbrick

2019
- Apogee & Rubix Software
- IT Vision Altus Integration

2020
- Bought new Morningside Office
- Released EzeScan Version 5.0
- TacoTechnologies became a distributor

2021
- First EzeScan CLOUD Customer
- Leap, Lexis, Link4, NetDocuments & Practice Evolve

2022
- First UK & USA CLOUD customers

Ransomware remains the most destructive cybercrime: ACSC

Ransomware tops of the list of threats to Australian online security according to the third Annual Cyber Threat Report by the Australian Cyber Security Centre (ACSC), a part of the Australian Signals Directorate (ASD).

The Report is the product of insights from across the Commonwealth, with the Australian Federal Police, the Australian Criminal Intelligence Commission, the Australian Security Intelligence Organisation, Defence Intelligence Organisation and the Department of Home Affairs also contributed.

The ACSC received over 76,000 cybercrime reports on 2021-2022, an increase of nearly 13 per cent from the previous financial year. This equates to one report every 7 minutes, compared to every 8 minutes last financial year.

There was also a rise in the average cost per cybercrime report to over $A39,000 for small business, $A88,000 for medium business, and over $A62,000 for large business

Ransomware remains the most destructive cybercrime according to the ACSC.

"The ACSC received 447 ransomware cybercrime reports via ReportCyber. While this is a 10 per cent decrease compared with the 2020–21 financial year, reports remain higher than in 2019–20. It is also likely that ransomware remains significantly underreported, especially by victims who choose to pay a ransom."

A 2022 study published by the Australian Institute of Criminology found only 19 per cent of ransomware victims sought advice or support from police or the ACSC. However, the study found nearly 60 per cent sought help from at least one formal source outside of their family or friends.

The study found 23.2 per cent of small to medium business victims paid the ransom, with many millions of dollars being paid in ransoms and other associated costs.

"The education and training sector reported the most ransomware incidents in 2021–22, rising from the fourth-highest reporting sector in 2020–21. The threat to the education and training sector is significant as its business model favours open collaborative environments. Remote learning during the coronavirus pandemic also introduced large numbers of personal devices and new software into this sector.

"Ransomware groups have further evolved their business model, seeking to maximise their impact by targeting the reputation of Australian organisations. In 2021–22, ransomware groups stole and released the personal information of hundreds of thousands of Australians as part of their extortion tactics.

"The cost of ransomware extends beyond the ransom demands, and may include system reconstruction, lost productivity, and lost customers."

The ACSC responded to 135 ransomware incidents in 2021-22, an increase of over 75 per cent compared to 2019–20. It notified 148 entities of ransomware activity on their networks.

(Continued Over)

"Cyber dependent crimes, such as ransomware, were a very small percentage of total cybercrime reports. Nevertheless, the ACSC assesses that ransomware remains the most destructive cybercrime threat.

"This is because ransomware has a dual impact on victim organisations - their business is disrupted by the encryption of data, but they also face reputational damage if stolen data is released or sold on. The public are also impacted by disruptions and data breaches resulting from ransomware," the report notes.

"The evolution of Cybercrime-as-a-Service (CaaS) continued to increase the overall cybercrime threat to Australia. The expansion of the CaaS industry has lowered the barrier to entry for actors seeking to conduct cybercrime.

"For instance, Ransomware-as-a-Service (RaaS) provides actors who may not have the technical skill to develop their own ransomware with an opportunity to launch highly profitable attacks. In addition, the CaaS industry allows actors to monetise their expertise in a particular skillset. As a consequence, cybercriminals have become more specialised over 2021–22, and pose a greater threat to Australians and businesses."

Top-tier ransomware groups are continuing to target Australian 'big game' entities—organisations that are high profile, high value, or provide critical services.

"Ransomware is a cyber dependent crime which can impact everyone from consumers through to countries. For example, the Costa Rican Government declared a state of emergency in May 2022 following ransomware attacks on nearly 30 government institutions, including its health, finance, energy and social services departments. While Australia has not experienced an incident of this scale, the potential remains for cybercriminals to cause widespread disruption.

"Top-tier ransomware groups are continuing to target Australian 'big game' entities—organisations that are high profile, high value, or provide critical services. While global trends indicate a decline in 'big game' targeting and a shift towards targeting small and medium sized businesses, that change has yet to be seen in Australia.

Dr Lennon Chang, Criminology, School of Social Sciences at Monash University said, ""There is no big change in terms of cybercrime types compared to last year's report. Money is still the main purpose for cybercriminals. The line between cybercrime and national security is becoming blurred. Cyberattack and cybercrime are now part of cyberwar. Cybercrime can become a national security issue, given the current landscape. More attention and resources need to be applied to understanding disinformation and developing countermeasures for the same. It is important for the Australian Government to work closely with its allies, including Taiwan."

Case Study 1: Local council ransomware incident

In April 2022, a NSW council was targeted by a ransomware incident. The initial access occurred at least 2 weeks before the incident, with the malicious

actor likely timing the incident to occur over the Easter long weekend.

Manual processes were immediately implemented to manage water-quality testing and level monitoring, and temporary servers were established within 24 hours to restore remote monitoring.

The incident impacted a wide range of business operations, including council minutes, employee financial data, and systems responsible for monitoring water quality. The incident also had a huge impact on council technology staff, who worked 40–80 hours overtime a week during their initial response.

The council engaged a commercial incident response provider, and its Managed Service Providers (MSP) deployed additional capabilities. The ACSC provided advice to the council and warned ACSC partners in the water sector to be alert to possible ransomware targeting.

The incident demonstrates the interplay between IT, operational technology, and the physical environment. The initial access through a legacy entry point impacted multiple systems, including operational technology systems, which meant that council workers had to manually test water quality and levels following overnight rain. A swift response by the council, its MSP, and the ACSC ensured there was no compromise of water or sewage services. The council's MSP continues to monitor the darkweb for data leaks.

The case study demonstrates the importance of decommissioning legacy systems and erecting firewalls between IT and operational technology systems.

Case Study 2: Australian social assistance organisation

In March 2022, an Australian social assistance organisation was targeted by ransomware resulting in the theft of data. The malicious actor gained access to the organisation's servers through exploiting an unpatched version of Microsoft Exchange.

Within 4 days, the malicious actor moved from initial access to encryption. The organisation's Chief Information Security Officer told the ACSC, "it spins my head about how quickly they were able to move around the network".

The organisation identified that its systems had been encrypted and immediately notified Commonwealth and state agencies. It engaged its existing commercial incident response provider to provide technical support and conduct an investigation.

The organisation credits its ability to recover so quickly to maintaining a strong relationship with their incident response provider and moving to cloud-based backups in the months before the incident. Remediation and related network security improvements cost approximately $A200,000, which was substantially less than the ransom demanded.

Since this incident, the organisation continues to monitor for residual risk, and is hardening its cyber defences more broadly, including enhanced restrictions for applications, and better managed network awareness.

During the organisation's engagement with the ACSC, it shared indicators of compromise, which the ACSC shared through the CTIS portal. This enabled other organisations to better protect themselves, ultimately strengthening the security of Australian organisations.

Read the report in full

ISACA Digital Trust Research Reveals Gaps

As enterprises worldwide compete in the race for digital transformation, the State of Digital Trust 2022 survey report from ISACA shows significant gaps between what enterprises are doing now and what they should do to establish leadership and earn customer trust in the future digital ecosystem.

The State of Digital Trust 2022 report features insights from 2,755 business and information technology professionals from around the world. ISACA defines digital trust as the confidence in the integrity of relationships, interactions and transactions among providers and consumers within an associated digital ecosystem. It is a driving factor in consumer decisions and enterprise resilience in a digital-dominated environment.

While nearly all respondents in Australia and New Zealand (95 percent) say that digital trust is important and 60 percent said that digital trust is relevant to their jobs, only 12 percent of their organisations have a dedicated staff role for digital trust. Looking to the future, 79 percent say digital trust will be even more important in five years than it is today, yet only 25 percent offer digital trust training to staff.

"Digital trust is the bedrock of business relationships, and is critical for strategic digital transformation," said David Samuelson, chief executive officer, ISACA. "Innovation, market leadership and financial performance rely heavily on trust that must be earned every day."

Just one breach of digital trust can cause devastating reputational, regulatory and financial repercussions. Yet only 71 percent say their organisation currently prioritises digital trust at a sufficient level.

Survey respondents are aware of the consequences and say that organisations with low levels of digital trust experience: reputation decline (68 percent vs 62 percent globally), more privacy breaches (73 percent vs 60 percent globally), more cybersecurity incidents (71 percent vs 59 percent globally), lost customers (51 percent vs 56 percent), less reliable data for decision-making (56 percent vs 53 percent globally) a negative impact on revenue (40 percent vs 43 percent globally) and a slower ability to innovate (33 percent vs 36 percent globally).

Even in an era in which enterprises heavily prioritise metrics and data analytics, only 27 percent say their organisation measures the maturity of its digital trust practices.

Those that measure digital trust have two areas in common—their board of directors has prioritised digital trust and they use a digital trust framework.

According to the ISACA survey, the most significant obstacles to digital trust are: lack of skills and training (53 percent), lack of alignment with enterprise goals (41 percent), lack of leadership buy-in (47 percent), lack of budget (43 percent) and lack of technological resources (32 percent).

Benefits of digital trust

Enterprises experience a range of key benefits when they prioritise digital trust in their strategic planning. According to respondents, high levels of digital trust lead to:

- Positive reputation (70 percent vs 66 percent globally)
- Fewer privacy breaches (74 percent vs 68 percent globally)
- Fewer cybersecurity incidents (69 percent vs 57 percent globally)
- Stronger customer loyalty (49 percent vs 55 percent globally)
- Faster innovation (54 percent vs 44 percent globally)
- Higher revenue (25 percent)

Even with global efforts such as the Digital Trust Initiative from the World Economic Forum, only 32 percent of respondents were extremely or very familiar with the term "digital trust." This underscores the importance of a consistent drumbeat about digital trust and its growing importance on the enterprise landscape.

An emphasis on digital trust also presents major opportunities for career growth, as 79 percent say digital trust will be much more important in their organisation and 24 percent say their organisation will likely have a senior staff role dedicated to digital trust in five years.

Respondents said the top three components of digital trust are security, data integrity and privacy, but only half of respondents agree that there is sufficient collaboration among professionals in these and other digital trust fields.

The top three roles for strengthening digital trust are IT strategy/governance (85 percent), security (80 percent) and risk and compliance (80 percent). Many organisations are still in early stages of digital transformation, so this is an excellent opportunity for professionals to step up, gain knowledge and lead a multi-disciplinary team.

Tools for the digital future

According to 70 percent of respondents, digital trust is very important to digital transformation.

Respondents also want tools to help with transformation—43 percent say that having a digital trust framework would be extremely or very important to their organisation.

To help enterprises grow their digital trust capabilities, ISACA is releasing the Digital Trust Ecosystem Framework (DTEF) in the fourth quarter of 2022. DTEF is a business framework designed for the entire enterprise and focuses on providing critical factors for organisational success by fostering trusted, meaningful and mutually beneficial relationships, interactions and transactions.

GDPR: Bureaucratic monstrosity or necessary for data protection?

By Andreas Dumont

On May 25, 2018, the EU's General Data Protection Regulation (GDPR) went into effect. It was intended to grant universal protections for personal data in all of Europe.

The COVID-19 pandemic sparked new discussions about loosening GDPR requirements, and companies are also constantly demanding revisions to the regulation. The four-year anniversary of GDPR is a good time to look back and compare what things are going well and what is not going so well.

Reasons for GDPR

Each user and every activity on the internet, whether private or work-related, leaves behind a trail of data. This data is highly valuable and is therefore collected, stored, and sold. With increasing amounts of data being processed and digitalization and automation becoming more normalized, so too grows the risk of data breaches and abuse.

The EU therefore created the common regulation as a legal framework for more awareness and security in the handling of data. Companies now have to provide extensive information on how they collect, process and store personal data.

(Many Australian and New Zealand businesses with customers in the EU, or that operate in the EU, are also covered by the GDPR. Data breach notification is required in certain circumstances under the GDPR and under the Australian Privacy Act. There are also certain situations where it applies to foreign government agencies)

The upsides of GDPR

GDPR has been instrumental in bringing the issue of data protection and privacy into the public eye and into the consciousness of "online" citizens. It grants the users of services the right to be informed of what is being done with their information, i.e. to know who has what data and what they intend to do with it. Many citizens now assert their rights as data subjects. Awareness within companies has grown just as much as in private individuals – this not only because of the hefty fines which await them should they not comply.

