



**The Rise of
Orchestration
and Agentic AI**



Is Your Data Ready for Customer Communication?

**How to safely deploy Microsoft
Copilot in your enterprise**

**Shadow AI: A New Insider Risk
for Cybersecurity Teams**

There must be a better way?



Scanner Rentals *POWERED BY* ezescan.

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

Call: 1300 EZESCAN (1300 393 722)

www.ezescan.com.au

WA Health Seeks Electronic Medical Record Solution

Western Australia's Department of Health has released an invitation for expressions of interest for a statewide Electronic Medical Record (EMR) solution, marking a significant step in the state's healthcare digital transformation journey.

The ambitious procurement project calls for a "single configuration, statewide EMR solution with a Patient Administration System (PAS)" to modernize healthcare delivery across Western Australia's vast and geographically diverse health network.

The invitation document outlines WA Health's vision to implement a comprehensive electronic medical record system that will connect healthcare providers and patients across metropolitan, regional, and remote areas of the state.

With submissions due by May 14, 2025, the project is expected to transform how healthcare is delivered to the state's three million residents.

"The people of WA expect the WA Health System to use technology to improve the safety, quality, equity, and sustainability of their health care," the invitation states. The EMR solution aims to address significant healthcare challenges including an aging population, increasing chronic disease prevalence, and healthcare worker shortages.

Currently, patient medical records are created within a single hospital and are serviced by a portfolio of applications and manual activities unique to each hospital.

A mixture of features from localised and WA Health System-wide technology are used to register, record, and share clinical information.

The multiphase procurement process will include an initial expressions of interest phase, followed by a request for tender phase, product demonstrations, site visits, and an implementation planning study

before final contract negotiations. The project anticipates an initial contract term of 10 years, with possible extensions totalling an additional 10 years.

WA Health has identified 10 key objectives for the EMR implementation, including delivering seamless care, providing transparent patient records, closing health equity gaps, optimizing safety and quality, and enabling a digitally empowered workforce.

The EMR program, which began in 2019, is part of a broader digital transformation initiative divided into two stages.

Stage 1 focused on establishing digital capabilities through initiatives like the Digital Medical Record (DMR) and ICU EMR systems. The current procurement falls under Stage 2, which aims to implement core features of a contemporary EMR over a 10-year roadmap.

This digital transformation represents a critical investment in Western Australia's healthcare infrastructure, promising to improve patient outcomes while enhancing efficiency across the state's healthcare system.

The successful implementation will enable healthcare providers to make better-informed decisions, reduce medical errors, and improve care coordination, particularly for patients in remote areas who often require multiple healthcare encounters across different facilities.

Respondents must demonstrate their ability to deliver a system capable of achieving Healthcare Information and Management Systems Society (HIMSS) Electronic Medical Record Adoption Model (EMRAM) stage 6 maturity, ensuring Western Australia's healthcare system meets international standards for digital healthcare excellence.

A non-mandatory briefing for interested parties was held on April 11, 2025, at the Department of Health offices in Perth.

idm.
information & data manager

Publisher/Editor: Bill Dawes

Email: bill@idm.net.au

Web Development & Maintenance: Cordelta

Advertising Phone: 02 90432943

Email: idm@idm.net.au

Published by Transmit Media Pty Ltd

PO Box 392, Paddington NSW 2021, Australia

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

Cyber Security Gaps Leave NSW Councils Vulnerable, Auditor-General Finds

A concerning number of New South Wales councils remain vulnerable to cyber attacks despite improvements in some areas, according to the NSW Auditor-General's 2024 report on local government cyber security.

The audit, which examined 128 councils, 13 joint organisations and nine county councils, found significant shortcomings in cyber security planning, risk management, and incident re-sponse capabilities across the sector.

Among the key findings, 36 councils had not rated their cyber risks at all, while 37% of those that did evaluate their cyber risks found they exceeded their risk appetite. Additionally, 41% of councils lacked formal plans to improve their cyber security posture.

"There are significant shortcomings in council plans to improve their cyber security," the re-port stated, highlighting a concerning gap between risk identification and remediation efforts.

The Office of Local Government (OLG) issued Cyber Security Guidelines for Local Government in December 2022 and updated them in January 2025. However, these guidelines remain recommendations rather than mandatory requirements, allowing councils to adopt various frameworks with differing levels of protection.

While 100 councils have adopted the Australian Cyber Security Centre's Essential Eight framework, the report noted this alone "may protect key systems and data, but may not provide sufficient focus on other cyber security elements that are included in the Guidelines."

The audit revealed 37 councils still operate without a cyber security policy, with 49% of these being rural councils. Furthermore, 64% of councils had not identified all information assets requiring protection, potentially leaving critical systems vulnerable to attacks.

Incident response capabilities also showed concerning gaps, with 33% of councils lacking a centralised register of cyber incidents and 43% operating without a cyber incident response plan. Of those with response plans, 44% did not have supporting playbooks detailing step-by-step actions for handling incidents.

The report detailed two case studies where councils experienced cyber security incidents involving third-party systems in 2024. In one case, a council's vendor-hosted payment system fell victim to a "carding attack" where threat actors verified stolen credit card numbers through the system. Another council faced a situation where a third-party library system was compromised, potentially exposing customers' personal information.

Cyber security awareness training, a critical defense against social engineering attacks, appears to be declining. Only 69% of councils required all employees to complete cyber awareness training in 2024, down from 74% in 2023, though still significantly better than the 24% recorded in 2019.

The Australian Cyber Security Centre's Annual Cyber Threat Report 2023-2024 noted over 87,400 cybercrime reports nationwide, with 12% of incidents reported

relating to state and local government, underscoring the sector's vulnerability.

Resource constraints remain a significant challenge, with councils struggling to attract and retain skilled personnel. Twelve councils acknowledged their cyber security spending was insufficient to adequately resource their improvement programs.

The Auditor-General's report suggests improvements in governance have occurred since 2019, but councils must address the identified gaps to protect essential services and infrastructure from increasingly sophisticated cyber threats.

OpenText Reaffirms Commitment to Content Manager

In response to persistent rumours about the future of Content Manager, OpenText has issued a strong statement confirming its continued investment in the platform, according to a blog post from Product Portfolio Manager Gwendoline Huret.

The statement comes as some competitors have allegedly been spreading concerns about the platform being "sunset" following OpenText's acquisition of Micro Focus, which was finalized in January 2023.

"The Content Manager product team would like to re-iterate that Content Manager is a growing product, with one of the highest renewal rates in all of OpenText, something we are very proud of," Huret wrote in the post.

According to Huret, OpenText has significantly expanded development of Content Manager since the acquisition, quadrupling its release frequency from annual to quarterly updates. The platform has seen numerous enhancements including new connectors for Amazon S3, Azure, Microsoft Office and Teams, a revamped mobile app, updated Microsoft 365 integration, Google Drive integration, and automated redaction capabilities for sensitive data.

The company has also integrated Content Manager with other OpenText products including IDOL Enterprise, Brava, and Blazon, with plans underway for integration with Magellan.

"These last two years have displayed visible development through innovations and integrations with OpenText existing tools," noted Huret.

To provide customers with planning certainty, the blog post outlines OpenText's support commitment for Content Manager, which includes a 3-year support lifecycle for all major releases, extendable by an additional 2 years for a total of 5 years of support.

The company's strategy for Content Manager focuses on four key directional themes: Enterprise Data Management, Collaboration, Modernization, and Automation and Machine Learning.

OpenText has maintained transparency about its development plans through quarterly release and strategy calls with customers and partners, which Huret says have "some of the highest attendance seen by OpenText marketing for roadmap and release events."

"The Content Manager product team is transparent in its commitment to Content Manager."

Practical AI Solutions for Records Professionals



POWERED BY
ezescan.

- ✓ AI Assisted Document Classification
- ✓ Seamless EDRMs Integrations
- ✓ Automated Email / eForms Capture
- ✓ Digital Mailroom Automation
- ✓ Simplified Back Scanning

Call: 1300 EZESCAN (1300 393 722)

www.ezescan.com.au

Governing Financial Data: A Cornerstone of Trust and Transparency

By Vladimir Videnovic

In today's data-driven working environment, all organisations face the critical challenge of managing vast amounts of sensitive data, including data related to their financial resources. Effective governance of financial data assets has emerged as a crucial discipline, ensuring data accuracy, regulatory compliance and informed decision-making.

Recently, I revisited the world of financials within the government sector. It reminded me of the days when I led the team tasked with designing and delivering a highly sensitive and strategic information system for the development and maintenance of the Australian government's budget.

This system was architected with core data governance principles in focus, introducing a range of new procedures, practices and tools to optimise the process of managing the budget information assets. Later, the same principles were applied to the initial solution architecture for the Victorian State Resources Information Management System.

Nearly two decades later, I found it quite disappointing that the fundamental challenges of poor data governance implementation remained, resulting in ongoing risks and issues across many government organisations. It probably should not surprise me that the main analytical tool in this domain is still almighty MS Excel. The sheer prevalence of manual processes and intricate data transformations, readily obviated by robust data standardisation, alongside the continued reliance on asynchronous email communication and the absence of a unified chart of accounts master data management, highlight some of the systemic deficiencies in data maturity.

Financial data governance encompasses the policies, procedures and controls that ensure the quality, integrity and security of financial data. It provides a structured approach to managing data assets, defining roles and responsibilities, and establishing clear guidelines for data usage. Some of the essential aspects of data governance in the domain of managing financial resources include:

■ **Decision-making** – data governance improves decision precision in budget development and management by clearly defining decision stewardship, including clear definition of roles and responsibilities concerning the use of data in decision-making, enabling informed decisions about resource allocation.

■ **Data to Decision Lineage** – data governance is responsible for establishing the trust in data by providing a clear understanding of the origin and flow of data from the source to the point of decision, essential for accurate analysis.

■ **Quality of Data** – the old “garbage in, garbage out” principle is still relevant. Data Quality Management is a very important component of data governance, reducing risks of errors and inconsistencies in reports, as well as increasing confidence in fiscal responsibility.

■ **Data Protection** – data governance provides a



framework that enables implementing appropriate access controls to limit access to sensitive data.

■ **Data Standardisation** – a mature data governance solution commonly includes a semantic layer, which enriches metadata by providing business context, definitions and relationships to financial data and ensures consistent definitions for key financial terms across different business units and systems, eliminating ambiguity and promoting accurate interpretation.

■ **Data Democratisation** – in support of a modern data governance, a Budget Data Hub or Budget Data Marketplace should be used as a centralised platform where authorised data consumers can access, share and exchange budget related information assets. By establishing an agency-wide data marketplace, government organisation can enhance data accessibility, improve transparency, establish accountability and foster collaboration. This marketplace should allow for the secure distribution of budget-related information, ensuring that data is accurate, consistent and up to date, with clearly defined ownership, terms of use, ways of distribution and records of a dialogue between data producers and data consumers.

Beyond compliance, robust data governance offers a pathway to increased efficiency, transparency and accountability in managing public resources. The benefits of having sound governance of the financial data are multifaceted, including improved decision precision, decreased likelihood of errors and inconsistencies in reporting and data analysis, enhanced collaboration, reduced vulnerability to data breaches and security risks, streamlined budget management processes, more accurate risk assessments, optimised accuracy of models and enhanced compliance with regulatory requirements.

The Australian Government is developing a comprehensive Data Governance Framework to ensure the effective management of data across all public sector agencies. This framework aims to define common rules, processes and accountability to maintain the privacy and compliance of government data.

Vladimir Videnović is Senior Manager, Audit & Assurance, Deloitte. This article was originally published [here](#).

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

Easily engage staff in digital business processes using RM Workflow.

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

RM Workflow controls your records in Content Manager to ensure information security, audit and compliance, while delivering ease of access and use for end users with the option to review and approve directly from the web browser on your mobile phone.

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



Request a demo
1300 426 400 | icognition.com.au

Tydd Warns of ‘Accountability Gap’ in Messaging Apps



The Australian Information Commissioner has found that government agencies are regularly using phone-based messaging apps without adequate policies to ensure they meet their legal obligations.

In late 2024 the OAIC asked 25 agencies to complete a questionnaire to better understand Australian Government agency information governance practices and policies in the context of messaging apps. Twenty-two of the 25 agencies responded.

In a review of the 22 agencies, OAIC Commissioner Elizabeth Tydd revealed that while 16 agencies permitted the use of messaging apps for work purposes, only half of those had specific policies governing their use. For the 8 agencies that claimed to have policies and procedures in place, 7 provided them to the OAIC. Of these, only one agency advised how messages are to be extracted from the app to its recordkeeping system, stating that a screenshot may be a means of extracting this information.

The report, the first of its kind published under powers in the Australian Information Commissioner Act 2010, highlights significant gaps in information governance across federal agencies. Most concerning was that existing policies generally failed to address freedom of information (FOI), privacy, and other key statutory obligations.

Only 2 agencies’ policies and/or procedures addressed the need for staff to search messaging apps in response to FOI applications.

Two of the 7 that provided policies addressed the disappearing messages functionality of these apps, prohibiting its use. One of these provided instructions to turn off this function.

“The failure to preserve information may result in a failure to comply with Archives Act requirements and preclude the operation of the FOI Act,” the OAIC noted.

"While the technology being used to conduct government business is evolving, the need for agencies to equip staff to uphold legislative obligations remains," said Commissioner Tydd.

"Messaging apps raise novel considerations for key pillars of our democratic system of government, including transparency and accountability."

The review found that Signal was the most commonly endorsed messaging app, with 12 agencies actively encouraging its use. One agency also preferred WhatsApp. Three agencies explicitly prohibited messaging apps, while three others had no formal position on their use.

National Archives of Australia Director-General Simon Froude welcomed the findings, noting they would help develop guidance for agencies about managing these important Commonwealth records.

The Commissioner made four recommendations: urging agencies to develop clear policies on whether messaging apps are permitted; ensure adequate procedures addressing information management, FOI, privacy and security concerns, develop policies and procedures for individual apps; and conduct due diligence on how personal information is handled.

The OAIC flagged it will work with the National Archives to support agencies in understanding their obligations and will revisit the topic in two years to assess progress.

Read the full report [here](#).

GenAI’s Enterprise Security Risks

New research from cybersecurity firm Netskope reveals a dramatic 30-fold increase in enterprise data being sent to generative AI applications over the past year, raising significant secu#rity concerns for organizations worldwide.

According to Netskope’s 2025 Generative AI Cloud and Threat Report, based on anonymized usage data collected by the Netskope One platform, employees are increasingly sharing sensitive information with AI tools, including source code, regulated data, passwords, keys, and intellectual property. This surge in data sharing substantially increases the risk of costly data breaches, compliance violations, and intellectual property theft.

The report highlights that “shadow AI” has become the predominant shadow IT challenge for organizations, with 72% of enterprise users accessing generative AI applications through personal accounts rather than company-managed solutions. Additionally, 75% of enterprise users are now accessing applications with embedded generative AI features.

The cybersecurity firm has identified 317 generative AI applications in enterprise use, including popular tools like ChatGPT, Google Gemini, and GitHub Copilot. The report also notes a significant shift toward local hosting of AI infrastructure, with the percentage of organizations running generative AI locally increasing from less than 1% to 54% over the past year.

Despite this move to local infrastructure, which can reduce the risk of unwanted data exposure to third-party cloud applications, Netskope warns that this transition introduces new data security risks, including supply chain vulnerabilities, data leakage, and prompt injection at-tacks.

To address these emerging threats, Netskope recommends that enterprises assess their gen-erative AI landscape, strengthen controls on AI applications, and implement comprehensive security measures aligned with frameworks such as the OWASP Top 10 for Large Language Model Applications and NIST’s AI Risk Management Framework.

Read the full report [HERE](#)

Our Best Medical Document, Insurance, & ID Card Scanners



Our medical document scanners optimize healthcare workflows by securely capturing and uploading documents directly into patient EMRs, ensuring immediate access across the system. fi Series scanners enable operational efficiency and cost-effectiveness by standardizing processes and reducing paper use. Trusted by leading medical offices, these scanners offer quality and reliability essential for your document management needs.



fi-8820 

Maximize ROI with speed and performance

Maximize ROI with speed and performance. The RICOH fi-8820 production scanner is purpose-built to deliver sustained performance, optimized throughput, and an efficient document workflow.



fi-8930 

High-speed performance and large batch sizes

The fi-8930 is powered by an innovative new engine that has multiple patents pending. Power through backlogged paper and digitize daily operations with high-speed performance and large batch sizes. Plus, enjoy user-friendly design and intuitive features..



fi-8950 

Innovative, Fast, and Built to Last

Ready for your toughest day, every day, the fi-8950 scans up to 150 pages per minute, has a 750-page hopper, and optimizes every document it digitizes.



fi-7600 

Dedicated, Flexible Production ADF Scanner

With a large, 300-page hopper and advanced engineering, this popular mid-office scanner can handle wide and normal-size documents at high speeds.



fi-7700 

Heavy-duty and flexible production scanner for professional use

The fi-7700 is a high-performance scanner designed for continuous high-volume scanning, while its advanced technologies and versatile document compatibility enhance user productivity.





Western NSW Local Health District

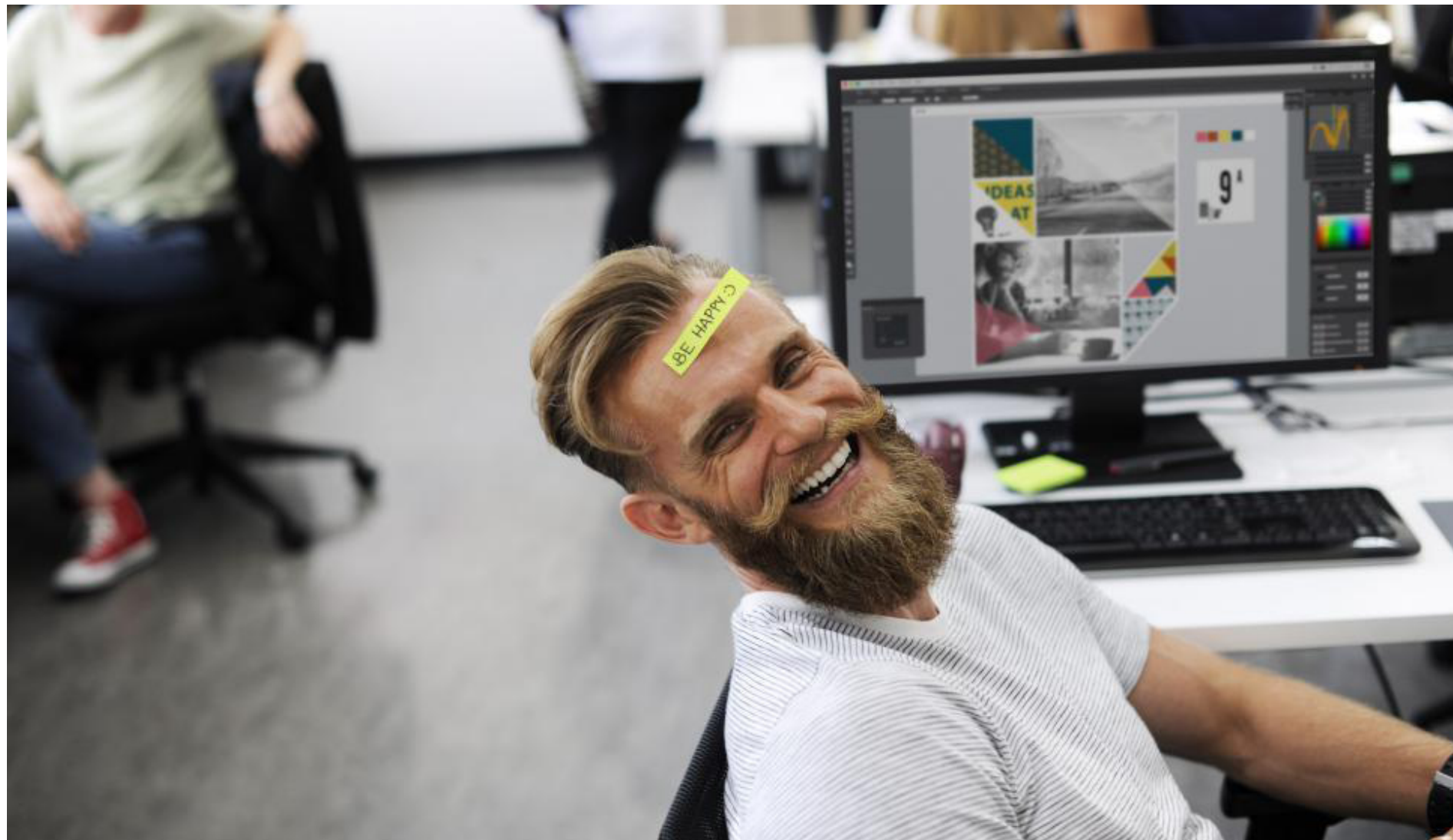
DocuVan provided a fast and efficient service, and scanners were competitively quoted and delivered in a short turn around. The Fujitsu FI 7900 scanners are used at multiple facilities throughout our District and provide a dependable, reliable service to ensure all documents are scanned into the health record without delay.

MAKE ENQUIRY 

RICOH
imagine. change.

DocuVAN
 **1300 855 839**
 **info@docuvan.com.au**

DOCUVAN
IMAGE and DATA SOLUTIONS



How to safely deploy Microsoft Copilot in your enterprise

By Jaimie Tilbrook, EncompaaS

Microsoft’s AI chatbot-turned-full system integration “Copilot” is quickly becoming commonplace in many workplaces. The AI software is capable of a range of tasks, from summarising large documents to automating repetitive tasks across different applications.

Microsoft Copilot has the potential to transform enterprise productivity by leveraging AI-driven insights and automation. However, with increased capabilities come heightened responsibilities around data security and governance.

Before integrating Copilot into your workflows, it’s important to establish a secure, well-governed data foundation to ensure compliance, minimise risks, and maximise the platform’s potential.

Is Microsoft Copilot safe for enterprise use?

The question many organisations are asking is: Is Microsoft Copilot safe? The answer largely depends on the measures taken to secure data before deployment.

While Copilot is designed with [built-in security features](#), its safety ultimately depends on how effectively enterprises manage their data ecosystems and apply robust data governance policies. Without a robust

strategy in place, organisations may face Microsoft Copilot security concerns such as unauthorised data access, compliance violations, or inadvertent exposure of sensitive information.

Enterprises must establish a secure, well-governed data environment. Implementing a comprehensive set of data governance policies and procedures with clearly defined boundaries will mitigate potential Microsoft Copilot security risks.

The importance of a secure data ecosystem for Copilot deployment

Deploying Copilot without securing your data can expose your organisation to unnecessary security risks. The tool’s effectiveness relies on access to high-quality, well-governed information. Without proper data classification, risk mitigation measures, and clear data governance policies, enterprises risk facing data breaches, compliance failures, and operational inefficiencies.

Achieving this level of AI data readiness requires a system that can discover, classify, and organise both structured and unstructured data across your enterprise. A robust data governance policy can provide the framework necessary for securing and governing data in preparation for Copilot deployment.

Key steps to protect enterprise data

By following best practices in data governance policies and standards, enterprises can minimise security risks, ensure compliance, and enable Copilot to operate efficiently within a secure environment.