Topics like the right to be forgotten and the transfer of personal data between service providers were hardly discussed before GDPR. GDPR has also made a big impact outside the EU and now serves as a role model for data protection in many non-European countries.

A well-functioning data privacy policy and compliance with GDPR build confidence in digital services and applications. Many companies see their GDPR conformity as giving them a competitive advantage.

What is not going so well

Not everything that glitters is gold. There are surely many points where adjusting might make sense – most notably concerning the nuisance of constant cookie confirmation requests. Users need to click their way through them to get to the content they actually want, and nobody really reads them anyway.

Many places, even public administrations, are still clueless regarding their data protection. Better and well-founded information including instructions for actions would be desirable here.

GDPR has still not achieved its foundational goal of harmonizing legal frameworks and practices with respect to data protection. Too many clauses allow for national workarounds to circumvent GDPR, so its application varies from country to country.

In Germany alone, there are 18 supervisory authorities with often different interpretations of GDPR. The German state of Bavaria even has two authorities dedicated to this topic.

Small businesses especially find themselves overwhelmed by GDPR requirements. The documentation and retention obligations come at a great cost. The effort required to correctly implement the regulation is not insignificant.

There is relief, however – suitable platforms include enterprise content management (ECM) systems like the ELO ECM Suite. Deletion deadlines, rights to information, obligations to document personal data – ECM solutions facilitate document management in compliance with GDPR and other legal requirements.

In the wake of the pandemic and the somewhat hastily implemented switch to widespread remote working policies, IT teams had little time to adjust their work processes to comply with GDPR and are still playing catch-up.

Summary and outlook

Despite the complexities and hurdles, GDPR has generally stood the test. But even after four years of GDPR, there is still much to do in terms of data protection. We should maintain our commitment and not allow interest in this important topic to wane. Businesses must find a suitable platform to implement and abide by GDPR requirements.

Legislators should regularly evaluate experiences with GDPR and make improvements where measures were overly bureaucratic without yielding significant results – but also take account of where sanctions are too lax. Perhaps GDPR will still fulfil its true purpose after all: ensuring the best possible data protection for all parties.

Technical solutions will also be necessary. When companies are not willing or able to operate without American services like AWS, Microsoft, and the like and allow data to be processed in the USA, it's hardly possible to guarantee compliant data security at the moment.

(ELO Australia has launched its own Australian-based cloud services, ensuring that data is stored in Australia and stays in Australia.)

How content intelligence is changing the use and management of information

A business perspective from David Gould

The content lifecycle times, they are a-changin'! In the good old days of information governance, the management lines between active content for use and passive content for retention were clear.

I remember the first time I was introduced to this concept by my colleague and now EncompaaS Chief Product Officer, Jaimie Tilbrook. He explained it to me 13 years ago, on a whiteboard in his Adelaide, Australia office. Above is a replica of his drawing:

Users created and consumed content during the active phase, and information governance and records managers became the custodian of passive content to ensure proper management until the end of lifecycle.

The main takeaway was that a solid, defined vertical border existed on a continuum (see orange circle) between active content, such as a Standard Operating Procedure or business plan (in use by the creator and anyone working on a similar project), and passive content, such as meeting minutes, or prior versions of travel policies that needed to be retained (because they were considered a record).

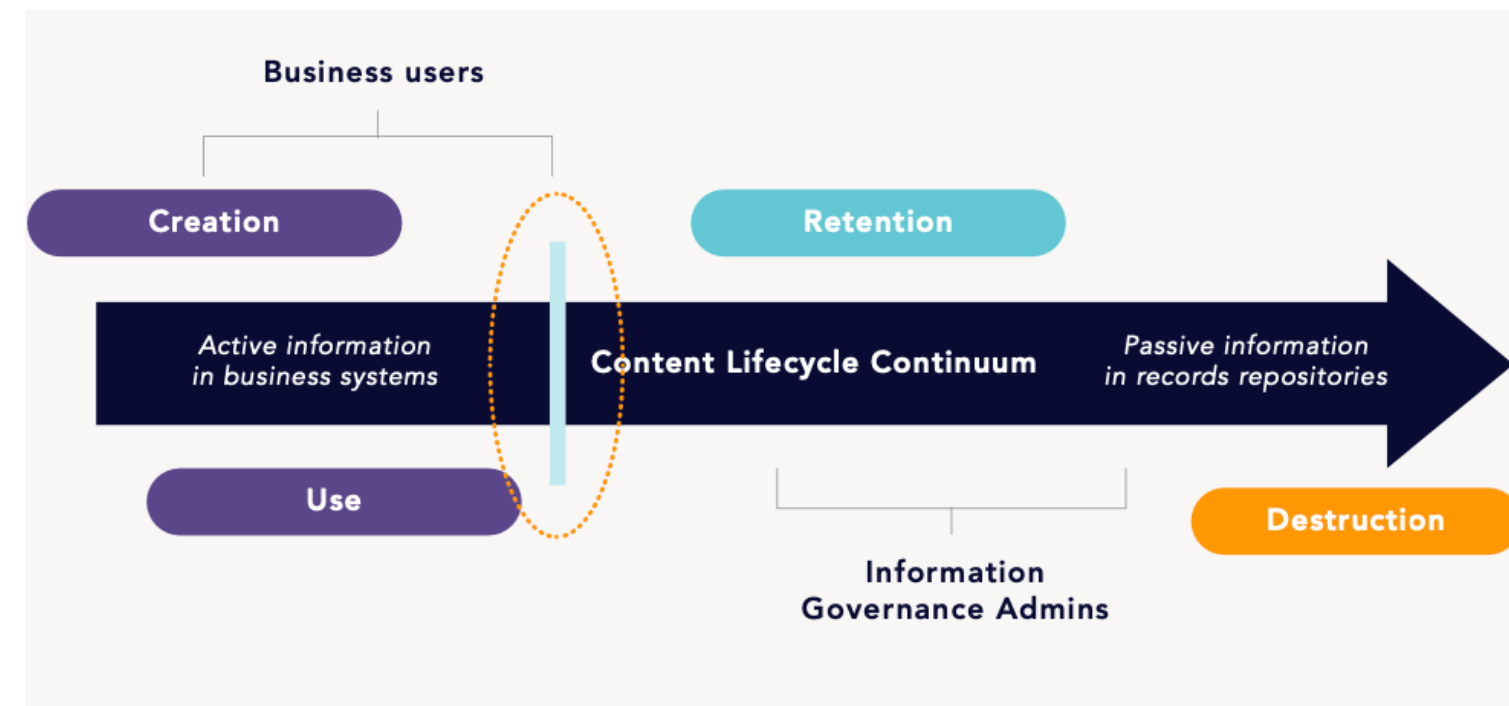For many years, this time-based continuum featured a hard line between what was considered active and what was considered passive. It was the methodology norm for content use and lifecycle management of information.

Once in a passive stage, the content usually never saw the light of day again, except for legally bound search. However, as noted lyricist Bob Dylan wrote early in his career: "The times, they are a-changin'".

Today, we are seeing not just a blurring of the distinction between active and passive management of content; we are seeing an obliteration of the entire concept.

The data lake, once the exclusive milieu for the rows- and columns-based data, is extending to the petabytes of unstructured and semi-structured content found in Microsoft 365, OneDrive, file shares, and hundreds of information repositories strewn across the enterprise.

The methodology transformation is enabled by new advances in machine learning and artificial intelligence, making it possible not only to classify information with great accuracy but also to find concepts and passages that are useful and required to support better business decision-making. It is what we at EncompaaS call content intelligence.

> **Today, we are seeing not just a blurring of the distinction between active and passive management of content; we are seeing an obliteration of the entire concept.**

Content intelligence is the next generation of content management, where AI extends the value of information throughout its lifecycle. It makes information valuable no matter if it is 30 days young or 300 months old.

The bottom line is that enterprises can continue to use unstructured information throughout the lifecycle for solving essential and hard-to-answer business questions.

A notable example of content intelligence is in the Life Sciences industry where those responsible for rebate management programs need to extract key values from tens of thousands of unstructured contracts to preserve and grow market share and increase business revenue.

With contracts in different formats, lengths, and locations, this is no simple task.

We would argue that without the ability to do content intelligence, it is next to impossible to successfully manage and get results using legacy, manual processes.

Another development in this next-generation content intelligence approach is that the ability to extract and analyse complex content is not limited exclusively to the data scientist domain.

Next-generation analytics software like our EncompaaS platform enables existing personnel to do the analytics themselves. Your teams can confidently oversee automation and focus on the insights and visibility this processing provides.

Before some start to celebrate, jump for joy, or deeply worry about changes to the job, these advancements do not mean that content management is a dead subject. The exact opposite is true.

The biggest difference is the shift from manually applied lifecycle methods to the use of full automation to discover, understand, govern and use content across the enterprise.

Content intelligence is the nirvana concept realised. It allows us to fully use insights in a permissible way, providing great answers to questions that could not be answered in the prior era.

You cannot put 20 people in a room and expect them to sift through thousands of contracts to find terms and phrases, extract them into a report, do calculations and visually present the information so it is understandable and actionable. It's simply not effective or sustainable.

Contracts evolve with amendments and the data we want to extract can change with regulations and commercial plans, requiring another manual search. For sites with agreements in the 10,000+ category, a few hours on an agreement is a significant expense.

The opportunity is to fully embrace this new era of content intelligence where people, performance, and business processes are directly supported by the next generation of solutions, such as EncompaaS, to automate your mission-critical business tasks.

The bottom line is improved business decision-making and outcomes in a more complete, timely, and accurate manner. For information governance and records managers, these opportunities are game-changing.

Feel free to reach out to me via LinkedIn to find out how EncompaaS can help your organisation discover the value of information and put it to work for better business outcomes.

https://encompaas.cloud/

David Gould
Chif Customer Officer
EncompaaS

Business users

Creation

Retention

Active information in business systems

Content Lifecycle Continuum

Passive information in records repositories

Use

Destruction

Information Governance Admins

Perfect storm pushing public sector towards AI: Survey

Micro Focus has released the findings of the *2022 Digital Challenges in the Public Sector* study, created in partnership with Omdia, which examines the common technology trends facing the Australian public sector.

While it was revealed technology investment is increasing across Australia, with more than 50 per cent of respondents anticipating an IT spending rise during the next 18 months, the public sector is facing a perfect storm driven by skills shortages, increased demand, and capabilities of legacy systems.

The public sector is under increasing pressure to supply comparable digital user experiences to private enterprises, such as eCommerce platforms, while protecting citizen data, on systems that can often be years or decades out of date.

The white paper reports the sector is struggling to fill almost any technical role and relies heavily on contract labour, with some projects having as few as five per cent public service staff within a delivery team.

Driven by this combination of shortfalls in skilled resource availability, the inability to be salary-competitive with the private sector, and increasing operational expectations, the public sector is anticipating a shift to artificial intelligence operations (AIOps) to ease pressure.

Key findings of the study include:

• **Technology resources are scarce:** Specifically, sourcing skilled cybersecurity, architecture, and developers are pain points. Agencies are addressing resourcing gaps by partnering with service providers or developing training programs in high-demand areas, such as cybersecurity.

• **AI presents a new opportunity:** Globally, the adoption of AIOps across all industries is accelerating, with most organisations expecting to see full adoption by 2023. In Australia, government agencies are actively investigating the use of Software-as-a-Service (SaaS)-based service solutions, underpinned by AI and automation to ease pressure, cost, and complexity.

• **Time-to-delivery is critical:** Stakeholders routinely compare agencies with agile, flexible, and consumer-focused commercial entities, and the primary criticism is that everything takes too long. As such, more than 50 per cent of respondents plan to invest in constituent experience software such as compliance management, enterprise resource planning, and business continuity in the next 18 months.

• **Technical debt undermines agility:** To bridge old and new solutions, government executives overwhelmingly agree progressive use of cloud-based solutions (Platform-as-a-Service (PaaS) and SaaS) can eliminate, or at least minimise, technical debt. Global agencies see less than 35 per cent of future capabilities being delivered under traditional models.