■ **Establish and enforce user permissions:** Restricting access to sensitive information by setting appropriate user permissions helps mitigate potential data breaches. Only authorised personnel should have access to critical data assets.

■ **Conduct regular access audits:** Routine auditing of user access ensures that permissions remain up-to-date and reflect the current organisational structure. EncompaaS automates these audits, allowing enterprises to proactively address any potential vulnerabilities.

■ **Manage AI outputs effectively:** Monitoring AI-generated outputs is essential to prevent unintended disclosures

of sensitive data. The EncompaaS platform offers [AI governance tools](#) designed to continuously monitor and maintain data quality and deliver sustained accuracy of AI-generated outputs over time.

Strategies for a safe and compliant deployment

A successful Copilot deployment requires alignment with your organisation’s broader data governance policies and standards. By embedding governance, privacy, and monitoring measures into your AI strategy, you can be sure your deployment is safe, compliant, and effective over time.

■ **Align with data governance frameworks:** Your organisation’s [data governance](#) policy should define how information is accessed, managed, and utilised. EncompaaS ensures that data governance policies are applied automatically, maintaining compliance with global regulations such as GDPR and CCPA.

■ **Anonymise sensitive data:** Anonymisation of sensitive information, such as personally identifiable information (PII), ensures that data privacy requirements are met. EncompaaS automatically analyses and classifies records in-place to appropriately reflect the sensitivity of the information.

■ **Monitor AI-generated content :** Ensuring the safety and integrity of AI-generated outputs is critical. The EncompaaS platform provides monitoring capabilities to detect irregularities, ensuring compliance with internal policies and regulatory requirements.

The role of data preparation in securing Copilot deployment

According to Gartner, more than 60 percent of AI projects fail to meet business objectives due to poor data quality and inadequate risk controls. In this context, the question shifts from “Is Microsoft Copilot safe?” to “Is your data governance policy robust enough to support Copilot safely?”

EncompaaS prepares enterprise data by normalising and organising it, ensuring its accuracy and relevance for AI applications. This preparation helps prevent common AI-specific issues, such as data drift, algorithmic bias, and compliance violations.

Mitigating Microsoft Copilot security concerns with better data governance

While Copilot comes with built-in security features, enterprises must take a proactive approach to mitigate Microsoft Copilot [security concerns](#). Key risks include permission management gaps, where poor control over user permissions could inadvertently expose sensitive data. There is also a risk of data repurposing, where data collected for one lawful purpose could unintentionally be used for another, creating compliance issues. Bias risks arise if Copilot amplifies inherent biases in datasets or relies on outdated information, potentially leading to inaccurate or unfair outcomes.

Mitigating these concerns requires establishing robust governance around how data is accessed, managed, and used by AI systems.

Effective data governance encompasses a strategic framework that controls how data is accessed, managed and utilised across the organisation. This involves setting clear policies on who can access specific types of data, defining usage guidelines for AI-generated outputs, and ensuring that sensitive information is handled in compliance with relevant regulations.

How EncompaaS enables secure and effective Copilot integration

Successfully deploying Microsoft Copilot requires a robust approach to data security, governance, and ongoing monitoring. EncompaaS helps enterprises establish a strong foundation for AI-driven initiatives by:

■ Automatically discovering and classifying data across repositories to reflect the sensitivity of the information

■ Applying governance policies that comply with organisation-specific requirements and international data protection standards

■ Monitoring data quality continuously to ensure consistent and reliable AI outputs

By integrating Copilot within a framework of strong data governance policies and standards, organisations can enhance data integrity, ensure compliance, and scale their AI initiatives securely.

Prepare for a successful Copilot deployment with EncompaaS

For enterprises looking to deploy Microsoft Copilot securely and effectively, EncompaaS offers a trusted solution. Our data preparation platform ensures that your data is secure, compliant, and fully prepared for AI-driven initiatives, enabling you to focus on innovation with confidence.

By embedding strong data governance policies and procedures into your deployment strategy, your organisation can mitigate Microsoft Copilot security risks while unlocking the full potential of AI.

Jaimie Tilbrook is Chief Product Officer at [EncompaaS](#).

Hacktivism Evolves into Cyber Insurgency

Hacktivist groups are rapidly evolving beyond traditional disruptive activities into more sophisticated and destructive cyberattacks targeting critical infrastructure and deploying ransomware, according to a new report from cybersecurity firm Cyble.

The report, which analyzes hacktivist activities during the first quarter of 2025, reveals that hacktivism has “transformed into a complex instrument of hybrid warfare” with some groups now employing advanced techniques previously associated primarily with nation-state actors and financially motivated criminal organizations.

Pro-Russian hacktivist groups, including NoName057(16), Hacktivist Sandworm, Z-pentest, Sector 16, and Overflame, were identified as the most active in Q1 2025. These groups primarily targeted NATO-aligned nations and countries supporting Ukraine, with a concerning 50% surge in attacks on Industrial Control Systems (ICS) and Operational Technology (OT) in March alone.

“Hacktivism is no longer confined to fringe ideological outbursts,” the Cyble report states. “It is now a decentralized cyber insurgency apparatus, capable of shaping geopolitical narratives, destabilizing critical systems, and directly engaging in global conflicts through the digital domain.”

The sectors most frequently targeted include government and law enforcement agencies, banking and financial services, telecommunications companies, and energy and utilities. The latter was particularly singled out for ICS attacks, with notable incidents affecting energy distribution and water utilities.

Geographically, India experienced the highest number of incidents in January, while Israel remained a persistent target throughout the quarter with a major spike in March, driven largely by pro-Palestinian hacktivist groups responding to the ongoing conflict in Gaza.

The United States saw an increase in attacks in March, which Cyble correlates with early actions by the new Trump Administration, including military strikes in Yemen and the implementation of import tariffs.

Perhaps most concerning is the adoption of ransomware by hacktivist groups. Cyble identified at least eight hacktivist groups and their allies “embracing ransomware as a tool for ideological disruption” during Q1.

In one notable incident, the Ukraine-aligned BO Team conducted a ransomware attack on a Russian industrial manufacturer allegedly linked to the Ministry of Defense, encrypting over 1,000 hosts and 300TB of data, which resulted in a \$50,000 Bitcoin ransom payment.

Other groups, including Yellow Drift and C.A.S., have focused on data exfiltration operations against Russian targets, with Yellow Drift claiming to have compromised over 250TB of government data from the Tomsk region and 550TB from Russia’s national e-procurement system.

The report also noted that hacktivist groups are increasingly employing more sophisticated website attack methods, including SQL injection, brute-forcing web panels, exploiting OWASP vulnerabilities, and using Dorking techniques to discover exposed databases.

Cyble warns that as the technical capabilities of these ideologically motivated actors continue to advance, the distinction between hacktivists, nation-state actors, and financially motivated threat groups is increasingly blurred, creating heightened risks for organizations in regions experiencing geopolitical tensions.

To mitigate these evolving threats, the security firm recommends organizations implement comprehensive cybersecurity measures, including network segmentation, Zero Trust architecture, risk-based vulnerability management, ransomware-resistant backups, enhanced protection for web-facing assets, and comprehensive monitoring of networks, endpoints, and cloud environments.

Backdoor Attack Exploits Teams

ReliaQuest has uncovered a sophisticated attack campaign that uses Microsoft Teams to deploy a previously unknown backdoor malware. The attacks, which began in March 2025, specifically target female executives in the finance and professional services sectors.

The attack chain begins with carefully timed phishing messages sent through Microsoft Teams from accounts posing as technical support staff. Once victims are convinced to launch Windows’ built-in “Quick Assist” tool, attackers gain access to their systems and implement a novel persistence technique called TypeLib hijacking.

“This is the first time we’ve seen TypeLib hijacking used in the wild,” said Hayden Evans, the primary author of the ReliaQuest report. “Attackers are modifying Windows Registry entries to redirect legitimate COM objects to malicious scripts hosted on Google Drive.”

The technique ensures that the malware, a sophisticated PowerShell backdoor, is automatically downloaded and executed whenever the system restarts. According to ReliaQuest, the backdoor contains extensive “junk code” designed to evade detection, with several space-themed keywords like “Galaxy,” “Cosmos,” and “Orion.”

Analysis of the attack infrastructure suggests the malware has been in development since January 2025, with early versions deployed through malicious Bing advertisements. The report notes that Telegram bot logs associated with the malware contained Russian text, indicating the developer is likely from a Russian-speaking country.

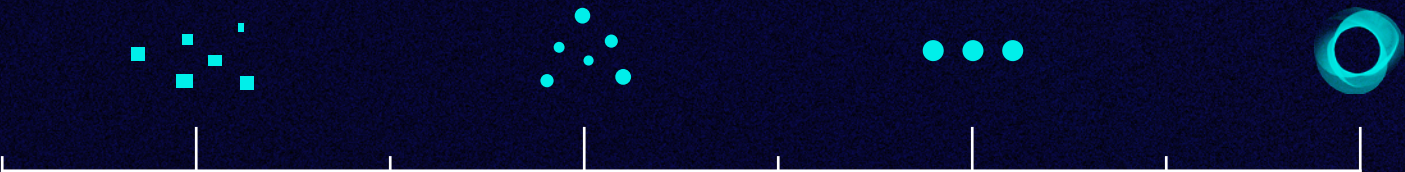
ReliaQuest believes the attackers may be connected to Storm-1811, a threat group known for deploying Black Basta ransomware. However, the report suggests several possibilities: either Black Basta has adopted new techniques, the group has splintered, or an entirely different group has begun using similar initial access tactics.

To protect against these attacks, ReliaQuest recommends disabling external communication in Microsoft Teams, blocking specific domains at the network edge, disabling JScript via Group Policy, and implementing Windows Defender Application Control to restrict PowerShell functionality.

The report highlights a concerning trend in cybersecurity: increasingly targeted attacks that exploit legitimate collaboration tools to bypass traditional security measures.

ENCOMPAAS.CLOUD

DATA



PREPARED

Get Data-Ready for the AI Era.
EncompaaS expertly prepares unstructured data to compliantly accelerate your GenAI success.

Did you know that over 60% of AI projects will fail by 2026 without an AI-ready data foundation?

Source: Gartner, “A Journey Guide to Delivering AI Success Through ‘AI-Ready’ Data”

LEARN MORE





What are AI hallucinations? Why AIs sometimes make things up

By Anna Choi and Katelyn Xiaoying Mei

When someone sees something that isn't there, people often refer to the experience as a hallucination. Hallucinations occur when your sensory perception does not correspond to external stimuli. Technologies that rely on artificial intelligence can have hallucinations, too.

When an algorithmic system generates information that seems plausible but is actually inaccurate or misleading, computer scientists call it an AI

hallucination. Researchers have found these behaviours in different types of AI systems, from chatbots such as [ChatGPT](#) to [image generators](#) such as Dall-E to [autonomous vehicles](#). We are [information science researchers](#) who have studied hallucinations in AI speech recognition systems.

Wherever AI systems are used in daily life, their hallucinations can pose risks. Some may be minor – when a chatbot gives the wrong answer to a simple question, the user may end up ill-informed. But in other cases, the stakes are much higher. From courtrooms where AI software is used to [make sentencing decisions](#) to health insurance companies that use

What springs from the 'mind' of an AI can sometimes be out of left field. [gremlin/iStock via Getty Images](#)

algorithms to [determine a patient's eligibility](#) for coverage, AI hallucinations can have life-altering consequences. They can even be life-threatening: Autonomous vehicles use [AI to detect obstacles](#), other vehicles and pedestrians.

Making it up

Hallucinations and their effects depend on the type of AI system. With large language models – the underlying technology of AI chatbots – hallucinations are pieces of information that sound convincing but are incorrect, made up or irrelevant. An AI chatbot might create a reference to

a scientific article that doesn't exist or provide a historical fact that is simply wrong, yet [make it sound believable](#).

In a 2023 [court case](#), for example, a New York attorney submitted a legal brief that he had written with the help of ChatGPT. A discerning judge later noticed that the brief cited a case that ChatGPT had made up. This could lead to different outcomes in courtrooms if humans were not able to detect the hallucinated piece of information.

With AI tools that can recognize objects in images,

(Continued Over)



Object recognition AIs can have trouble distinguishing between chihuahuas and blueberry muffins and between sheepdogs and mops. [Shenkman et al, CC BY](#)

hallucinations occur when the AI generates captions that are not faithful to the provided image. Imagine asking a system to list objects in an image that only includes a woman from the chest up talking on a phone and receiving a response that says a woman talking on a phone [while sitting on a bench](#). This inaccurate information could lead to different consequences in contexts where accuracy is critical.

What causes hallucinations

Engineers build AI systems by gathering massive amounts of data and feeding it into a computational system that detects patterns in the data. The system develops methods for responding to questions or performing tasks based on those patterns.

Supply an AI system with 1,000 photos of different breeds of dogs, labelled accordingly, and the system will soon learn to detect the difference between a poodle and a golden retriever. But feed it a photo of a blueberry muffin and, as [machine learning researchers](#) have shown, it may tell you that the muffin is a chihuahua.

When a system doesn't understand the question or the information that it is presented with, it may hallucinate. Hallucinations often occur when the model fills in gaps based on similar contexts from its training data, or when it is built using biased or incomplete training data. This leads to incorrect guesses, as in the case of the mislabelled blueberry muffin.

It's important to distinguish between AI hallucinations and intentionally creative AI outputs. When an AI system is asked to be creative – like when writing a story or generating artistic images – its novel outputs are expected and desired. Hallucinations, on the other hand, occur when an AI system is asked to provide factual information or perform specific tasks but instead generates incorrect or misleading content while presenting it as accurate.

The key difference lies in the context and purpose: Creativity is appropriate for artistic tasks, while hallucinations are problematic when accuracy and reliability are required.

To address these issues, companies have suggested using high-quality training data and limiting AI responses to follow certain [guidelines](#). Nevertheless, these issues may persist in popular AI tools.

Large language models hallucinate in several ways.

What's at risk

The impact of an output such as calling a blueberry muffin a chihuahua may seem trivial, but consider the different kinds of technologies that use image recognition systems: An autonomous vehicle that fails to identify objects could lead to a [fatal traffic accident](#). An autonomous military drone that misidentifies a target could put civilians' lives in danger.

For AI tools that provide automatic speech recognition, hallucinations are AI transcriptions that include words or phrases that were [never actually spoken](#). This is more likely to occur in noisy environments, where an AI system may end up adding new or irrelevant words in an attempt to decipher background noise such as a passing truck or a crying infant.

As these systems become more regularly integrated into health care, social service and legal settings, hallucinations in automatic speech recognition could lead to inaccurate clinical or legal [outcomes that harm](#) patients, criminal defendants or families in need of social support.

Check AI's work

Regardless of AI companies' efforts to mitigate hallucinations, users should stay vigilant and question AI outputs, especially when they are used in contexts that require precision and accuracy. Double-checking AI-generated information with trusted sources, consulting experts when necessary, and recognizing the limitations of these tools are essential steps for minimizing their risks.

Anna Choi is a Ph.D. Candidate in Information Science, Cornell University and Katelyn Xiaoying Mei is a Ph.D. Student in Information Science, University of Washington. This article is republished from [The Conversation](#) under a Creative Commons license. Read the [original article](#).






Future-Proof Your ECM Strategy Today



Traditional ECM is at its limits. Adopt a modern content services platform that enables scalability, efficiency, and seamless integration.

Don't just upgrade your systems—lead the transformation of your financial institution.

Modernise your ECM with Hyland →

-  Consolidate silos and reduce information gaps.
-  Deliver omnichannel experiences to customers.
-  Minimise regulatory risks with advanced compliance tools.

Data Governance Gaps Threaten AI Ambitions

There is a significant disconnect between businesses' ambitions for AI and their investment in compliance and risk mitigation, according to the *Ataccama Data Trust Report 2025: Turning Compliance and Risk Mitigation into a Foundation for Strategic AI*, which found that that one in five businesses lack a data governance framework.

The report is based on a survey of 300 data professionals at organizations generating revenue over \$500 million in the banking/finance, business services, healthcare, insurance, manufacturing, retail, software, and telecommunications industries in the US, Canada and UK.

The report found that while 42% of organizations prioritize regulatory compliance, only 26% focus on it within their data teams. This gap exposes businesses to risks such as regulatory fines and data breaches, which can erode customer trust and financial stability.

Currently, only 24% of organizations have implemented AI at scale, highlighting a significant gap in readiness.

The report suggests that organizations must view compliance as a foundation for long-term business value and trust.

Automation is identified as a critical component for sustainable risk mitigation. With 47% of organizations recognizing data quality as crucial for compliance and 39% emphasizing data accuracy for risk mitigation, the report underscores the need for automation in data validation, accuracy, and scalable risk mitigation.

To gain access to AI-ready data, innovative companies should be embedding automation into their workflows for data validation and accuracy, scalable risk mitigation, and auditing. Without automation as the foundation for scalability, businesses risk their AI investment failing.

Leadership misalignment is another significant barrier to responsible AI adoption, with 33% of organizations citing it as a major issue. The rapid evolution of AI necessitates strategic leadership alignment, which many businesses currently lack.

The report also highlights regulatory tension, with 55% of organizations feeling that current frameworks are too restrictive. Despite this, automation has the potential to improve regulatory adherence by 40% this year, suggesting a path forward for businesses to adapt to regulatory changes in realtime.

ABBYY Labs to Accelerate AI Innovation

Document processing and automation leader ABBYY has announced the establishment of new AI Labs across multiple countries, aiming to develop more powerful and developer-friendly document AI models.

The new labs, located in the United States, Hungary, and India, will focus on creating AI solutions specifically designed for intelligent document processing and process automation, with an emphasis on enterprise security and compliance.

"We're building upon decades of leadership in OCR, machine learning, computer vision, and natural language processing, while extending innovations in AI with our industry expertise," said Sanjay Nichani, Vice

President of AI & Computer Vision, who will lead the ABBYY AI Labs.

The initiative comes as the intelligent process automation (IPA) market is projected to reach \$US102 billion by 2028, according to IDC estimates cited by the company. OCR and intelligent document processing are expected to be the fastest-growing segments within this market.

ABBYY's move also responds to developer needs. According to a SlashData survey referenced in the announcement, more than half of developers using AI (53%) are utilizing third-party APIs, open-source models, or creating customized AI models for their applications.

Nick Hyatt, Vice President of Engineering R&D at ABBYY, emphasized the importance of the developer experience in the company's strategy: "The underlying IP and technology Sanjay is building from the AI Labs is the future to improving how businesses can leverage AI and LLMs within their organization to fast-track new applications and capabilities."

The company plans to release new document AI and process intelligence technologies and solutions during the second and third quarters of 2025.

Patrick "PJ" Jean, CTO/CPO of ABBYY, highlighted challenges that their customers face with current AI solutions: "All too often we hear from customers that they are missing ROI targets and needing to adjust expectations due to hallucinations, unpredictability, and costly models."

Jean added that the AI Labs will focus on "predictability, compliance, and effectiveness, making it easier for developers to consume document AI and deliver value to their organizations faster."

Data Recovery Experts Launch in Australia

After rescuing critical data for tech giants, government agencies, and Hollywood celebrities for over 40 years, data recovery specialist DriveSavers has officially established its Australian headquarters in Sydney.

The California-based company - whose impressive client roster includes Google, Coca-Cola, and NASA - is now bringing its advanced recovery capabilities to Australian businesses and consumers facing data disasters.

"With over 40 years of expertise, our mission has always been to help customers recover their valuable and often irreplaceable data," said Alex Hagan, DriveSavers' Chief Executive. "Our Sydney expansion ensures Australian customers receive the same world-class service that has made us the trusted recovery partner for organizations worldwide."

The Australian launch includes risk-free evaluations and a no-recovery, no-fee guarantee that eliminates financial risk for clients facing potential data loss.

Industry veteran Adrian Briscoe, who brings two decades of Australian data recovery experience, was appointed in October 2024 to spearhead the company's Asia-Pacific and Japan business development.

"My aim is to build a strong DriveSavers partner program, creating a trusted ecosystem where IT resellers become true extensions of the DriveSavers brand, driving innovation and helping their customers successfully recover valuable data," Briscoe explained.

<https://drivesaversdatarecovery.com/en-au/>

INGRESS by iCognition

The next generation
Content Services
Platform has arrived!

Find the right information at the right time.

UPGRADE TODAY

Fast track your information, securely!

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

iCognition's trusted service offers:

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

DISCOVER

PROTECT

SECURE

USE

1300 426 400

icognition.com.au



The Rise of Orchestration and Agentic AI Transforming Business One Process at a Time

By Frank Volckmar

Economists have long talked about the “productivity dividend” from AI. We’re finally seeing it come to life.

AI will reshape our industries one process at a time. The tools are here. The technology is ready. The only question is—who will lead the transformation, and who will be left behind?

For those willing to experiment, adapt, and lead, the future is incredibly exciting.

Over the past three decades, the IT industry has observed significant transformations and breakthroughs that have revolutionized business operations. However, since the advent of the internet, it is argued that no development will be as impactful as the rise of Artificial Intelligence (AI).

From the reduction of operational overheads to the enhancement of productivity, AI is considered the most significant productivity driver encountered.

Yet, according to the OECD, the global productivity growth rate has slowed. This raises the question of what is holding business back and how these challenges will be overcome?

Businesses have successfully navigated numerous IT obstacles to growth over the years, stemming from changes in architecture and processing capability. While these changes may initially be met with resistance, the promise of improved productivity ultimately makes their adoption inevitable.

Many examples illustrate this, including the widespread adoption of mobile phones, Software as a Service (SaaS), and cloud computing.

It would have been difficult to imagine twenty years ago that enterprise companies would be comfortable subscribing to applications shared with competitors, hosted in the cloud, and accessible from any device, anywhere in the world.

AI Isn't New—But It's Entering a New Era

AI is not a novel concept. It has been employed in various forms, such as machine learning, for two decades to decrease administrative overheads in finance and document processing.

This has not eliminated the need for human involvement entirely but has reduced their role to managing exceptions. Applications utilizing AI measure the confidence level, or calculated accuracy, for each action.

If this level falls below a desired target, for instance, 95% confidence, the process is routed to a human for review and correction.

The hyperscalers, namely Microsoft, AWS, and Google, have elevated the accuracy of document extraction from OCR, extractor, and machine learning techniques by introducing prebuilt AI services for extracting information from structured and semi-structured documents (such as invoices and fixed high-volume forms), and even handwritten documents. Organizations have held differing views on using these hyperscalers for processing inbound documents due to concerns about cost, security, and flexibility.



The Game-Changers: Generative, Extractive and Agentic AI

A pivotal change has been the easy accessibility of generative AI following the launch of Chat GPT in late 2022, and the subsequent development of extractive and agentic AI.

While generative AI is being utilized by many workers as a “co-pilot” for quickly generating plans, research, and content, extractive AI takes document processing to the next level, and it is agentic AI that offers substantial gains in the productivity of knowledge workers.

Extractive AI uses Natural Language Processing (NLP) to identify and extract specific information from an unstructured document accurately.

Unlike generative AI, it doesn't create content, it only transforms complex documents into structured information to support efficient processing.

Agentic AI enables processes to operate with a degree of independence by making decisions based on incoming information. It can analyse situations and act on decisions automatically.

If it is uncertain about a decision, based on established business rules, it will forward the information to a human for intervention.