John Garratt, federal government director, Micro Focus, said, "As the world recovers from the global pandemic, this year's Digital Challenges in the Public Sector report highlights the pressure that Australian government agencies have experienced the last few years.

At a time of increased demand, departments have been struggling to deliver services with skeleton teams, out-of-date systems, and competition with the private sector.

"In the next 18 months, dependence on solutions like SaaS, PaaS, and AI will increase, easing the strain on already-burdened departments."

This year's *2022 Digital Challenges in the Public Sector* report also outlined recommendations for public sector agencies to deal with their underlying technical challenges:

1. Leverage AIOps to maximise scarce skilled resources. Agencies should take advantage of modern SaaS AIOps offerings to avoid the cost and complexity of multiple on-premises monitoring tools. Automating discovery, monitoring, and remediation will ensure that valuable staff can focus on activities that deliver maximum benefits.

2. Use a value-based and risk-based lens approach to communicate the trade-offs in technology investment decisions. As management boards focus ever more closely on risk, they should translate IT investment priorities into relatable concepts for senior decision-makers.

3. Progressively use SaaS, where appropriate, to minimise future technical debt. SaaS solutions are updated by the provider, and therefore never more than one release behind the current version.

4. Adopt and promote a standardised platform-function PaaS architecture to speed up the delivery of new capabilities. Minimising delivery time is essential. Building common functions from PaaS components will make delivery more responsive to stakeholder requirements.

5. Understand the profile of legacy applications and appropriately mitigate associated risks. Solutions running on unsupportable hardware and/or software embed organisational risk and should be prioritised for retirement or replacement.

John Garratt said, "Delivering seamless services involves a balancing act between modern and legacy systems, expectations, and capability to provide good value for staff and end users alike.

"With investments in IT set to rise, it is essential that public-sector agencies take advantage of technology to bridge gaps in efficiency, boost positive outcomes, and keep costs low."

In partnership with Omdia, the study was developed from primary data drawn from Omdia's *2022 Enterprise Insights Survey* coupled with one-on-one interviews with senior executive decision-makers in the Australian public service and government technology space.

Confidential interviews were held during June 2022 to confirm underlying trends within the government technology space.

Click here to read the full *2022 Digital Challenges in the Public Sector* whitepaper.
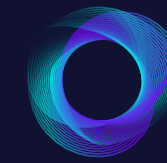
Don't Let Data (In)Visibility Limit Your Digitisation Dreams

By Ryan Tandler, Gartner Inc.

Since the inception of the home printer, one question has bewildered humanity: How do you predict the point at which the quality of the printed page will decline to such a degree that any residual ink in the cartridge isn't worth extracting? Or, to put it more simply, when should you replace the ink, and thus, when do you need to buy more ink?

Today, the most modern printers can order toner when the levels are low. You don't need to predict it. You don't need to have excess on hand just in case. You don't even need to click an order button.

Apply the same concept to an entire production line. A manufacturer's production equipment is equipped with sensors that predict when a piece of machinery will need to go offline for maintenance.

That means fewer man-hours for inspections, less premature maintenance, less overdue maintenance and less downtime.

Procurement can help limit that downtime by ordering parts and supplies in advance, optimizing to minimize the risk of being caught short with the expenses associated with inventory.

This is possible because of machine data, which is exactly what it sounds like: data produced by machines doing their jobs. Right now, your home internet modem is producing data by the millisecond. Your car produces and stores data. Your Alexa generates its own data, and it records the data you create when it's listening in, which is all the time.

Imagine the sheer volume of data your household devices produce every day, and then imagine how much your organization's devices produce every hour.

Data in the Dark

This has created a problem people in tech call *dark data*: all the data an organization has but doesn't know it has plus all the data a company knows it has but isn't able to leverage.

Two-thirds of IT and business leaders told data analytics platform provider Splunk that half or more of their organization's data is dark.

Why? Because of the sheer volume of data compounded by other factors such as legacy devices that weren't designed with data collection and analytics in mind. All that data is lost value and opportunity.

Think again about that piece of production equipment able to predict its maintenance needs. If that equipment is connected to a purchasing system, not only can it predict when it will need maintenance, it can order the supplies itself.

Data Collected and Put to Work Today Will Lead to Possibilities We Haven't Thought of Yet

Machine Generates Data → Sensor Added to Machine Collect Data → Data Is Analyzed by Predictive Maintenance Software → Data Tells Purchasing System to Order Supplies

XYZ Leads to ??? ← Spend Analytics Identifies XYZ ← Purchase Record Is Stored in Purchasing Database ← System's Artificial Intelligence Chooses the Supplier

??? → ??? → ???

Source: Gartner
11012022_C

Transforming Records Management

Making You Digital-ready for 2023 and Beyond!

Top Eight Considerations for Modern Records Management

1 Secure indexing & archival

5 Well-defined retention & disposition policies

2 In-place records management

6 Comprehensive ready-to-use adaptors

3 Taxonomy & metadata management

7 Compliant with DoD 5015.02, ISO 15489, ISO 16175, VERS

4 Security & confidentiality

8 Cloud-native & support for large files

Request a Demo

About Newgen

Newgen is the leading provider of a unified digital transformation platform with native process automation, content services, and communication management 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.

That's known as a machine customer, which have existed for a while but are still in their infancy.

They're a form of robotic process automation driven by the Internet of Things. Theoretically, that purchasing system could utilise artificial intelligence to compare suppliers and make a selection optimising cost, speed and whatever other factors supply chain wants to include in that decision.

When that machine makes the purchase, the record and associated metadata would be entered alongside data from human-initiated purchases in your purchasing platform.

Future spend analysis may need to account for distinctions between human versus machine purchases, human versus machine vendor selection, etc.

That spend analysis could lead to who knows what changes in purchasing, contract management, inventory control, and so on.

The only limits are (1) how data generated by different activities are pooled to enable different analyses and (2) whether that data has been captured to be analysed at all.

Ask New Questions

What does this mean for supply chain leaders?
The analytics in data analytics gets all the glamour. We naturally think of the questions that analysis can answer, but our imaginations tend to be limited by what we can see.

We can see the data we have, so we ask questions of, and about, that data and make plans for what we'll do with the answers.

Data collection, though, gets scant attention, not just in supply chain but across functions and industries. Supply chain needs to get in the habit of asking some new questions of itself and especially of its partners in the business, where the vast majority of data is generated:

- What data are we generating?
- What data are we collecting?
- What are we doing with the data we have?
- What could we do with our dark data if only we could capture it?

The more accurate the assessment, the better supply chain leaders will be able to answer questions they're already asking all the time:

- How do we get the most ROI out of the technology we have?
- What should our technology roadmap look like?
- What should our technology strategy be?

This last question benefits especially from a more thorough accounting of what data the organization has at its disposal.

Strategy is the coordination of the ends and the means, a plan for how you use what you have to achieve what you want.

Data is a means, and the lack of visibility into what data exists limits what we perceive as possible and leads to missed opportunities to more easily achieve and capitalize on those possibilities.

Supply chain may not be able to solve the dark data problem, but it can prod those who can to make sure its own capabilities take the best possible advantage of their organization's data assets in its digitization journey.

Ryan Tandler is Director, Research, Gartner Supply Chain

What is the Future of Data Architecture?

A study into the Future of Data Architecture has revealed major discrepancies in how data architecture and management is viewed across organizations – with central data and analytics teams generally satisfied with the future viability of their data landscapes, but business users unconvinced that existing architecture is modern enough to meet constantly evolving business needs.

The report from the Business Application Research Centre (BARC) found that while 70% of business users believe that implemented data and analytics applications do not cover their current or future requirements, only 32% of central data and analytics teams share the same sentiment.

Furthermore, 52% of business users agree that existing data is not suitable for necessary business analysis, compared to only 36% of central data and analytics teams. The results show a clear disconnect between data and analytics teams and their key stakeholders – with business users unable to rely on trusted data for confident decision-making.

"As businesses increasingly focus on becoming more data-driven, they are being faced with huge volumes of data being generated at accelerated rates," said Emily Washington, Senior Vice President, Product Management at study sponsor Precisely.

"The report clearly indicates a growing need for organizations to ensure that existing data management and architecture can meet, and adapt to, the fast-changing needs of the modern business. If organizations are lacking a clear strategy for data integrity, they will quickly find that the data fuelling their most important decisions is inaccurate, inconsistent, and lacking vital context."

The research further revealed the key challenges highlighted by business managers, including extensibility of real or near-time requirements (41%), comprehensibility of the data landscape or architecture as a whole (39%), and flexibility of extended data requirements (32%). The main drivers for modernization are the optimization of existing data models and processes, migration to cloud platforms, and efforts to improve the quality of source data or data interfaces.

Despite facing challenges with rising volumes of disparate data sources, the research revealed that 50% of organizations are continuing to rely on data warehouses as a design paradigm when redesigning their data architectures. However, executives and business users criticize the fact that centralized approaches cannot prevent the emergence of further data silos. Therefore, companies are looking to improve their source data to streamline their data pipelines.

Download a copy of the full report here.

What is M365 Operational Governance and Do You Need It?

By Kayla Haskins, AvePoint

Your hard work is finally paying off: after months of planning, preparing, and piloting, you are finally ready to launch your new Microsoft 365 (M365), Microsoft Teams, SharePoint Online, or other collaboration platforms. Your team is on its way to better digital collaboration and streamlined productivity. Once it's implemented, you can finally relax, right?

Wrong. If you decide to lean back and put your feet up, leaving your collaboration spaces to fend for themselves, your newly minted environment might be at risk.

Now is the time to ensure the pristine environment you have created stays that way by implementing operational governance.

Operational governance, whether called that or not, is practiced by most organizations in all industries. Put simply, it is the rules that dictate business processes.

Microsoft 365 operational governance is no different – it's a set of policies that an organization follows throughout its day-to-day use of the platform.

These rules should be designed with the goal of standardizing Microsoft 365 operations across the organization and ensuring your digital workspaces are controlled and secured.

Why You Need Operational Governance

Rules are an important part of everyday life. They give us a framework of how to act and operate.

The same can be said about rules in our digital workplaces.

As companies utilize Microsoft 365 more, they need to implement operational governance to optimize their investment, sustain ongoing management, and more effectively manage the data lifecycle, empowering users and reducing IT burden in the process.

Consider these benefits:

■ **Control workspace creation:** How many collaboration workspaces has your organization created since implementing M365? 100? 1,000? 10,000? Of these workspaces, how many were necessary and actually used? Operational governance helps you establish rules around who can create a new workspace in Microsoft Teams, SharePoint, and Groups, limiting sprawl and helping you meet compliance standards.

■ **Manage workspace lifecycle:** Is every workspace in your M365 tenant active? Does each still have a clear owner, utility, and permissions? If you answered no to any of these questions, you're at risk of unnecessary storage costs, oversharing, and security threats. With governance, you can establish guidelines for recertification and attestation to ensure all workspaces are still active and intentional, and that all access is properly managed.

■ Protect your sensitive information: Do you know which of your workspaces have sensitive information? How about who has access to these workspaces with confidential information? If you're storing and sharing sensitive information in your Microsoft 365 tenant, you need proper rules and guidelines to protect it. With governance, you can establish policies around the types of workspaces that can store this information and what sort of users – external or otherwise – can be invited to the workspace.

Proper, effective operational governance will help you protect your digital workspaces and your investment in M365.

3 Steps to a Safer Microsoft 365 with Operational Governance

Instituting a new operational governance strategy can be a big undertaking, and it's difficult to know where to start. The path to effective governance begins with the optimization of your Microsoft 365 environment, which can be achieved in three simple steps:

1. Discovery – Understand and Clean Up Your Environment

You need to understand your M365 workspaces – where your team is working, what they're doing, and who owns what. The better you know them, the better you can build logical policies to manage them.

How to do it:

■ Create a workspace catalogue

■ Establish data ownership

■ Gain visibility over activity

2. Ongoing Management – A Sustainable Path Forward

You must create an ongoing management plan that simplifies, preserves, and protects your environment. As you develop this plan, be sure to consider more than

the needs of today; your organization will continue to grow and your environment will likely get more complex. Build a framework that is scalable and agile for long-term success.