So Why Isn't Everyone Using Agentic AI?

While this may seem straightforward, the widespread adoption of agentic AI to reduce operating costs and improve customer response times faces challenges.

These advanced agentic AI Large Language Models (LLMs) require significant computer processing power, data centres, and power sources. Current power demands may make it difficult for many countries to power larger LLMs domestically, leading to data privacy and security concerns for users.

This raises questions about how to leverage the power of these large LLMs securely and economically. Will countries need to revise their privacy regulations concerning organizational use of private information in transactions crossing borders and accessible by foreign governments?

(Continued Over)

Smart Scanning Solutions for Any Document Type



Up to A3 Production



Book Scanners



Wide Format Scanners



Flatbed Scanners

DocuVan is a Distributor and Reseller of higher end scanning equipment. We can supply, install, train and support you in operating your own scanning solution. We can help you integrate with a document management system and setup workflow processes to automate most paper based legacy systems. Our solutions are scalable and we offer a wide variety of options to suit most budgets.

DOCUVAN
IMAGE and DATA SOLUTIONS

MAKE ENQUIRY

info@docuvan.com.au or call on 1300 855 839

The Rise of Orchestration and Agentic AI

(from previous page)

The prospect of waiting for such changes is not ideal. Alternatively, will technology evolve to reduce the size and computing power requirements of LLM models, allowing them to be hosted on secure localized servers and trained on specific use case data?

Historically, technological evolution, driven by feedback from early adopters to early conservatives and broad market adoption, has often provided the answer.

China’s launch of Deepseek AI demonstrates that there are methods to reduce the size and energy consumption of LLMs without compromising performance. A different trajectory is emerging, and it is believed that many small, secure, trainable, and specific LLMs will become available in the market in the coming years.

These could be highly specialized, such as estimating car repair claim costs based on images for cars in a particular state or city. The LLM would be integrated into a local business process, run on a local service, and be isolated from other systems for security.

An industry focused on maintaining and selling these specific LLMs as services to drive productivity and assist knowledge workers is expected to develop.

The Key: Orchestration of Agentic AI Services

The next challenge will be orchestrating these agentic AI services to streamline business processes. The technology and capabilities for this already exist.

The primary difference will lie in the number of services being orchestrated to achieve the most effective outcome.

It is foreseen that business processes will require several AI services to achieve desired outcomes, including models for understanding incoming information, extracting information, summarizing information, reasoning and acting, generating responses, and finally, monitoring the process for potential exceptions and improvements.

Assembling all the capabilities into a single process whereby you can change out services as technology develops is the value an orchestration platform offers.

Humans currently manage business processes using these skills daily and automating this human capability accurately and at scale within individual process activities, while becoming easier, requires experience and expertise.

“The singularity” discussed by Ray Kurzweil in his book “Singularity is Nearer” refers to the theoretical point in the future where AI surpasses human intelligence. Futurists are predicting singularity to occur around 2045, and until then, orchestration of AI services will be key to automating business processes.

The Time to Act is Now

Although many boards and management teams are still in the process of establishing governance and secure usage policies for AI and related services within their organizations, a significant portion of their employees are already using AI daily through various online applications, Office 365, and streaming services.

AI is becoming increasingly integrated into everyday

life, and people have either willingly or unknowingly accepted the trade-off between convenience and the sharing of some personal information.

Boards and management teams should now be considering how to transform their key business processes to improve employee, customer, and operational performance.

While this may seem like an obvious necessity, many companies already have established strategies focused on expansion through acquisition, product expansion, or market reach, and may not prioritize the new opportunities presented by orchestrating AI services until compelled by competitive pressures.

This delay can be detrimental, as properly managed change takes time. Leaders need to recognize that the introduction of next-level technologies facilitates the entry of new “AI first” players into their markets, and these entrants will leverage AI.

The opportune time to begin transforming legacy processes is now, before disruptive entrants and second-tier players fundamentally alter the market landscape. This undertaking is not overly complex; it requires leadership and process transformation. The necessary tools are available and continue to improve. Partnering with vendors and consultants who can share their expertise and assist in orchestrating various AI services to continuously enhance capabilities and processes is advisable.

Where Should Organisations Start?

Organizations should prioritize transforming processes that represent the “soft underbelly” of the organization, such as those driving customer experience like claims and applications; processes that consume significant administrative resources, such as triage and invoice automation; and processes requiring expensive knowledge workers to summarize and analyse unstructured information before responding to customers. These are the processes within various industries that will be transformed by AI, altering the nature of competitive dynamics.

Public companies should evaluate the impact of these changes on their business models by considering scenarios such as a 70% reduction in customer response time and the cost of serving customers, and how this would reshape their business.

Government agencies, departments, and councils can enhance their contributions to their communities and vulnerable stakeholders by increasing productivity with existing resources. An accessible starting point is the automation of information and application ingestion into their teams. It is not uncommon for local government councils, for instance, to have over 50 online forms, completed in multiple languages, for community service requests, with most of these forms typically emailed to the council for processing.

Often, one or two administrative roles are responsible for triaging these requests to the appropriate department or individual. With AI-driven process automation, the triage task, along with extracting necessary information from the forms, can be completed in seconds. By augmenting the process with business rules, applicants may receive a response within minutes with minimal or no human intervention. The resources currently dedicated to managing administrative tasks can be redeployed to higher-value community benefits, thereby driving productivity.

Frank Volckmar is Managing Director CANZ of TCG Process

Kapish

Empowering Secure Technology Solutions



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



Is Your Data Ready for Customer Communication?



By **Stephanie Pieruccini**

When we look at evolving customer communications, we often focus on improving the experience by adding new delivery channels, improving content by adding colour and variable images based on the audience or improving self-service.

Some organizations focus on making the communications interactive in digital channels, adding video or improving self-serve preference management to encourage digital adoption and reduce print costs.

Despite efforts over the years to merge transactional and promotional (marketing) communications, it's still more common than not that these communications continue to be managed and generated in siloed

systems, separating their stakeholders in name of privacy and security of the data.

Marketing needs to have the freedom to explore any and all options when it comes to lead generation and customer nurturing while transactional communications need to maintain guardrails to retain trust with existing customers by protecting their sensitive data.

Unfortunately, this approach often impacts the customer experience. Inconsistencies in communication look and feel, silos by line of business, disconnected or limited integration between systems ultimately leaves gaps in the customer's ability to navigate the vast web pages and content available through self-serve.

This causes them to turn to support channels such as the contact centre, customer service, agents, chats, etc. More often than not, these employees in the front lines of customer support often request patience from the customer as they need to navigate several internal systems in an effort to find the desired information or answers.

While many strategies look to new software, business process automation or to redesign communications as a way to improve the overall experience, the goldmine at the root of every experience is the customer data.

Customer data management needs to change to improve experiences

Customer data management is done in a variety of ways within an organization, even within individual lines of business. CRMs are often used to capture information for preference management, CDPs (customer data platforms) are used for website tracking and personalization, often missing the full omnichannel experience tracking.

Marketing automation has included lightweight CRMs which are evolving to CDPs but are sometimes just their own database specific to their content-focused use cases. Campaign management is often separate as well, holding its own set of data used for personalizing campaigns and understanding customer behaviour within them.

Journey management solutions also have a unique set of data not stored elsewhere around the events, actions and behaviours, both planned and reality, that reflect customer interactions. Segmentation is another function that is often solved through custom scripting or homegrown systems or is embedded within other marketing systems but holds valuable insights.

The result is a vast system of siloed data sources that customer experience executives and communication centres of excellence (COE) see a need to address, but it requires a level of attention and effort to sort through. At best, go forward efforts such as zero copy policies helps to reduce adding to this complexity, but can slow down adoption of new technologies.

Adding more complexity are AI and LLMs. Generative or Content AI is really where many communications and data tools have focused to generate or tweak content. However, concerns around intellectual property can limit how organizations want to use these tools.

In communications management, assisting content creators to craft messages has shown some value, but is only the tip of the iceberg of the potential value AI can provide to communications experiences.

The more data available to be fed into an LLM, the more we can leverage other AI variations such as Insights AI and Responsive AI, which have the potential to analyse the vast amount of data available in these siloed systems and make recommendations for improving customer experiences from individual touch points to the overall sentiment of the business relationship.

Knowing that this data exists today within organizations but in disparate systems is a good problem to start with. Many have attempted to solve this through business process management/automation and integration, but that approach can create complexities of its own. Aggregating all of this data to persist in a single, centralized database is an unrealistic effort that will get shut down by every CIO and IT department. So, how can we address this?

The first step is understanding where this data exists today. A few questions to ask... What systems exist and where? What type of data is stored in these systems? Is it usable? Is it actionable? Where and when is it used and to what extent?

"Customer data is a goldmine of information that holds the power to make experiences impactful and engaging."

For example, can it be used for personalization of content within a communication, personalization of an experience touchpoint or automating orchestration follow ups?

Once you begin to understand the complexity of your organization's data infrastructure and the valuable data it holds, you open the door to the opportunity to connect these systems with a customer data solution that can provide a powerful, complete view of the customer that is both actionable and insightful.

The work is not done yet. Understanding the personas who need to use this data, creating a data governance strategy and aligning key stakeholders are also critical steps to success.

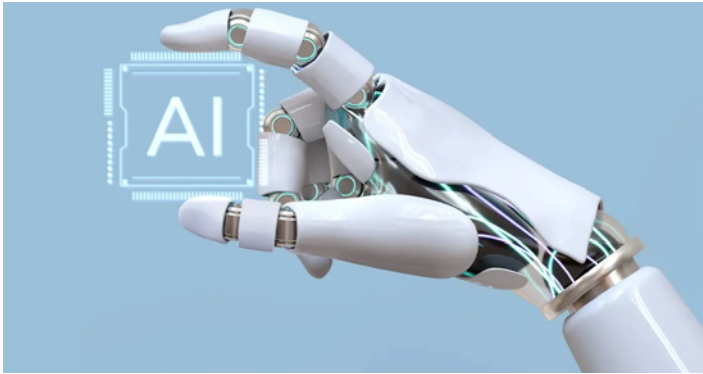
What are the desired outcomes and their respective priorities of this data once it's aggregated, normalized, analysed and able to provide a more complete view of your customers and their behaviours? This goldmine of data is powerful and desirable, so having clear priorities is key.

As we know in customer communications, data is sensitive and must be protected but can provide powerful insights that can improve business outcomes and enhance personalized experiences when used correctly.

New solutions are becoming readily available that are approaching disparate enterprise data systems with a different approach that does not require ripping out the existing infrastructure. It is important to remember that the software and solutions are only as good as the strategy that is driving the ROI and outcomes of centralizing customer data.

*Stephanie Pieruccini is a Senior Manager of Product for **OpenText DX**. In this role she is responsible for communication orchestration and platform support for OpenText Exstream as well as the StreamServe solution.*

McKinsey Finds AI Fears Overblown



A new McKinsey Global Survey on AI reveals that organizations are making structural changes to generate value from generative AI, with large companies leading the transformation. The comprehensive survey gathered insights from 1,491 participants across 101 nations.

According to the report titled *“The state of AI: How organizations are rewiring to capture value,”* 78% of respondents say their organizations now use AI in at least one business function, up from 72% in early 2024 and 55% a year earlier. Similarly, 71% report regular use of generative AI, compared to 65% in early 2024.

The survey identifies key organizational changes that correlate with higher bottom-line impact from AI implementation. CEO oversight of AI governance emerged as particularly significant, especially at larger companies where it has the most impact on EBIT attributable to generative AI. Twenty-eight percent of respondents whose organizations use AI report that their CEO is responsible for overseeing AI governance.

Another critical factor is workflow redesign, which shows the strongest correlation with EBIT impact from generative AI use. Currently, 21% of respondents reporting generative AI use say their organizations have fundamentally redesigned at least some workflows as a result.

Survey responses show that organizations are most often using gen AI in marketing and sales, product and service development, service operations, and software engineering.

“The organizations that are building a genuine and lasting competitive advantage from their AI efforts are the ones that are thinking in terms of wholesale transformative change that stands to alter their business models, cost structures, and revenue streams - rather than proceeding incrementally,” notes Alex Singla, Senior Partner and Global Coleader of QuantumBlack, AI by McKinsey.

The survey also reveals that companies are increasingly mitigating generative AI-related risks, with larger organizations leading risk management efforts, particularly in cybersecurity and privacy domains.

While AI adoption is accelerating, most organizations are still in early implementation stages. Less than one-third of respondents report that their organizations are following best practices for AI adoption and scaling, such as tracking well-defined KPIs for generative AI solutions.

Regarding workforce impact, respondents most often report that employees are spending time saved via

automation on entirely new activities. A plurality (38%) predict that generative AI will have little effect on the size of their organization’s workforce in the next three years, though expectations vary by industry and function.

Organizations have employees overseeing the quality of gen AI outputs, though the extent of that oversight varies widely. Twenty-seven percent of respondents whose organizations use gen AI say that employees review all content created by gen AI before it is used - for example, before a customer sees a chatbot’s response or before an AI-generated image is used in marketing materials.

A similar share says that 20 percent or less of gen AI-produced content is checked before use. Respondents working in business, legal, and other professional services are much more likely than those in other industries to say that all outputs are reviewed.

The findings suggest that while generative AI use continues to surge, meaningful bottom-line impacts remain limited at the enterprise level. As Michael Chui, Senior Fellow at McKinsey, observes: “It will be interesting to see what happens when more companies begin to follow the road map for successful gen AI implementation in 2025 and beyond.”

Read the full report [HERE](#)

University Fights Dual Cyber Breaches

Around 10,000 current and former students at Western Sydney University have had their personal information hacked in a major data breach.

Western Sydney University is the 11th largest in the country, with around 46,000 students enrolled.

In a statement, the university revealed that attackers gained access through one of its single sign-on (SSO) systems in January and February 2025, compromising demographic, enrolment, and academic progression data.

Additionally, the university discovered personal information belonging to its students posted on a dark web forum dating back to November 2024.

“Western Sydney University has been the subject of persistent and targeted attacks on our network,” said Vice-Chancellor and President, Distinguished Professor George Williams AO.

“The University is very aware of the personal impact these incidents are having on its students, staff and wider community.”

The university immediately engaged internal and third-party cyber experts to shut down unauthorized access when detected and has activated its incident response plan. Affected students are expected to be notified next week.

Universities are attractive targets due to their vast stores of personal data, intellectual property, and research information, combined with typically less robust security infrastructure compared to corporate environments.

Western Sydney University has sought and obtained an interim injunction from the NSW Supreme Court to prevent access, use, transmission, and publication of any data associated with the dark web post.



Data capture solutions that makes sense

What if information got where it needed to go... friction-free?

Signal is not the place for top secret communications, but might be the right choice for you

A cybersecurity expert on what to look for in a secure messaging app



By Frederick Scholl, Quinnipiac University

When top White House defence and national security leaders [discussed plans for an attack](#) on targets in Yemen over the messaging app Signal, it [raised many questions](#) about operational security and recordkeeping and national security laws. It also puts [Signal](#) in the spotlight.

Why do so many [government officials](#), [activists](#) and [journalists](#) use Signal for secure messaging? The short answer is that it uses [end-to-end encryption](#), meaning no one in position to eavesdrop on the communication – including Signal itself – can read messages they intercept.

But Signal isn't the only messaging app that uses end-to-end encryption, and end-to-end encryption isn't the only consideration in choosing a secure messaging app. In addition, secure messaging apps are only part of the

AP Photo/Kiichiro Sato

picture when it comes to keeping your communications private, and there is no such thing as perfect security.

I'm a [cybersecurity professor](#) who worked for several decades [advising companies on cybersecurity](#). Here are some of the factors I recommend considering when looking for a secure messaging app:

Secure app choices

The most common messaging protocol, SMS, is built into every smartphone and is easy to use, but does not encrypt messages. Since there is no encryption, carriers or government agents with a warrant, which are typically submitted by law enforcement and issued by a judge, can read the message content. They can also view the message metadata, which includes information about you and your recipient, like an internet address, name or both.

Truly secure messaging is based on cryptography, a

mathematical method to scramble data and make it unreadable. Most secure messaging apps handle the scrambling and unscrambling process for you.

The gold standard for secure messaging is end-to-end encryption. End-to-end encryption means your message is fully encrypted while in transit, including while transiting the communications provider's networks. Only the recipient can see the message. The communication provider does not have any encryption key.

How end-to-end encryption works.

Apple iMessage and Google Messages use end-to-end encryption, and both are widely used, so many of your contacts are likely already using one of them. The downsides are the end-to-end encryption is only iPhone to iPhone and Android to Android, respectively, and Apple and Google can access your metadata – who you communicated with and when. If a company has access to your metadata, it can be compelled to share it with a government entity.

[WhatsApp](#), owned by Meta, is another widely used messaging app. Its end-to-end encryption works across iOS and Android. But Meta has access to your metadata.

There are a number of independent secure messaging apps to choose from, including [Briar](#), [Session](#), [Signal](#), [SimpleX](#), [Telegram](#), [Threema](#), [Viber](#) and [Wire](#).

You can use more than one to adapt to your individual needs.

Default end-to-end encryption is only the first factor to consider when thinking about message security.

Depending on your needs, you should also consider whether the app includes group chats and calls, self-destructing messages, cross-device data syncing, and photo and video editing tools. Ease of use is another factor.

You can also consider whether the app uses an open-source encryption protocol, open-source code and a decentralized server network. And you can weigh whether the app company collects user data, what personal information is required on sign-up, and generally how transparent the company is.

Human factors

Beyond the messaging app, it's important to practice safe security hygiene, like using two-factor authentication and a password manager. There's no point in sending and receiving messages securely and then leaking the information via another vulnerability, including having your phone itself compromised.

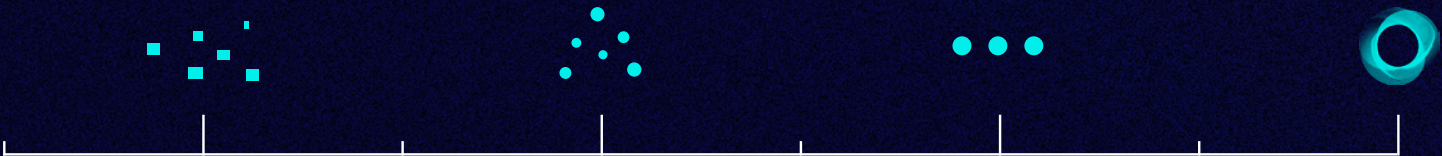
People can be lured into compromising their apps and devices by unintentionally giving access to an attacker. For example, Russian operatives reportedly [tricked Ukrainian troops](#) into giving access to their Signal accounts.

Also, if you use Signal, you should probably [use its nicknames feature](#) to avoid adding the wrong person to a group chat – like National Security Adviser Michael Waltz apparently did in the Signalgate scandal.

Frederick Scholl is Associate Teaching Professor of Cybersecurity, Quinnipiac University, This article is republished from [The Conversation](#) under a Creative Commons license. Read the [original article](#).

ENCOMPAAAS.CLOUD

DATA



PREPARED

Get Data-Ready for the AI Era.

EncompaaS expertly prepares unstructured data to compliantly accelerate your GenAI success.

Did you know that over 60% of AI projects will fail by 2026 without an AI-ready data foundation?

Source: Gartner, "A Journey Guide to Delivering AI Success Through 'AI-Ready' Data"

[LEARN MORE](#)



Shadow AI: A New Insider Risk for Cybersecurity Teams to Tackle Now

By James McQuiggan

Disclaimer: Don't get me wrong, I love using generative AI daily for research and writing. This is about how other users could be using it when they don't know what they don't know and are accidental in their actions to hurt the organization where they work.

Shadow IT has always lived in the background of organizations' environments with unapproved apps, rogue cloud services, and forgotten BYOD systems. Like all technology, the Shadow IT ecology is evolving. It's evolved into something more challenging to detect and even more complex to control, and that's Shadow AI. As employees lean on AI to get their work done faster, they may introduce risk without realizing it. From marketing teams using Claude to research and write content to developers pasting proprietary code into Gemini, the line between productivity and exposure is thin. These tools promise speed and convenience but can become a growing liability without governance.

Nearly 74% of ChatGPT usage in corporate environments happens through personal accounts. That means enterprise controls like data loss prevention (DLP), encryption, or logging are nowhere in sight. Combine that with the 38% of employees who admit to inputting sensitive work data into AI tools without permission, and you've got a significant insider threat. While accidental, it's no less dangerous than a user clicking on a link in a phishing email.

The Security Risks Lurking in Plain Sight

The risks tied to Shadow AI extend beyond accidental data leaks. Developers using AI coding assistants may inject insecure code into applications, especially when no review or validation process is in place as part of the software development life cycle. Customer support teams might lean on chatbots to handle inquiries, which introduces privacy risks when sensitive customer data flows through third-party tools. Even browser plugins with AI functionality can quietly siphon everything from form data to clipboard content to recordings of confidential meetings. And then there's the network side. Employees who use AI-powered proxies or VPNs to get around access controls aren't just sidestepping policies. They are opening doors that attackers can exploit. AI-enhanced meeting tools like transcription services can store confidential conversations offsite, outside IT's control and purview. We are no longer dealing with isolated risks as we increase our attack surface, all created by convenience and productivity.

Strategies to Tackle Shadow AI

Now, we don't need to start blocking all aspects of generative AI platforms in our firewalls because that's like putting a finger into a crack in the dam to prevent water from spilling out. It's futile, and like how water will always find a way, so will your users.

To get ahead of Shadow AI, we start with transparency. Organizations must create clear acceptable use policies (AUP) that address what is acceptable regarding AI usage.

It is a considerable undertaking to communicate with the organization what AI practices are permissible. Teams must know which tools are approved, what kinds of data can be input, and where the line is drawn. Education must go deeper than awareness and focus on managing the human risk element. People aren't misusing AI tools because they want to cause harm, they are looking to solve a problem. Education should focus on the consequences of these tools to build an understanding and not as a scare tactic. When users see how a prompt can lead to a data leak or a compliance breach, it allows them to see the dots connected between their action and the impact. Visibility is also critical. Monitoring systems should be in place to detect when unapproved AI tools are used, whether through browser telemetry, endpoint detection, or network traffic analysis. Rather than blocking everything outright, IT and security teams should focus on understanding their users' needs. If that's access to a GenAI platform, consider a GenAI portal, where users can interact with various platforms through API but with a filter to ensure no sensitive organizational data is exfiltrated. Finally, reviewing AI tools before approving them for use must become a formal part of your software procurement process.

When a user wants to utilize an AI tool or platform, having a process to address the need and business case ensures that people are not just jumping on the latest GenAI bandwagon but allows for your organization's legal, communications, IT, and cybersecurity teams to review and ensure that data is protected. The process should include vetting how data is stored, processed, and shared and verifying whether the tool offers enterprise features like encryption, single sign-on (SSO), and audit logs. If a tool can't meet those standards, it shouldn't be in your infrastructure.

Real-World Example: Samsung's Shadow AI

A recent case that brought Shadow AI risks into sharp focus happened at Samsung in 2023. Several engineers reportedly used ChatGPT to help debug code and optimize workloads. But in doing so, they inadvertently submitted sensitive internal data, including proprietary source code, into ChatGPT.