How to do it:

■ Manage external sharing and guest users

■ Secure sensitive data

■ Preserve Microsoft Teams configurations

3. Lifecycle Management – Reduce Your Workload With Good Beginning and End of Life Practices

This can feel like a lot of work, especially for busy IT admins. Reduce your workload with self-service, automated, and delegated lifecycle management.

Solutions like AvePoint Cloud Governance automate operational governance, with self-service IT resources for provisioning, moving, or restructuring content, as well as lifecycle and permissions management.

How to do it:

■ Enable self-service provisioning

■ Require continuous workspace renewal by the owner

■ Automate end-of-life practices

Bottom Line

It may seem difficult to implement operational governance, both in a soon-to-be and already released tool, but as your organization continues to increase its activity in Microsoft 365, it will be impossible to protect your investment if you don't.

Without operational governance, your digital workspace will soon grow unmanageable and unruly. Without automated operational governance, IT will spend its days trying to get a handle on it. Avoid both while saving time and money with automated operational governance.
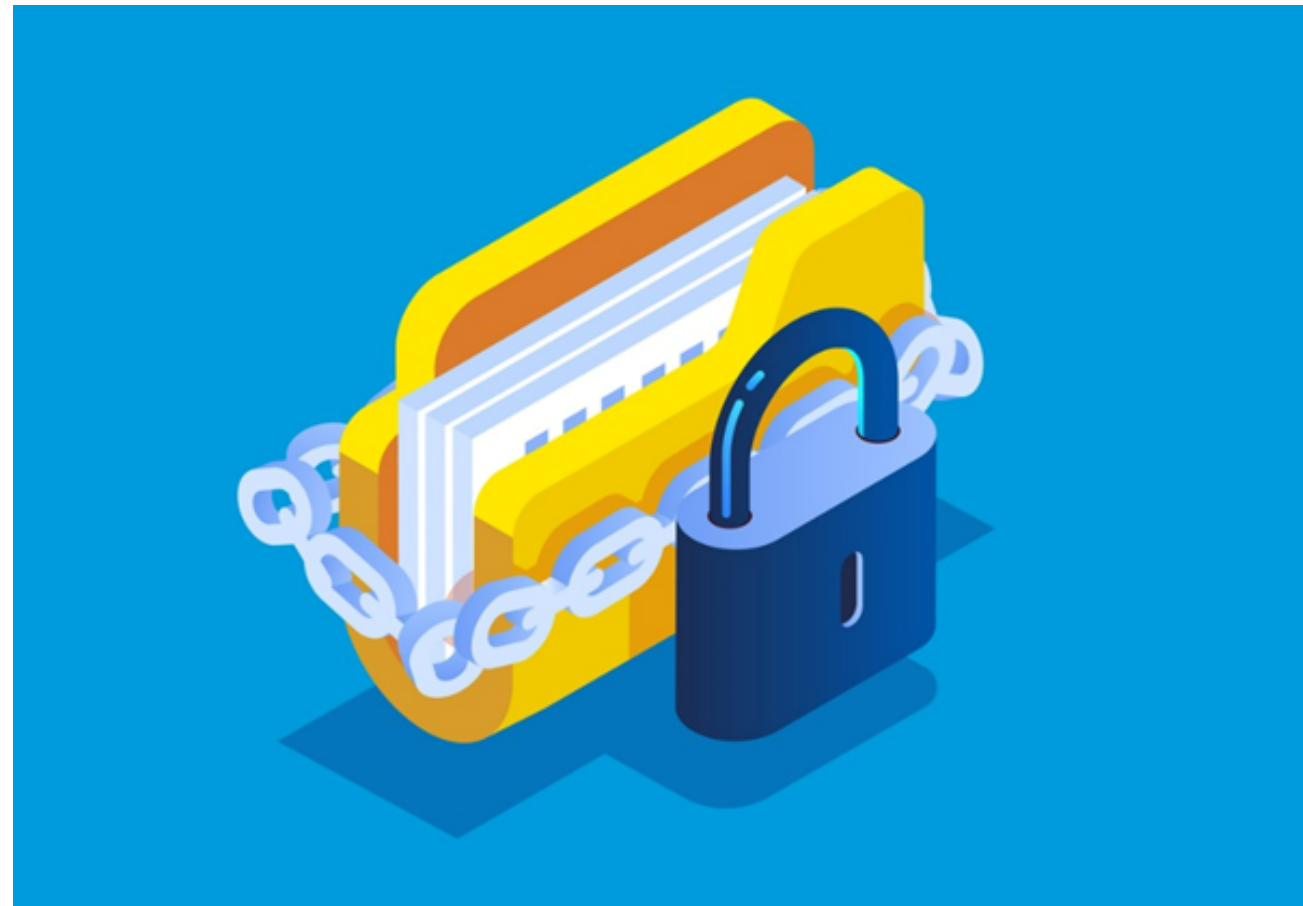
Find SharePoint info 10x Faster

CogniVision OneView is a new patented universal viewer for Microsoft SharePoint that is claimed to dramatically reduce the time to review and find information from search results - by a factor of ten.

"Search typically takes one to five seconds," said Basker Krishnan, Chief Executive Officer, CogniVision and a McKinsey alumnus.

"However, reviewing search results and finding specific information within documents is often tedious, time-consuming, and takes a long time,"

CogniVision claims OneView is the first major reinvention of document viewing and display technology in decades. It pairs technological advances with human capabilities to provide a better viewer interface for AI-driven enterprise content search.

Leveraging a person's innate pattern recognition and cognitive capabilities, CogniVision OneView enables users to find needed information extremely fast without having to read through pages of tedious text.

SharePoint offers options to display search results in either a list or modified list view to enhance reading.

However, the human brain operates in an analogue world, storing and recognising information as images rather than text.

A study by leading neuroscientists from MIT published in the journal Attention, Perception, and Psychophysics and referenced in MIT News found that "the human brain can process entire images that the eye sees for as little as 13 milliseconds."

Searching images is hundreds of times faster than reading text. Users can quickly refine relevance in SharePoint search when search results are displayed as thumbnail images in CogniVision, rather than textual summaries.

However, CogniVision is not just an image-centric thumbnail viewer.

CogniVision is a "display engine" offering patented document navigation using progressive adjacent display panels and page filtering to just the relevant pages within a document containing specific search keywords highlighted.

CogniVision's display and navigation system replicate the analogue user experience of working with paper files in finding information within digital documents from SharePoint's search results – at speeds it claims ten times faster than current viewers.

Improving the enterprise content search experience within SharePoint only requires using CogniVision as an alternate Viewer to accelerate the review process.

CogniVision has a minimal footprint. It does not alter anything within SharePoint. It requires no schema changes and will work with existing document repositories, without any changes to taxonomy or metadata.

Initial deployments have proven invaluable to banks and financial institutions and can address significant pain points in other enterprises.

CogniVision OneView is provided on a subscription basis and is available for deployment either on-premises, in a private cloud, or as a secure SaaS.

To request a demo, visit https://cognivision.com/
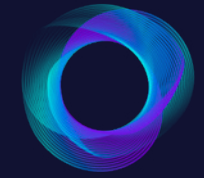
ENCOMPAAS

PRESENTED BY
PLATINUM PARTNER

INFORMOTION

Race ahead with next-gen AI

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

encompaas.cloud

Maintain the pace says Bain & Co.

Nearly 80% of companies that are considered as "digital disrupters" gained market share over the last two years, according to new research by Bain & Company. Bain's fifth annual Benchmarking Survey of Corporate Digital Transformation shows that digital disrupters put "digital" at the very top of their agendas, yet even they are having to adapt to a fresh wave of emerging technologies that are enabling new competitors and business models.

Of the 1,400 business leaders across 13 countries that Bain surveyed, 70% of them said they are experiencing significant digital disruption, and 85% of business leaders believe disruption will either maintain its pace, or accelerate, over the next five years. With no company invulnerable, Bain is explaining the ways disrupters stand out and reminding executives of the six digital transformation challenges that are likely to determine future winners and losers.

"The astonishing outperformance of tech stocks may have eased, but don't expect a corresponding slowdown in digital disruption," said James Anderson, partner in Bain's London office and leader in Bain's Vector capability.

"In fact, we are seeing a fresh wave of disruption today driven by new business models and emerging technologies such as deep-learning artificial intelligence, the metaverse, Web3, advanced robotics, and connected devices supported by edge computing and 5G networks."

According to Bain, disrupters believe we are living through a profound shift in how business operates; when compared to what is known as "digital chasers," disrupters are twice as likely to say that digital technologies will radically alter their sector. Bain found that disrupters are:

■ **Talent magnets:** Disrupters are eight times more likely than late digital adopters to attract and retain the right people, with the right skills, in the right roles.

■ **Innovative:** Nearly two-thirds of disrupters are building "Engine 2" digital businesses outside their core as a response to both opportunity and disruption; another source of resilience and growth.

■ **Attentive to environmental, social, and governance (ESG) progress:** Most disrupters view ESG initiatives as being intertwined with their digital activity; about 60% consider ESG a primary criterion in the prioritization of their digital initiatives, and about 90% clearly track the role of digital initiatives in ESG progress.

Six Key Digital Transformation Challenges

Although 97% of the executives Bain surveyed indicated that digital transformation is a priority, fewer than 20% of them believe that their company has achieved more than 80% of their digital transformation goals. Bain found that there are six priority areas that companies should focus on:

■ **Commit to the cause:** More than 80% of early-stage transformers said their top-level commitment to change hadn't yet cascaded through the ranks or been fully codified into compensation and career management.

■ **Refactor tech architecture:** Accelerate the shift to cloud technologies and invest in a modular and flexible enterprise technology stack.

■ **Extract full value from data:** Embed repeatable processes for scaling advanced analytics; deploy artificial intelligence (AI) and machine learning at scale.

■ **Make Agile the norm:** Ditch siloed operating models and ensure that Agile and other new ways of working extend beyond the IT department.

■ **Ignite innovation:** Rekindle a risk-taking culture; only 1 in 10 early-stage transformers currently feel they have the risk-taking culture (and effective risk management) that is commonplace at disrupters.

■ **Become a talent magnet:** Invest more in employee training, give employees room to pursue experimental side projects and search internally for "digital dreamers".

NSW adds mandatory breach notification

NSW is set to become the first state or territory in Australia to have a mandatory notification scheme for its government agencies to respond to breaches of NSW citizens' personal data.

Attorney General Mark Speakman said the Privacy and Personal Information Protection Amendment Bill 2022, introduced by the NSW Government into Parliament, would create new standards of accountability and transparency for government bodies and introduce a mandatory notification of data breach scheme in NSW.

"Every day, the people of NSW offer their personal information to government agencies, which is a significant undertaking of trust," Mr Speakman said.

"In doing so, they enable the government to provide them with quality, connected services, and the information required to continually improve these services to best meet their needs.

"In return, the government has a responsibility to effectively and proactively protect and respect that personal information.

"Once passed, this new law will provide consistency across public sector agencies by making it mandatory for public sector agencies to notify the Privacy Commissioner and those impacted by a data breach involving personal information which is likely to result in serious harm.

"Agencies will also have to satisfy a number of data management requirements, including making reasonable attempts to mitigate the harm done by a data breach, maintaining an internal data breach incident register, and have a publicly accessible data breach policy."

Minister for Customer Service and Digital Government Victor Dominello said the NSW Government has taken a number of steps to protect customer privacy and personal information.

"The protection of people's privacy is crucial to ensure public confidence in NSW Government agencies. It is imperative that the highest standards of privacy and security prevail to safeguard data," Mr Dominello said.

"The NSW Government has made significant investments to protect citizens' data, including funding $A315 million to bolster our cyber systems and by launching ID Support NSW to help those impacted by identify theft.

"The bill will provide greater certainty for the public and government agencies regarding personal information and the steps required if a data breach occurs.

The scheme would apply to all NSW 'public sector agencies' as defined in the Privacy and Personal Information Protection Act 1998, including all NSW agencies and departments, statutory authorities, local councils, bodies whose accounts are subject to the Auditor General and some universities.

The bill will also expand the Privacy and Personal Information Protection Act 1998, including the new scheme, to cover all NSW state-owned corporations not subject to Commonwealth privacy law

Structured Data drives IT Spend: IDC

The workload driving the largest share of enterprise IT infrastructure spending in the first half of 2022 (1H22) was Structured Databases/Data Management, according to analyst firm International Data Corporation (IDC).