The incident prompted Samsung to get their legal team to contact OpenAI to request they remove the source code upload to prevent it being used in their training models. Within the organization, a ban on generative AI tools was implemented across the company.

This event wasn't an advanced persistent threat. There was no malware or phishing campaign. Just users trying to do their jobs better. And in the process, they exposed critical intellectual property.

Case Study: Building a Proactive AI Governance Program

A Fortune 500 financial firm saw early signs of Shadow AI use across marketing, legal, and IT teams. Employees were using GenAI tools to summarize documents, create internal reports, and generate content for social media. Leadership recognized the risk and launched a six-month initiative to bring it under control.

The firm started with a survey to understand which AI tools were used and why. They discovered over 20 unique AI tools used without approval. Most of these were routing data through unsecured APIs. Next, they created an AI AUP that clearly defined approved tools, banned use cases, and outlined employee responsibilities.

With the policy in place, governance was needed. They developed an allowlist of vetted AI tools for use by the users. They also deployed browser telemetry tools to flag unauthorized tools and added AI usage reviews to their internal audit checklist.

Most importantly, to address the human risk element, they rolled out quarterly training sessions focused on GenAI and AI risk to keep their users updated on the latest AI trends, threats, and attack vectors.

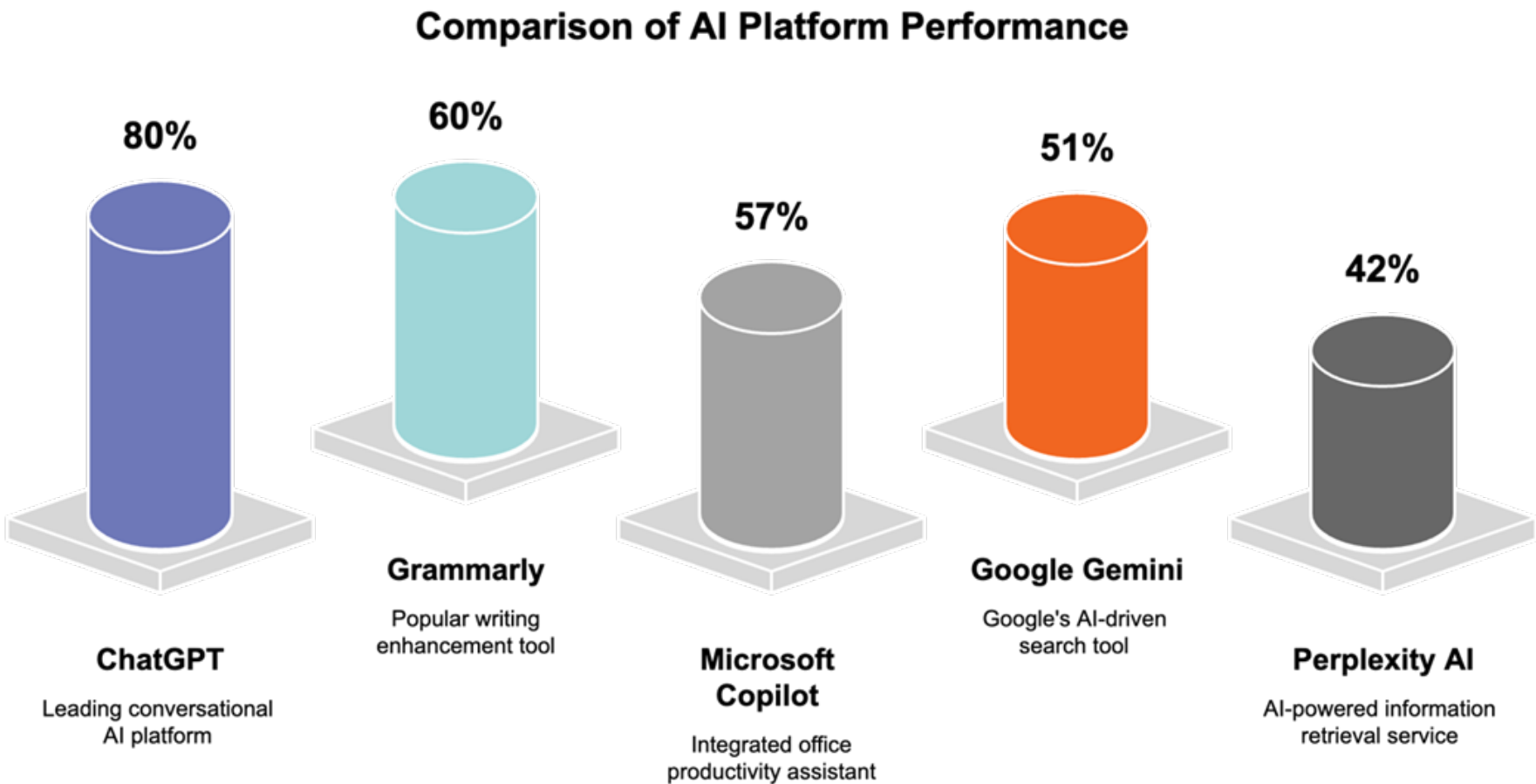
By focusing on enablement instead of enforcement, they saw a 60% drop in Shadow AI usage within four months. More importantly, employee satisfaction remained high because the tools they needed were available, now with much needed guardrails.

A Cultural Shift Is Required

Shadow AI isn't a technology problem. It's a human one. And like any insider risk, it stems from people doing what they think is right without realizing the implications. Organizations that treat this as just another enforcement issue will fall behind. Those who work to cultivate a secure culture and ensure users feel empowered and supported will continue to be ahead of the curve.

- Ask yourself:
- Can you see how AI is used within your organization?
 - Do your employees understand where the boundaries are?
 - Do your systems and policies reflect the reality of how work gets done?
- If not, now's the time to fix that. Shadow AI is here. It's not going away. It's your move.

James McQuiggan is a Security Awareness Advocate for KnowBe4. Article originally published [here](#).





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



EncompaaS is a global software company specialising in information management, powered by next-gen AI. Leading corporations, government departments and statutory authorities trust EncompaaS to govern and optimise information that resides within on-premises and multi-cloud environments. Organisations are empowered to solve information complexity, proactively address compliance and privacy risk, and make better use of data to act strategically at pace. EncompaaS is distinguished in the way the platform utilises AI to build a foundation of unparalleled data quality from structured, unstructured and semi-structured data to de-risk every asset. From this foundation of data quality, EncompaaS harnesses AI upstream to unlock knowledge and business value that resides within information. EncompaaS maintains a robust partner ecosystem, including global consulting and advisory firms, technology partners, and resellers to meet the diverse needs of highly regulated organisations.

encompaas.cloud | enquiries@encompaas.cloud | 1300 474 288



DocuVAN is a Distributor and Reseller of higher end scanning equipment, including Ricoh's state-of-the-art scanning solutions in the workgroup, departmental, and production-level scanner categories. Ricoh fi Series Best-in-Class Document Scanners deliver speed, image quality, and great paper handling, along with easy integration and compatibility with document imaging applications. We also represent Image Access in Australia, NZ, Pacific Islands and PNG as the distributor of their suite of Bookeye and WideTEK Scanners. If it is deemed part of your core business, DocuVan can supply, install and train you to operate your own scanning solution. We can help you integrate with a document management system and setup workflow processes to automate most paper based legacy systems. Our solutions are scalable and we offer a wide variety of options to suit most budgets.

www.docuwan.com.au | info@docuwan.com.au | 1300 855 839



OPEX® Corporation is the industry leader in document and mail automation, providing innovative, unique solutions that help streamline processes, and set the standard for operational efficiency. This includes seamless mail opening and sorting as well as document imaging (scanning), which increases throughput, maximises efficiency, saves time and money, and provides better output. Since 1975, the family-owned and operated company has served as a trusted partner to clients around the world, with more than 1,500 employees continuously reimagining automation technology that solves the most significant business challenges of today and in the future. OPEX provides advanced document and mail automation solutions across numerous industries, including service bureaus, law firms, banks, medical and health organisations, forms processing and archival agencies, and government institutions. OPEX is headquartered in Moorestown, NJ, with facilities in Pennsauken, NJ; Plano, TX; France; Germany; Switzerland; the United Kingdom; and Australia.

<https://opex.com> | info@opex.com



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 | 02 80466880



Established in 2003, iCognition is a leading Information Management and Governance (IMG) specialist. With over 20 years of customer success stories in delivering IMG services and solutions, we provide managed services for OpenText Content Manager (formerly TRIM) to over 130 government and private sector enterprises across Australia. With information governance at our core, iCognition empowers customers in their digital transformation projects to maximise the value of their information assets. Whether that be on-premises or transitioning to our secure cloud solution, Ingress by iCognition, we enable customers to meet the challenges of managing information across the enterprise. Ingress is a Content Services Platform with OpenText Content Manager at its heart. We can transition your Content Manager system to Ingress or provide a greenfields solution in your cloud or ours. Our Ingress cloud is ISO27001 Information Security Management certified and IRAP assessed to PROTECTED.

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



Hyland is a leader in providing software solutions for managing content, processes and cases for organisations across the globe. For 30 years, Hyland has enabled more than 16,000 organisations to digitise their workplaces and fundamentally transform their operations. Hyland has been a leader in the Gartner Magic Quadrant for Content Services for the past 12 years and named one of Fortune's Best Companies to Work For® since 2014. Hyland is widely known as both a great company to work for and a great company to do business with. Our solutions are intuitive to use so organisations can focus on what they do best. Managing information doesn't have to be complicated. At Hyland, our mission is to empower efficiency and agility so our customers can grow and innovate with confidence. We help organisations handle their most critical content and processes with flexible, configurable software solutions.

www.hyland.com/en/ | info-onbase@onbase.com | 02 9060 6405



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



Kodak Alaris is a leading provider of information capture solutions that simplify business processes. We make it easy to transform documents and data into valuable business information and is where digital transformation starts. Kodak Alaris delivers intelligent document processing and information capture solutions that make sense. We exist to help the world make sense of information with smart, connected solutions powered by decades of image science innovation. Unlock the power of your information with our award-winning range of scanners, software and professional services available worldwide, and through our network of channel partners.

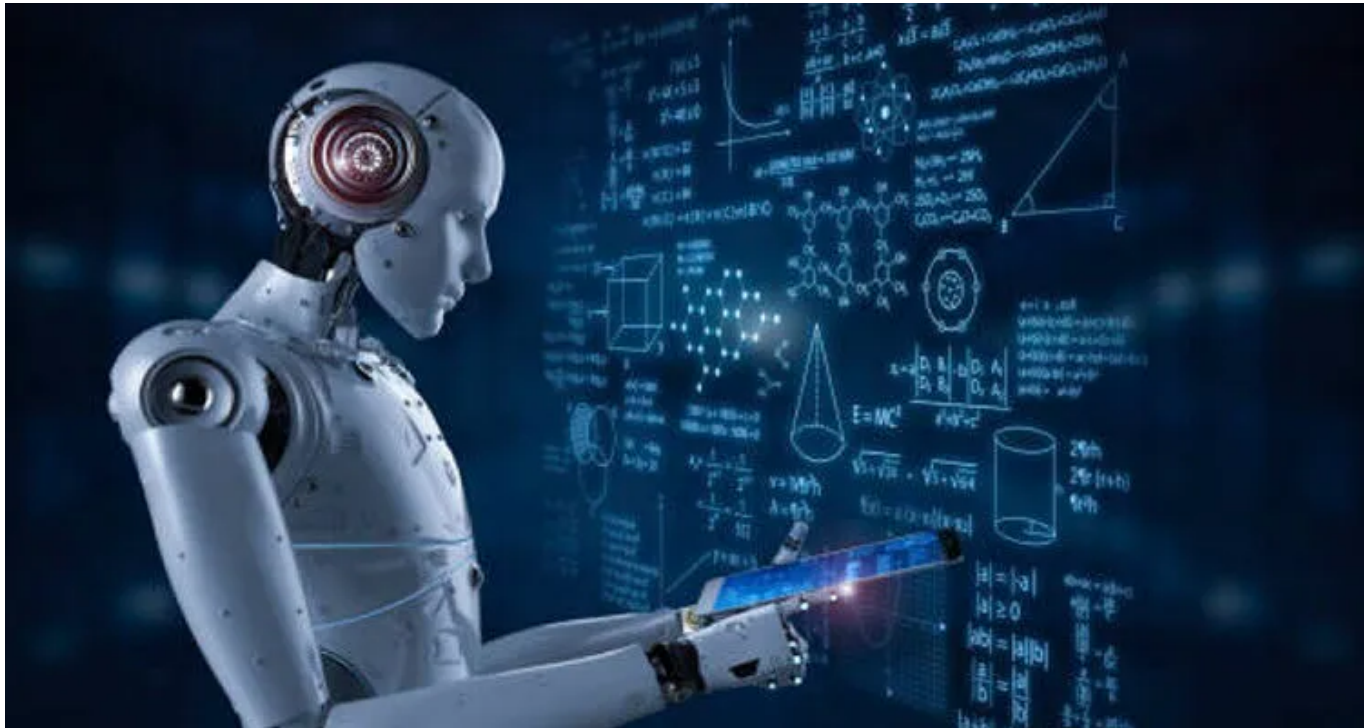
www.alarisworld.com/en-au | AskMe@kodakalaris.com | 1300 252 747



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

Are Autonomous Agents the Future of Data Management?