Organizations spent $US6.3 billion on compute and storage infrastructure to support this workload in 1H22, which represents 8.5% of the market total. This is also one of the most mature enterprise workloads with 2.2% growth year over year.

Unstructured Databases and AI Lifecycle were two workloads experiencing the highest growth in hardware infrastructure demand with spending growing at 52.9% and 40.2% respectively from 1H21.

Unstructured Databases are still one of the smallest consumers of compute and storage infrastructure at $US2.3 billion, while AI Lifecycle workload, which includes platforms mostly related to AI training tasks, accounted for $US4.4 billion.

The majority of workloads map to secondary or functional software markets while several, including Content Delivery and Digital Services, have no equivalent in the software market structure.

Workloads are further consolidated into seven workload categories, which include: Application Development & Testing, Business Applications, Data Management, Digital Services, Email/Collaborative & Content Applications, Infrastructure, and Technical Applications.

In 2022, the Data Management workload category, which includes five workloads – AI Lifecycle, Business Intelligence and Analytics, Structured Database/ Data Management, Text and Media Analytics, and Unstructured Database – will be the largest with $US41.1 billion in spending on compute and storage infrastructure products.

It will remain the largest throughout the forecast period with a five-year compound annual growth rate (CAGR) of 9% and reaching $US56.3 billion in infrastructure spending in 2026.

Most of the growth in this category will come from the fastest growing workloads related to unstructured data and artificial intelligence.

Data Management will also be the fastest growing category of infrastructure spending in shared cloud and one of the fastest in dedicated environments at 15.9% CAGR and $US23.5 billion spending in 2026 in shared, and 5.3% CAGR and $US32.8 billion in 2026 in dedicated environments (this includes dedicated cloud and non-cloud infrastructure deployments).

A Smarter Way to Modernise Legacy Data and Systems

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. atalynx is currently working with a large

NSW government cluster on a 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.

With over 4 billion transactions and millions of files already successfully migrated, 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.

(Continued over)

Features of the Datalynx DMS Phoenix legacy migration solution.

A Smarter Way to Modernise Legacy Data and Systems

"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 disproportionally 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

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. 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/

Kodak alaris

Guide to Handwritten text Extraction and Hyperautomation

By Walter Lee, Ephesoft

Capturing handwritten data has been a source of hardship for most organizations, which is why we're covering the top five factors to consider when working on any hyperautomation initiative that touches handwritten data and documents. With that in mind, Ephesoft has some exciting new capabilities and best-in-class accuracy rates that are the highest in the industry for cursive handwriting.

Anyone who thinks handwritten data only exists on fixed, standardized forms has never really dug into a government process or worked on a non-fillable, online form for an application in the commercial industry. Form variations and versions, poor scan quality, fax conversions and more can all impact the layout of information that exists on a form. When those factors come into play, templatized data extraction just doesn't cut it.

Extrapolating from an AIIM survey of about 300 respondents, more than a quarter of all organizations use forms and documents that contain handprint as a part of their key business processes. This includes processes that have been automated – or attempted to be automated – with tools like RPA systems and BPM applications.

- 26% of organizations rely on forms and documents with handprinted data for key business processes

- 42% of organizations that use forms for information and application submissions receive at least half of those forms with handprint data

Handprint-submitted information is the norm, rather than the exception for public and private sector organizations.

Bottlenecks

The public sector is one of the biggest culprits of handwritten data process bottlenecks. Where constituents are concerned, most government functions involve form submissions. Whether we're looking at federal departments or state and local agencies, budget and technology adoption are definitely factors.

Operational budgets are always in jeopardy, and even more so after the fallout of the COVID-19 pandemic. Then, think about processes like permit applications, information requests, benefits applications, tax deferrals and more that need to serve across all socio-economic classes. With limited staff, furloughs and an overall diminished work capacity, government agencies are going to be inundated with a manual data entry backlog for all these constituent-driven requests.

In addition, new privacy laws add complexity to the process by requiring the ability to redact Personally Identifiable Information (PII) on documents, including handwritten forms.

However, the commercial world is not immune to the informational black hole that is handprint data. For example, insurance companies accept claim forms from policyholders submitted with handwriting. Or,

remember every time you've been to your primary physician and had to fill out the "updated insurance and contact information form" in the waiting room with all the other coughing, miserable-looking fellow patients. All of that medical information is crucial and must be maintained in a digital, searchable and actionable format.

Intelligent Document Processing Platform

Within Ephesoft Transact, content moves from the point of actual document capture or ingestion – either as a part of an external system's workflow or a standalone action – through to the point at which processed documents and their associated metadata and index values are routed to their final destination or the next step in the business process.

What's new and exciting for Transact is what we've added more data extraction capabilities. First, we have a new advanced hOCR Plugin, which provides capability for handprint, cursive and machine print extraction.

Second, Transact's handwriting recognition/Intelligent Character Recognition (ICR) feature builds on the bounded-block printing (OCR) along with checkbox/Optical Mark Recognition (OMR) extraction tools launched in a previous release. Together, they offer a highly comprehensive, reliable yet fast and easy way for users to extract handprint values from documents and detect signature or checkbox filled areas.

The technology reads both printed and cursive writing at an accuracy up to 88% out-of-the-box, even handwritings that are not easily legible by human review. Users can use a scanner, tablet, phone or other means to scan the document or form.

ICR converts images of handprinted text to an editable and/or searchable file format. Traditional ICR engines range in accuracy and server requirements, and there are new, cloud-based and machine learning-trained ICR engines hitting the market on a fairly regular basis. OMR captures data from form elements such as checkboxes and multiple-choice bubbles.

5 Factors for a Successful Digital Transformation Project

According to a PTC report on digital transformation, executives report that the key benefits of these

initiatives are improved operational efficiency – key for shrinking IT budgets, faster time to market with new products and services and a closing gap between customer expectations and company delivery.

And for most organizations, handprint data is inextricably linked to a holistic approach to hyperautomation. So, let's look at the top five elements of a successful digital transformation project where handprint data is concerned.

1. Document Source: First, consider the source of your content. How are you receiving documents with handprint data? This will vary by industry and process, but it's important to the overall workflow and success or accuracy rate of your automated data extraction project. Are documents coming in as faxes, emails, to a centralized location as snail mail, or are pictures of handprinted forms and letters being uploaded to a company portal from a snapshot on a mobile device? These methods of getting formerly paper documents into your organization's key information systems should be aggregated and routed through a centralized process to ensure uniformity and optimize your document-specific business processes. Fortunately, with an application like Transact, we support ingestion of documents from all these sources.

2. Security: The second factor to consider for a successful digital transformation that includes documents with handprint are the security requirements of your organization or industry. Are there security requirements specific to accessing or integrating with public cloud applications?

On the other hand, Transact can be installed on-premises or leveraged in a private cloud. There's no need to send sensitive information or customer data outside of your organization's network and firewalls to take advantage of the rich capabilities of ICR.

3. Complexity and Variation: Transact utilizes key-value (or KV) pairs to identify and extract information from unstructured documents. This means the application looks for a particular pattern of text representing the key, and then finds the corresponding value based on the desired extraction field value's relationship to the key. This approach eliminates the need to configure coordinate-based templates to extract data and can be applied to handprint data.

Some handwriting solutions impose character limits or a per field-basis cost that can be inflexible or costly. However, with Transact, OpenText Capture Recognition Engine (formerly Recostar) OCR engine as well as advanced hOCR Plugin (powered by Google Vision or Azure (coming late 2022) in the product utilizing a whole-page OCR approach, there's a minimal cost to you or your clients for using handprint extraction, either on a per field or per page basis.

Many capture products will require that you create fixed forms or coordinate-based templates in order to extract handprint data from scanned documents. If you have a project where you only have a single form and a single variation of that form, this might not be a big deal from a project configuration and management perspective. But, what if there are historical variations of that form accessible to the public? Maybe the form gets updated each year or expanded. What if – in the government space – the form varies by state?

Now, you have to consider the document source and the impact that could have on the actual layout of the documents. If a form is captured on a mobile device, that could impact the aspect ratio of the digital image.

When physical documents are scanned, they could be skewed or laid incorrectly on a scanner bed, again, impacting the actual zonal coordinates of a document. The same holds true for distortions that take place when a document is faxed. If you're relying on a fixed area of a page to find handprinted information, your ability to scale in any true digital transformation project is going to be limited on the time or cost that must be dedicated to design each coordinate-based template.

That's why it is important to find a solution that can balance the level of predictability and extraction accuracy you require with the costs to accommodate the variations of forms you need to process, while still meeting your timelines. The good news is that Transact provides a comprehensive and flexible array of tools for your use case to find that balance. Everything from traditional fixed form extraction to more advanced ruleless AI entity extraction is included and works seamlessly with our handwriting solution.

4. Signature Detection: The fourth factor for a successful digital transformation project where handprint and handwriting are involved is interacting with and managing documents with signatures. Signature detection can be a manually intensive, time-consuming step that slows application processing across all industries.

Take the mortgage industry, for example. There is typically a large packet of loan-related documents that range in page length and complexity. Validating that any borrower and co-borrower have signed is crucial. But when a human being enters the mix, they spend time flipping through pages to find that one field and give the packet the green light. Automating this step saves time and therefore money in expediting the loan process.

Another example is the background investigation processes. Or, human resource employee onboarding. Every industry and every company has some type of application process where people are required to sign documents, forms or letters of explanation. And putting some automated validation checks in place for these ubiquitous tasks has enormous time-saving potential. I believe it should be a key element of digital transformation initiatives.

5. OCR, ICR or OMR – Extract what you need: Lastly, just make sure you understand whether relevant data is machine printed, handwritten, presented with optical marks like checkboxes or radio toggles, or in some combination thereof. Sometimes there are project requests where a company or agency wants to have every field on a form or piece of information on a document extracted. But when I ask why... when I ask about the purpose of the information downstream, there is no answer. Limit the scope of your project to include relevant data only – whether that data is a signature on a contract, a checkbox on a form, machine or handprinted piece of information – and your project timeline and cost of implementation will benefit.

In summary, items to add to your digital transformation initiative play list are: consider your document sources, look into security requirements for data transmission out of your organization's network or firewall, look for the complexity and variety of forms and documents, single out workflows that require signature validation, and get a solid understanding of the OCR, ICR and OMR data extraction requirements as they relate to the business process at hand.

For more information, click here or watch the webinar replay here.

Why cybersecurity continues to be a problem for industry

Three recent cyber attacks resulted in identity leaks that have sent ripples around Australia. Has the triple-A of cyber security (Authentication, Authorisation and Accounting) failed?

In the recent MyDeal.com.au incident, early reports suggest that a compromised credential, most likely related to elevated users, was used to access a database storing user information. The attack led to the scrambling of 2.2 million customers data, which included email addresses, full names, phone numbers, delivery addresses and some customers' birthdates.

In an interview with Channel 9 News, Professor Sanjay Jha, Chief Scientist for UNSW Institute for Cybersecurity (IFCYBER), said: "… the breach raises serious concerns for the end user's confidence in using online services and poses a serious challenge for the industry".

"Compromised credentials should not provide easy access to malicious actors when multi-factor authentication (MFA) is in place," he added.

"You would expect more stringent authorisation and access control and network partitioning to protect these critical assets."

Following basic practices on Cyber Security Guidelines listed by the Australian Cyber Security Centre can help a business protect their systems from cyber threats.

Dr Arash Shaghaghi, a Senior Lecturer in Cybersecurity from the UNSW School of Computer Science and Engineering and UNSW Institute for Cybersecurity, says it's evident from the recent attacks that some industries are not adopting the latest research on cybersecurity fast enough.

"Users' data is collected by various services without any control from the end user, and often the data collection to join these services is excessive – leaving end users vulnerable and with limited options when a serious breach occurs," he says.

"Other parts of the world are investing heavily in technological measures such as Self-sovereign identity (SSI), where users would have better control over who has access to what part of user identity and other information.

"SSI gives individuals control over the information they use to prove who they are to websites, services and applications across the web.

"We need to enhance investment in practical research and think of measures that facilitate the adoption of the latest technologies to reinforce our resiliency against the growing number of attacks targeting Australia."

Optus

Last month, 10 million Optus customers experienced a similar fate when cyber criminals hacked into the system, stealing personal details such as passport ID and licence numbers. It was reported the breach suggests that an open port without authentication for testing purposes was left in the production version.

Unfortunately, these problems are well-known to the industry, says Prof. Jha.

"About five years ago, we were white boxing early versions of Philip Hue bulbs and Phillip Hue Bridge. We found that you could control these devices through such open ports," he says.

"This was reported to the company who fixed the problem in their future version. A simple penetration testing of servers before deployment could have potentially made such attacks difficult, if not impossible."

Prof. Jha is also concerned about the state of risk assessment and authorisation processes across the industry and says further stringent penalties for negligence would go a long way.

Often these processes are a box-ticking exercise in an Excel spreadsheet, and many conducting these tasks don't have adequate background in cybersecurity, he says.

"This re-emphasises the need for quality education along with more research in quality tools to improve these processes," says Prof. Jha.

"My team is working on such tools for a Distributed Energy Resource Management Security project at UNSW funded by Cyber Security Cooperative Research Centre.

"Cyber Security is a cat-and-mouse game. Researchers and industry experts need to come together in Australia and work closely to build stronger and more resilient capabilities that help safeguard businesses and users in today's world of cyber war and cyber terrorism.

"We need to regain the community's confidence in our cyber capabilities."

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

ABBYY powers intelligent automation. The company reimagines the way people work and how companies accelerate business by delivering the intelligence that fuels automation platforms. Its solutions transform enterprise data and empower organizations with the insights needed to work smarter and faster. ABBYY helps more than 5,000 companies globally, including many of the Fortune 500, to drive significant impact where it matters most: customer experience, profitability, and competitive advantage. ABBYY is a US-based global company with offices in 14 countries. For more information, please visit www.abbyy.com and follow ABBYY on LinkedIn, Twitter and Facebook.

www.abbyy.com| sales@abbyy.com.au | 02 9004 7401

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

ELO Digital is a truly global ECM company with Australian expertise! Servicing more than 1,000,000 users in over 40 countries, ELO has become the natural choice in ECM. With more than 30,000 live projects the ELO product suite provides process enhancements, stability and compliance. The Australian-based subsidiary engages with Certified Business Partners to deliver 1st class solutions for Records Management, Document Management, Accounts Payable processing, Workflow Management, Mobile access and much more. ELO provides consultancy, development and support services from its offices in Australia – we are local and global. ELO's solutions can be deployed on-site, in the cloud or as a hybrid solution either as a CAPEX or OPEX such as subscriptions, SaaS. ELO is fully scalable from as little as 5 users to large enterprises in excess of 10,000 users. ELO is a Federal, State and Local Government supplier compliant with Australian standards as well as GDPR and FDA requirements.

www.elo.com/en-au | eloinfo@elodigital.com.au | 02 9460 0406

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

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

Supply Chain digitisation

Inspectorio has introduced new document and collaboration technology that eliminates paper processes, streamlines workflows, and ensures regulatory compliance for the supply chain

Inspectorio DocuFlow allows supply chain partners to automate and streamline document management workflows, collaborate with users both inside and outside the boundaries of your organization, and ensure proper document control.

It eliminates paper processes and also supports regulatory compliance through strict controls of document versioning, approval, sharing, and storage. Inspectorio's new document management platform streamlines the management of business-critical documents, automating the creation and review process, including tracking who has approved paperwork and ensuring the right documents are shared with the right people at the right time.

As compliance requirements increase, document control becomes a more high-risk focal point for supply chains. Research shows that 92% of executives risk losing documents in their email, and 83% of employees must recreate documents that go missing in their company's network.

Inspectorio DocuFlow addresses these inefficiencies by reducing manual work and streamlining document management workflows, automating the creation, review, and approval of documents, and tracking the document's chain of custody. This helps companies abide by compliance requirements, ensuring all document workflows are executed according to schedule and governed properly.

Inspectorio helps digitise quality, compliance, and production tracking and removes data silos by bringing all production chain activities and data into one platform. Inspectorio's solutions allow realtime data analysis and reporting across all these activities, enabling organizations to have a predictive rather than reactive approach.

https://inspectorio.com/

Self-service tools for Unstructured Data

The latest release of Komprise Intelligent Data Management introduces self-service features for line of business (LOB) IT, analytics and research teams.

Now, central IT can authorize departmental end users to interactively monitor usage metrics, data trends, tag and search data and identify datasets for analytics, tiering and deletion.

These new capabilities bridge the longstanding gap between IT's focus on optimizing storage infrastructure and costs and users' focus on finding and operating on the right data sets.

The new release builds upon Komprise Smart Data Workflows, a new capability which allows IT teams to automate the process of tagging and discovering relevant file and object data across hybrid data storage silos and feeding the right data to cloud services.

The new Deep Analytics user profile gives authorized users read-only access to view their own data characteristics such as number, type and age of files and collaborate with IT on data management, delivering compliance and storage savings benefits while giving data owners greater control of their data.

Possible applications include:

■**Showback:** Authorized departmental users can monitor and understand their data usage (examples: how many and what type of files, where stored and biggest consumers) in an interactive dashboard and create queries to get real-time visibility and manage costs, rather than ask IT to create static reports.

■**For example:** A new research initiative at a life-sciences organization requires 100TB of data storage and the project lead needs to work with IT to move older file shares to cloud storage and free up space.

■**User-driven tagging:** Users can enrich data with additional metadata tags to facilitate easier search and data management actions such as archival storage or compliance and legal hold. For example: the HR director needs to ensure that all files with employee PII data are tagged so that information is properly and securely stored for privacy requirements and searchable for deletion when the employee leaves. Read this post on a sample data workflow for handling PII using Komprise and Amazon Macie.

■**User-driven tiering and data mobility:** Authorized users can identify data sets with certain characteristics (such as project or age) to move to cloud storage or other secondary storage for more cost-effective data management or research initiatives. For example: All files related to a project need to be copied to the cloud for data analytics. The entire workflow between users and IT is automated via Komprise.

www.komprise.com

Gadens launches Cyber Attack toolkit

National law firm Gadens has released a cyber incident manager to navigate the legal reporting obligations of businesses during a cyber breach. The digital workflow tool steps a user through issues and ramifications, reducing the complexity and time required to investigate and report potential cyber incidents.

2022 has already seen several high-profile companies being hit with cyber attacks where customer data has been breached, and cyber ransoms have been demanded.

Many organisations have a cyber incident plan in place, but important time-critical legal compliance can be at risk of getting overlooked during a cyber incident.

The Gadens Cyber Incident Manager is a cloud-based solution powered by Lawcadia's technology. It streamlines the information collation, assessment and reporting process of potential cyber incidents in one online platform, allowing companies to ensure defensible, timely and cost-effective compliance with multiple pieces of cyber incident relevant legislation and standards including the Security of Critical Infrastructure Act (the SOCI Act).

Gadens Cyber Incident Manager incorporates regulatory reporting requirements, so when a cyber incident has occurred, it is easy to immediately request legal advice and preparation of the regulatory report, if required.

The workflow tool also provides practical guidance on what to do next within sharp statutory timeframes, dramatically reducing the risk of legal ramifications for organisations and their senior accountable employees.

Powered by Australian legal technology company Lawcadia, the Gadens Cyber Incident Manager is available off-the-shelf, utilising their intelligent and secure platform engine – Lawcadia Intelligence – all supported by an ISO 27001 certified information security management system.

Gadens Director Robert Feldman said, "When you are in the middle of a cyber incident, there are a lot of moving parts, and someone needs to manage your legal compliance."

"One of the biggest issues is a complicated and overlapping patchwork of legislation and other standards – some of which have very tight reporting timeframes," he said.

"The tool will help organisations navigate that patchwork and keep them on track to meet their legal compliance obligations while they get on with everything else involved in managing the incident," said Mr Feldman.

Lawcadia founder and chief executive officer Warwick Walsh said he is excited by the continuation of its innovation partnership with Gadens.

"Gadens has been able to continually leverage innovation to solve clients' pain points firstly with the Gadens Breach Manager for financial services and now with the Gadens Cyber Incident Manager, a timely and important tool for the current climate", he said.

More information about the Gadens Cyber Incident Manager, including an upcoming webinar, is available here.

EzeScan Link4 team up on e-invoicing

EzeScan has announced an integration with Link4 to allow for the processing of e-invoices within a traditional invoice capture workflow. The integration with PEPPOL access provider Link4 allows for EzeScan to process any type of incoming invoices while eliminating the need to manually verify invoicing details, resulting in a more automation-driven process.

Existing users of EzeScan Invoice Data Capture solutions will simply need a Link4 connection to begin receiving e-invoices instantly, and at no additional EzeScan module licensing costs.

In 2019, the Australian Government adopted the PEPPOL framework and established the ATO as the Australian PEPPOL Authority to develop and administer the framework in Australia.

To use e-invoicing, a government agency or business needs to connect to the PEPPOL network through an authorised access point, such as Link4.

While the move to PEPPOL e-invoicing in Australia and New Zealand is at a very early phase, the Link4 Access Point combined with EzeScan enables organisations to manage the inflow of PEPPOL and ongoing emailed PDF/Paper invoices in the same workflow.

Mike Kirkby, CEO at EzeScan, said, "Many organisations want an invoice capture system that provides one invoice stream, that's where EzeScan comes in. We don't care whether incoming invoices are hard copy scans, e-invoices, or emailed PDF attachments."

"EzeScan can provide an extra level of validation and security for e-invoices by validating invoice data and flagging any changes in supplier details. Our dashboard also provides overall visibility of key invoice processing metrics including the number of invoices received and the types of invoices.

"Overall, this automation will simplify your Accounts Payable workflow while reducing the time you spend managing accounts, decreasing your overheads and ensuring a secure invoicing process," said Kirkby.

"This arrangement between EzeScan and Link4 provides additional safety and security measures for any size business," noted Robin Sands, Link4 CEO. "We look forward to supporting more Australians using their current invoice processing channels."

https://www.ezescan.com/solutions/invoice-processing-automation

IBM 'air-gapped' Tape Library
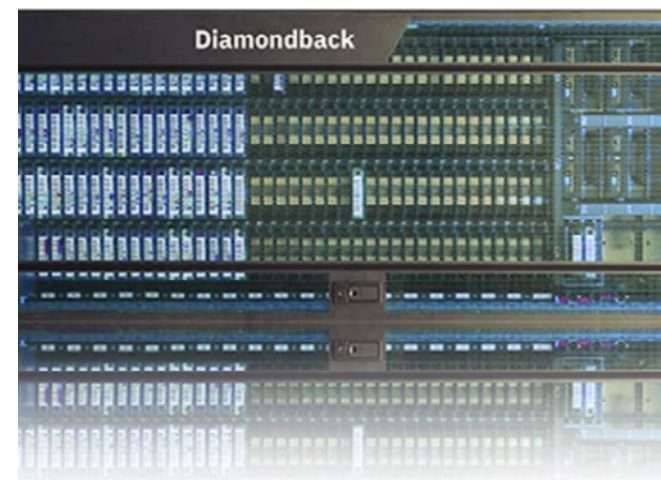
The IBM Diamondback Tape Library is a new high-density archival storage solution that is physically air-gapped to help protect against ransomware and other cyber threats in hybrid cloud environments.

IBM Diamondback is for organizations needing to securely store hundreds of petabytes of data, both traditional and "new wave" hyperscalers – global enterprises aggregating massive customer data sets. It provides long-term storage and is designed to provide significantly smaller carbon footprint compared to flash or disk storage, and with a lower total cost of ownership.

"With data breaches and ransomware attacks now a constant threat, we are seeing hyperscale enterprises increasingly turning to the data resilience provided by IBM Tape solutions," said Scott Baker, Vice President and Chief Marketing Officer of IBM Storage.

IBM claims Tape is approximately one-quarter the total cost of spinning disk storage and public cloud archival services, creating a significant cost advantage.

IBM Diamondback provides cost-effective archival storage for the massive capacity demand of the zettabyte era, supporting vertical markets such as big data, analytics, cloud storage services, the internet of things, healthcare, and life sciences.

These organizations typically generate enormous amounts of high-value unstructured data, much of which is stored as archives awaiting future reference, and can often benefit from an active archive implementation leveraging high capacity, low-cost tape systems.

https://www.ibm.com/products/diamondback-tape-library

Syntex automated document processing

The application formerly known as SharePoint Syntex has been rebranded as Microsoft Syntex and now offers a new set of AI capabilities to automate content creation, indexing, and discovery. Syntex offers backup, archiving, analytics and management tools for documents as well as a viewer to add annotations and redactions to files.

The new release of Microsoft Syntex enables organizations to archive entire site collections within the Microsoft 365 ecosystem, allowing organizations to index the content for eDiscovery and compliance purposes. Microsoft Syntex now gives IT administrators visibility into sharing links and sensitive files in SharePoint sites, with the ability to then initiate reviews by those responsible for the sites that are housing these files. Syntex can automate content-based workflows such as e-signatures, supports annotations and redactions, and integrates tightly with Microsoft Search.

Writing on the Microsoft blog, Seth Patton, General Manager, Microsoft 365, said, "Syntex services offers new ways to create content-centric apps and processes. Many Syntex services, such as content assembly and structured document processing models, are tightly coupled to Microsoft Power Automate and Microsoft Power Platform. Syntex also lets you use AI Builder models for structured and freeform document processing alongside unstructured document models.

"Most critical line of business applications consumes and generates lots of content. But too often, those content stores are siloed and disconnected from Microsoft 365. Most content begins in Microsoft 365 - statements of work, for example - but once uploaded to your accounting system, they get disconnected from your cloud. Wouldn't it be great to use the content platform you already have?

"Next year, we'll roll out new business app integration plugins, allowing you to use Microsoft 365 as the content engine for critical line of business systems. Today, these systems all work with and generate thousands of pieces of content, but often require a disconnected repository outside of Microsoft 365, or even storage within the line of business system's expensive database storage, for storing the content. Syntex will allow you to use Microsoft 365 as the content platform for Dynamics 365 and many other critical line of business applications from third parties."

AvePoint announced it is one of the select featured partners for the launch of Microsoft Syntex, which uses advancements in cloud computing and artificial intelligence to transform how content is created, processed and discovered in Microsoft 365.

"We're excited about the interoperability between AvePoint products and Syntex to enhance, connect and manage information in SharePoint and OneDrive," said John Peluso, Chief Product Officer, AvePoint.

Workflow for Jira, Slack, Teams users

To support cross-ecosystem workflows between Atlassian and the Slack and Microsoft communities, Appfire has announced its strategic acquisition of Nextup.ai, a software technology company that provides collaboration software solutions for Slack and Microsoft Teams.

The portfolio of apps from Nextup.ai empowers teams across enterprises to work more efficiently through the reduction of context switching. This acquisition allows them to have productive conversations without disruptions, ensuring access to multiple tools through one application. Seamless collaboration becomes the primary focus, giving teams the support needed to successfully work wherever and however they prefer.

In today's hybrid-remote workforce, seamless collaboration is key for both cloud and on-prem environments across organizations of any size. With IT and development teams under immense pressure to deliver results faster and under tight deadlines, the workflow needs to be streamlined and tools need to communicate with each other. Nextup.ai and Appfire solutions live at the intersection of planning and delivery where all work can be conducted smoothly in one place, reducing waste in the workflow process.

Through integrations with Slack and Microsoft Teams, Appfire customers using the Atlassian suite will now have the ability to streamline ticket submissions, capture and share communication threads and create more efficient daily scrum meetings.

"As work evolves in organizations, critical workflows continue to occur in chat programs like Slack and Microsoft Teams. To exist at the heartbeat of a company's processes with AI-powered applications is an advantageous place to be because it enables us to see how work truly flows and build products to help organizations reduce silos," said Randall Ward, co-founder and CEO of Appfire.

"Together with Nextup.ai, we are committed to empowering teams everywhere to continue focusing on work that really matters."

"The tech stack integration of our solutions will benefit both Appfire and Nextup.ai customers by heightening connectivity, building up machine learning models, and understanding behaviours that work to provide ultimate chat first workflows."

Over the past year, Nextup.ai has released four apps, including new solutions for ITSM, documentation, meetings and sales teams to further integrate Slack and Microsoft Teams into core workflows.

The suite of apps from Nextup.ai include:

- Integration+ leading two-way integration for Jira that allows teams to create, update, edit and monitor Jira issues without switching context.

- Helpdesk+ elevates internal support by creating a two-way integration between Jira Service Management and chat to resolve issues faster with automation, knowledge base integration and easy approvals.

- Docs+ powerful two-way integration for Confluence that lets you create, share, and update company knowledge directly in chats.

- Meeting+ integrates scrum meetings with Jira to automatically help your team remember what they worked on, clean the board and run faster meetings with just a few clicks.

- Deals+ connects your conversations with your CRM and enables your team to track customer relationships and close deals faster.

https://appfire.com/

Astera Data now includes AI Capture

The version 10 release of the Astera Data Platform includes AI Capture, a new AI-powered data extraction feature in the ReportMiner module.

Astera ReportMiner is part of the Astera Data Platform that utilizes template-based extraction to help business users structure large volumes of unstructured data in a code-free environment.

The availability of AI Capture significantly reduces the efforts needed to create reusable data extraction templates. The new feature automatically detects and captures data regions and fields using natural language processing algorithms and table detection.

Users can now leverage this AI-powered data extraction process to create templates with just one click and capture unstructured data in seconds.

Astera's COO, Jay Mishra, said: "AI-driven opportunities in data extraction have paved the way for enterprises to simplify and streamline data processing.

"Automation helps businesses process large volumes of documents and perform analytics for intelligent decision-making and business growth.

"AI Capture accelerates the data extraction process and fast-tracks the business intelligence initiatives of our clients."

In addition to the AI Capture, Astera 10.0 update comes with numerous improvements and new changes.

There have been several UI enhancements to provide a more seamless user experience.

Furthermore, users can now take advantage of Astera's native connectivity to effortlessly access cloud storage destinations, including Amazon S3 and Microsoft Azure Blob.
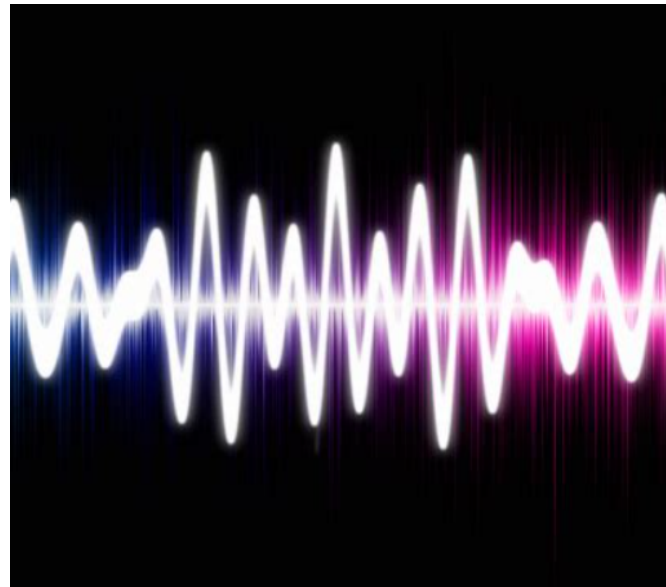
https://www.astera.com

AI text analytics for audio data

AppTek and expert.ai have entered into a strategic technology partnership to bring AI-based text analytics to dynamic audio content in multiple languages.

The partnership leverages AppTek's Automatic Speech Recognition (ASR) and Neural Machine Translation (NMT) technologies with expert.ai's natural language understanding (NLU) capabilities to enable organizations to leverage audio content in the unstructured data sets that they manage for improving decision making and augmenting intelligent automation.

As organizations increasingly utilize language data - emails, documents, reports and other free form text - for an ever-growing range of enterprise use cases (knowledge discovery, contract analysis, policy review, email management, text summarization, classification, entity extraction, etc.), natural language capabilities will play a critical role in powering any process or application that relies on unstructured language data.

The combined capabilities of AppTek and expert. ai enhance enterprise and government NLU and NLP (natural language processing) applications, expanding the data types and sources available for analysis to provide even more informational output.

Using AppTek's speech-to-text technology within the expert.ai Platform, organizations can automatically transcribe audio types from different sources, including high-quality media broadcast content, podcasts, meetings, one-to-one interviews or even low-bandwidth telephone conversations.

In addition, they can leverage advanced multilingual functionalities to generate highly accurate, customizable and scalable translations across hundreds of language pairs.

http://www.apptek.com, https://www.expert.ai

Evisort introduces smart OCR AI for contracting

Evisort has updated its no-code contract intelligence platform with enhanced AI and expanded platform capabilities to make the contract lifecycle easier, faster and more reliable for global teams.

The improved user experience features enhanced Optical Character Recognition (OCR) technology, multi-language capabilities, and an expanded intelligent clause library for more efficient drafting and more confident negotiation.

Evisort's updated OCR addresses the historical issues that OCR technology industry-wide has struggled with, including deciphering handwriting, blurry text, tables, headers, footers, watermarks, and multiple languages.

With these AI enhancements, Evisort's solution will empower customers to better manage global business contracts, including contracts in multiple languages.

Evisort's expanded clause library will provide insights on data-driven preferred language and will eliminate the need to manually build a clause library.

"Evisort's AI-powered contract lifecycle management (CLM) capabilities support fast implementation and return on investment by reducing manual work required to ingest, analyze, and create contracts," said Amine Anoun, Evisort co-founder and CTO.

"These recent advancements will enable users to draft and manage contracts more efficiently and confidently than ever, and we are excited to be on the forefront of innovation in this critical space."

Evisort's technology parses the nuanced context and meaning of legal language and helps operational teams scale faster, reduce costs, and deliver greater business impact.

Headquartered in San Francisco, the company supports legal, finance, sales, procurement and IT organizations around the globe

https://www.evisort.com/

OCR module for Contractor app

Contractor Compliance Inc., a developer of Contractor Management Software, has announced the launch of an OCR (Optical Character Recognition) module, available to enterprise clients with both assisted and automated approval workflows.

Over the last two years, Contractor Compliance Inc. has seen the number of requirements actioned by their users grow by 263% as the demand for Contractor Management Software grows.

Contractor Compliance Inc.'s OCR module enables organizations to more efficiently ingest data

from third party contractor, supplier and vendor submissions.

Through the OCR module, clients can:

■ Configure specific requirements to extract relevant data from third party submissions, defining mandatory data fields and acceptable submission values.

■ Use Assisted Approvals to display OCR results and expedite a user's ability to review third party submissions by isolating only relevant information.

■ Use Automated Approvals to disposition third party submissions without the need for human intervention.

https://www.contractorcompliance.io/

Business Process Visualization tool

Bonitasoft has announced the first release of the Bonita Digital Business Process Management platform.

It includes tools to customise the visualization of processes and cases for improved process monitoring, giving businesses a deeper understanding of how processes are performing as they run.

These come from the Process Analytics project, an open source project, distributed under the Apache license, that is developing tools to help developers to visualize and monitor process execution data using the BPMN2 standard notation.

After two years of development, the Process Analytics project is now advanced enough to offer a set of re-usable, embeddable libraries that can be easily integrated into other existing BPM, RPA, iPaaS, and process mining applications and platforms.

"We see process analytics as a sub-segment of the Data Analytics market, in which the data model is related to process execution use cases.

"The more data about business processes that the platform can mine and offer to business users in an easy-to-consume format, the better decisions they can take about where to optimize, improve, and innovate," said Charles Souillard, CEO and co-founder of Bonitasoft.

The current release of Bonita 2022.2 also has a brand-new Reporting Application that includes process execution reports, with relevant historical data of processes and cases, for analysis of past process performance that will aid in pinpointing areas for improvement.

Further, Bonitasoft also announces that it has achieved ISO 27001 certification for its Bonita Cloud development, user support, and operations.

The Bonita Community open-source edition includes all capabilities required to develop and deploy process automation projects, and can be downloaded here.

APEX Backup IRAP PROTECTED Level

Dell Technologies has successfully completed an Infosec Registered Assessors Program (IRAP) Assessment of APEX Backup Services, its hosted data protection offering for Software as-a-Service applications, endpoints and hybrid workloads, at the PROTECTED level.

APEX Backup Services delivers high-performance and secure digital data backup with disaster recovery, long-term retention and automated compliance. The completion of the IRAP assessment represents Dell Technologies' investment in meeting Australian cybersecurity requirements for Australian organisations in addition to its existing certifications.

Achieving the "protected" information classification level also assures government agencies that they can use a vendor's offerings to process and store workloads in a range of use cases.

The Australian Cyber Security Centre (ACSC), in conjunction with the Australian Signals Directorate (ASD), initiated the IRAP Assessment process to ensure the standard of cybersecurity and information security assessments for ICT systems processing or storing government information.

APEX Backup Services uses cloud infrastructure to offer a Dell-managed solution that delivers resiliency and speed organisations need to meet business service level agreements. With no infrastructure to manage, businesses can get started within minutes. Customers have complete visibility through a single console and a consistent management experience across SaaS applications, endpoints and hybrid workloads. Customers can easily scale their infrastructure as needed with infinite, on-demand scalability, and better manage IT budgets with predictable and controllable costs.

Critical to the APEX Backup Services offer is its Zero Trust architecture. Dell Technologies aims to serve as a catalyst for customers to achieve Zero Trust outcomes by making the design and integration of this architecture easier. Security is critical to everything built at Dell Technologies and Zero Trust is one of the foundational pillars for APEX Backup Services.

Following this assessment, Dell Technologies will be submitting its other APEX offerings for approval for Australian Federal Government use in the coming months.

"Undertaking an IRAP assessment is part of our ongoing global commitment to adhere to local regulations and certifications to ensure customer data is safe during their digital transformation initiatives.

"As a result, more government departments and agencies will be able to innovate faster and deliver superior customer experiences using hosted data protection like APEX Backup Services," said Angela Fox, senior vice president and managing director of Dell Technologies ANZ.

Filevine Legal Document Assembly

Filevine, a legal work platform, has launched .vine, a document format designed for legal drafting. It powers Filevine Document Assembly, a document generation tool that replaces word processors such as Microsoft Word and Google Docs. Document Assembly auto-populates data, clauses and other information stored in Filevine to accelerate legal document generation and ensure accuracy.

Combined, the company says .vine and Document Assembly introduce a vastly better way to draft complaints, demand letters, interrogatories and more. Since the 1990s, most legal teams have relied on Microsoft Word to draft documents. This legacy technology drove a wedge between case management systems where teams collect data and the document management systems where they store and edit Word Docs.

Typically, teams must copy-paste everything from names and dates to company holdings and expenses from their case management system to documents. After acquiring the contract lifecycle management system, Outlaw, in 2021, Filevine recognised an opportunity to utilise Outlaw's drafting technology to improve on legacy word processors and static document formats.

"In 2017, when we set out to create a new word processor and doc format from scratch, we focused on contracts because they're harder than other legal scenarios in terms of workflow, content structure, negotiation/redlining, permissions and version control," said Outlaw's CTO and Co-founder, Evan Schneyer.

"We had the sense that if we could solve these problems in the contract space, we could solve them anywhere. And now, the .vine format represents the extension of Outlaw's market-proven contracting technology to add loads of formatting capabilities that are mission-critical in a broader legal context: firm-specific headers & branding, pleading lines, captions and much more."

By inventing a new document format and assembly tool for legal documents, Filevine aims to make the drafting process faster, less tedious and more accurate. Teams in Mass Tort, Personal Injury, Immigration, and Corporate Legal will especially benefit from dynamic .vine files and the Document Assembly tool. Combined, they enable users to:

■ Auto-populate data stored anywhere in Filevine. This includes names, dates, tables, expenses, company holdings, saved clauses, and more.

■ Bidirectionally sync data, meaning that changes to data in a .vine document automatically update data in the Filevine database, and likewise, changes in the Filevine database are automatically pushed to .vine documents.

■ Use conditional logic so that .vine templates adapt to multiple contingencies. For example, conditional logic can automatically change language in a letter to an insurance company based on the insurance type (Liability, UIM, No-Fault, etc.).

■ Make redlines and comments to facilitate contextual feedback and accurate edits.

■ Securely store and share documents with clients, colleagues,and co-counsel. A .vine can be viewed in any web browser or exported as a docx or pdf.

https://www.filevine.com/

Form builder adds automated workflow

Cognito Forms, SaaS provider of an online form builder, has launched workflow automation, a set of upgraded features that triggers meaningful connections while collaborating around data.

Cognito Forms customers use online forms for applications, contracts, expense reports, purchase orders, and service requests.

Allowing employees to fill out forms digitally has been around for years.

What has been missing is the ability to take action to approve, deny, or add additional information and store that information together.

Cognito Forms has built workflow automation into it online form builder to work with a company's workflow from initiation to completion.

Trigger email notifications support users' busy schedules and notify them when it's their turn to act.

For example, Cognito Forms can collect clear decisions from each participant and ensure documented decisions, such as approved or denied.

Integrated into Cognito Forms' online form builder, workflow allows users to:

■ Assign custom roles to different employees inside and outside of their organization

■ Create custom statuses based on actions each participant needs to make

■ Automatically change statuses based on actions from the different roles

■ Trigger emails that ask for participants' actions

https://www.cognitoforms.com/

Micro Focus debuts Data Protector 11.02

By Brett Knudson

More data has traditionally meant more problems. An increase in data can result in problems such as ransomware, disasters, or data loss of any kind. Data Protector standardizes and consolidates backups across multiple platforms. It provides secure, comprehensive backup protection for business–critical data and applications whether virtual, physical, or online in the cloud.

Data Protector 11.02 widens the net of protection previous versions have offered with new features such as role-based access control, deduplication updates, and integration agent updates. Role-Based Access Control (RBAC) allows for the assignment of users and groups to roles, addressing more granular rights management in hybrid enterprises.

Role-Based Access Control helps users assign individual users or groups to certain backup or recovery tasks. Data Protector can be set up using dedicated rules for enterprise activity, which is standard for many solutions. Users have granular choices for whether a user can back up, restore, or even see certain backup clients. More restrictions can be applied to the main backup server, the Cell Manager.

Deduplication Update

The newest update to the Data Protector Deduplication capability allows for cloud tier migration, immutability of stored data, and support for VM Power-On and Live-Migration.

Data Protector 11.02 update allows for automatic data migration between cloud tiers such as AWS S3 to Glacier or Azure Hot à Cool à Archive. Migration is kicked off after several predefined days and provides cost-saving potential for customers storing long-term data. The migration process is fully automated and doesn't need any manual input, relieving administrative personnel from mundane maintenance tasks.

Setting an immutability timeframe on stored data ensures information cannot be changed or deleted before the timeframe has expired. This helps prevent accidental or rogue deletion and prevents ransomware from changing data sets.

Users will now be able to Power-On or Live-Migrate VMware virtual machines directly from DPD stores. Power-On will run a VM on top of DPD without any restore operation, allowing for fast checks and access to VM content. Live-Migration will power in the VM and restore it in the background. The VM is Live throughout the process, shortening RTO to a few seconds.

Integration Agent Updates

The new SAP HANA integration agent allows for differential backups in addition to restoring workflows controlled by the DP GUI.

This 2nd step of the SAP HANA integration agent update provides the ability to run a differential backup, supporting special backup strategies. When compared to incremental backups, differential backups allow for faster restore chains. This approach enables an improved RTO.

The SAP HANA restore workflow has now been fully embedded into the DP GUI workflow, enabling dedicated data protection teams to run standard DP operations on SAP HANA instead of relying on SAP tools. Users have the choice of DP and/or SAP-based protection and recovery.

The new Unified Agent platform allows for faster integration of NoSQL-type databases since they share certain similarities. This underlying framework will also provide capabilities for customers and partners to build their own integration plugins.

Data Protector 11.02 will ship with a plugin for MongoDB, the first of many plugins utilizing this new Unified Agent architecture. The MongoDB plugin will support standalone and clustered databases and provides features comparable to existing application integrations such as redirected restores and point-in-time restores. The plugin will be hosted in the DP Web GUI space.

Micro Focus has two data protection offerings: Data Protector Premium supports hybrid and more traditional infrastructure environments and has many built-in advanced capabilities. For more modern workloads Data Protector for Cloud Workloads offers extensive backup functionality for Microsoft 365 Online products, as well as extensive hypervisor and container backup, and support for a wide range of cloud storage targets.

In addition to offering backup support for the Microsoft 365 online products including Exchange, SharePoint, Teams, and OneDrive for Business, it provides backup support for containers and a wide range of hypervisors. An extensive list of cloud storage providers is selectable as backup targets.

Access a free trial of Data Protector.

Access a free trial of Data Protector for Cloud Workloads.

APPS & APPLIANCES

A Better Contract for Banking/FSI

Icertis has announced the launch of Icertis Contract Intelligence (ICI) for Banking and Financial Services. The CLM out-of-the-box functionality includes a range of contract types, rules to identify obligations, and workflow and reporting to support specific challenges in business processes across front, middle, and corporate offices of Banking and Financial Services organisations.

The new solution helps banks and financial services institutions to better author and manage complex contracts to power all aspects of their business through improved efficiency, visibility across business units and third-party suppliers, and control to manage risk and adhere to regulatory requirements.

The Banking and Financial Services Solution, built on the end-to-end ICI CLM platform, meets needs across banking and capital markets with a package of attributes, clauses, templates, associated documents, obligation management, and reporting.

While business operations-related contracts provide agility, efficiency, and assurance and compliance to business teams, common contract types enable corporate functions like procurement to manage the complexity related to the high volume of third-party suppliers. Deep insights from existing banking and financial services clients have led to several packaged banking and capital markets agreements; a sample includes:

■ Blocked account management to support the complexity of managing non-performing assets.

■ Treasury management to facilitate the creation of treasury management services.

■ The creation of engagement and reservation of rights letters for mergers and acquisitions.

■ Global custody management to generate custody agreements to meet the specific needs of each relationship and streamline negotiations and approvals.

■ Trading agreements, including ISDA master agreements, schedules, credit support annexes, and repurchase loan agreements.

■ Banking and Financial Services Agreements with Regulatory and Compliance Obligations.

"According to our research, the total addressable market (TAM) for cloud-based Contract Lifecycle Management (CLM) software will expand rapidly from over $US4.1 billion in 2022 to over $US8 billion in 2026, representing a Cumulative Aggregate Growth Rate (CAGR) of 19.4% and totalling close to $US30 billion over the five years," said Igor Stenmark, Managing Director, MGI Research.

"Financial services organisations of all stripes – from retail and commercial banks to insurance providers and capital market participants stand to benefit significantly from modern CLM solutions that can help accelerate their digital transformation, optimise costs, and improve client engagement and service.

"Leading financial services providers seek to take advantage of out-of-box CLM capabilities to remove friction from key business processes – from loan origination to M&A to compliance management, among others."

www.icertis.com/bfsi

IMTF and Parashift in compliance push

Parashift, a provider of advanced machine learning-based document classification and data extraction software, has announced a technology partnership with IMTF, a leading global provider of RegTech solutions for financial firms.

The integration of Parashift's technology with IMTF solutions will enable companies to easily map out processes such as mortgage applications, KYC reviews, or general inbox processing with minimal effort. At the core of the Parashift solution is Document Swarm Learning. AI models are trained at the field level and across use cases, significantly reducing time-to-value. Natively integrating with IMTF applications, it allows structured document data to be integrated into any process, minimizing manual interactions.

"With this integration, IMTF and Parashift are working together to simplify data management across organizations and drive operational improvements. This enables our customers to automate internal processes significantly and ultimately serve clients better" said Gion-Andri Büsser, CEO of IMTF.
www.parashift.io

AI-Powered Sales Order Automation

Kanverse.ai has announced the launch of Jasper release of its patented AI-powered Intelligent Document Processing Product suite for Enterprises.

With Kanverse Sales Order automation, sales operations and customer success teams can now automate the intake of sales orders, extraction of order details with up to 99.5% accuracy, validation of orders based on business needs, and filing in the ERP system. The release also introduces new capabilities for AP Invoice Processing Automation for multi-layer invoice approval workflows, processing bulk invoices as a single MS Excel document, and non-PO invoice processing automation with intuitive capabilities.

The Jasper release delivers innovative features for Insurance document processing automation. A new insightful analytical dashboard provides a holistic view of the entire document proceeding, while API support for claims processing leverages powerful Kanverse image processing technology. This technology will detect and classify damages from images with 99.5% accuracy.

www.kanverse.ai