“Data Management is witnessing its ChatGPT moment,” claims Rohit Choudhary, founder and CEO of Acceldata, which has just launched its own Agentic Data Management (Agentic DM) platform.

“For too long, enterprises have struggled with fragmented, inefficient, and reactive data operations—where teams spend more time firefighting issues than extracting value,” said Choudhary.

“Agentic Data Management eliminates this complexity by making data management autonomous, intelligent, and self-healing, all while ensuring reliability at scale. Now is the time for change as AI redefines how businesses operate, compete, and innovate.

“Organizations that fail to modernize their data management strategies will find themselves at a severe disadvantage in an AI-first economy.”

The Agentic DM platform offers several capabilities to address enterprise data management challenges:

AI Agents: Deeply understand data context, detect anomalies, and take precise corrective actions - either without human intervention or with a human in the loop. By continuously learning from data patterns, it demystifies complexity, ensures reliability, and optimizes AI and analytics workloads in realtime. This intelligent, autonomous approach transforms data management from a reactive process into a proactive, AI-powered system that keeps enterprises ahead of disruptions.

xLake Reasoning Engine: At the core of Agentic

DM, xLake is a powerful, scalable AI-aware data processing engine that runs anywhere - hyperscalers, data clouds, and on-premise environments. Proven at exabyte scale, it significantly surpasses traditional data quality systems, data governance systems, data catalogs and other observability tools. With built-in data management and business ontologies, the xLake Reasoning Engine understands the fine-grained nuances of managing data within the enterprise business context, offering a completely new way of managing data.

The Business Notebook: is a collaborative, notebook-style interface that lets teams interact with data using natural language. With contextual memory, it continuously learns, recalls past decisions, and explains its reasoning - making AI-driven data management more transparent and intelligent over time. Its interactive visualizations transform complex data into clear, actionable insights, empowering confident decision-making.

Agent Studio: Empowers enterprises and partners to build and deploy their own AI agents within the Agentic DM platform. With a rich API and the ability to orchestrate workflows using multiple agents, organizations can create tailored automation for their unique data management needs. This flexibility enables true autonomy, allowing businesses to optimize, govern, and scale their data operations with AI-driven precision.

Acceldata Agentic DM is currently in private beta with several large enterprises. It launches with over 10 Agents including Data Quality, Profiling, Anomaly Detection, Data Drift, Cost, and Query Optimization.

<https://www.acceldata.io/>

archTIS announces Direktiv Acquisition

ASX listed archTIS has completed the US\$750,000 purchase of open-source workflow engine Direktiv’s, and will integrate its attribute-based access control (ABAC) and event-driven orchestration platform into its product offerings.

The acquisition will extend archTIS’ data protection capabilities to include access control management across enterprise infrastructure, data lakes, and applications. This expansion is particularly significant for organizations required to implement zero trust architectures as a defense against increasing cyber threats.

“I am excited to announce the completed acquisition of Direktiv’s technology, employees and customers,” said Daniel Lai, archTIS Managing Director and CEO.

“The acquisition positions us to accelerate product improvements, shorten time to market, and cross sell to offer our joint customers a comprehensive solution for securing and integrating various types of data using data-centric, zero trust enabled technology. The integration of Direktiv’s technology enhances our ability to implement zero trust across network, server and application data, establishing archTIS policy orchestration as the backbone connecting all of these points.”

The asset purchase will also enhance archTIS’ innovation capabilities by integrating the Direktiv development and technology teams from Europe and Australia to support the expansion of the company’s portfolio of products for securing data and infrastructure.

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

Cloudflare Threat Intelligence Tool

Cloudflare has unveiled its new Cloudforce One threat events platform, designed to deliver realtime intelligence on cyberattacks occurring across the global internet landscape.

The platform is available Cloudforce One subscribers and leverages the company’s extensive global network infrastructure, which reportedly blocked an average of 227 billion cyber threats daily during the final quarter of 2024.

As cybercrime costs are projected to reach a staggering \$US10.5 trillion this year, organizations face an increasingly urgent need for comprehensive threat intelligence. Traditional threat feeds have often been criticized for providing alerts without sufficient context or actionable information.

Built on Cloudflare Workers AI, the new platform aims to provide organizations with a consolidated view of attack streams across the internet. The company claims this will enable security teams to prioritize the most pressing threats specific to their environment, industry, or region.

The platform provides detailed information about threat actors, including indicators of compromise (IoCs) and tactical profiles that break down methods used in attacks. This level of detail is intended to help security teams respond more efficiently to emerging threats.

Blake Darché, Head of Cloudforce One at Cloudflare, highlighted the problem of information overload in cybersecurity: “Most industry tools flood security teams with threat intelligence that’s irrelevant, often leading to false positives and/or negatives.”

The new platform promises to filter out this noise, keeping organizations focused on real threats ranging from minor risks to complex scenarios like CVE exploitations or insider threats.

<https://www.cloudflare.com/en-gb/application-services/products/cloudforceone/>

Quantum-Ready Security Solution

DigiCert, a global provider of digital trust solutions, has announced the integration of UltraDNS into its flagship DigiCert ONE platform. This strategic move combines Public Key Infrastructure (PKI) and Domain Name Systems (DNS) into a unified digital trust platform designed to reduce outage risks and streamline operations.

Today, DNS teams manually change records with every PKI update. But as disruptors like shortened certificate lifespans and quantum computing drive faster change cycles, manual processes can no longer keep up. Frost and Sullivan advises organisations to automate manual processes and streamline trust solutions to keep digital interactions secure and flowing.

DigiCert ONE addresses these challenges by enhancing cryptographic agility and automating key processes that keep digital trust infrastructure aligned.

“As organisations across APAC accelerate their digital transformation, they require solutions that simplify security operations while ensuring compliance and resilience in the quantum age,” said James Cook, Group Vice President Sales, APJ, at DigiCert.

The combined platform offers several key advantages according to DigiCert, including unified digital trust management, improved uptime and business continuity, automated security and compliance processes, and enhanced performance and security features.

According to Ozgun Pelit, Senior Industry Analyst at Frost & Sullivan, the integration addresses critical challenges that enterprises face with fragmented security infrastructures.

“As certificate lifecycles shorten and cyber threats grow more sophisticated, solutions that streamline digital trust management will become essential for enterprises navigating an increasingly complex security landscape,” Pelit said.

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

From Bookeye to BookTEK: Image Access Modernises Brand



In a strategic rebranding move, Image Access, manufacturer of large format scanners and digitization solutions, has announced that its Bookeye product line will now be known as BookTEK.

The Wuppertal, Germany-based manufacturer indicated that the name change aligns the book scanner line more closely with its existing WideTEK scanner brand, creating a more cohesive product portfolio.

The company emphasized that while the name is changing, customers can expect the same high-precision technology that has made the scanners popular among libraries, archives, and collections worldwide.

“The new name BookTEK stands for the high-precision technology that not only delivers detailed images but also focuses on the preservation of valuable assets,” said a company representative. The BookTEK name has been registered in more than 50 countries, reflecting the global reach of Image Access products.

The BookTEK line features 10 different scanner models with formats ranging from A3 to A1+ and scanning resolutions up to 600 dpi.

BookTEK scanners are currently used by global institutions including the National Libraries and Archives of Russia, Japan, Nigeria, and Norway, as well as Queens University Belfast, Harvard University, The Museum of Modern Art, National Archives of Australia and the Parliamentary Libraries of Australia, SA and VIC

With 25 years of experience behind the technology, Image Access now claims to offer “the most comprehensive portfolio in the industry” through its combined WideTEK and BookTEK scanner lines.

For customers in Australia, New Zealand, Papua New Guinea, and Pacific Islands, DocuVan serves as the authorized distributor for the newly branded BookTEK scanners.

<https://www.docuvan.com.au/book-scanners/>

Digitech Systems Adds Generative AI

Digitech Systems announced the availability of AI Query within Sys.tm Intelligence, a flexible GenAI tool that enhances the Sys.tm information management and automation platform.

Sys.tm Intelligence enables workers to embed generative AI tasks like document summarization and outlining, report creation, and new content creation directly into automated business processes. Intelligence also inherits Sys.tm’s modular design and usage-based pricing.

Numerous time-consuming business tasks can be simplified through the implementation of generative AI. While workers can see the potential, however, many aren’t sure how to get started. In Sys.tm, GenAI tools are available within an employee’s information management platform, so they don’t have to learn a new system or interrupt their flow to embed AI into their work. In addition, Sys.tm Flows, the Business Process Management (BPM) service already available in Sys.tm, enables GenAI tasks to be seamlessly executed as part of an automated workflow.

For example, instead of spending days manually collecting monthly sales figures and compiling the information by hand into an annual report that also identifies important trends, a Sys.tm user would simply choose which documents to pull data from and ask the service to compile the information.

With Sys.tm, a Business Process Management (BPM) service already available within Sys.tm, AI generated content can be output directly to a document and even emailed to approved individuals.

“Every business today, needs to evolve quickly to meet customer needs and to stay ahead in their marketplace,” says Digitech Systems CEO, HK Bain.

“Generative AI offers significant promise of streamlining efficiencies to reduce costs while simultaneously enabling employees to spend more time on revenue-generating tasks. However, it’s been hard for many workers to understand how to apply the tools to the content-based parts of their jobs in a way that positively impacts revenue.

“Sys.tm Intelligence makes it easier for any business to utilize GenAI as part of an automated business process, so report generation, document summaries, and more get created simply and automatically within the normal business environment.”

The cloud-based service innovates how businesses consume and pay for these foundational capabilities. Built using a [microservices architecture](#) (also known as composable and flexible consumption), Sys.tm allows users to turn on more features as needed, but they only pay for the capabilities they actually use. Sys.tm eliminates the expense of traditional software licenses or cloud services tiers where as much as 80% of the purchased features are rarely, if ever, used.

<https://www.sys.tm/welcome>

Hyland Expands AI Capabilities

Hyland has unveiled new AI advancements to Hyland Automate and Hyland Knowledge Discovery, along with major updates to its core products Hyland OnBase and Hyland Alfresco.

“We continue to deliver on the unified Content Innovation Cloud roadmap and meet evolving customer needs by extending the value of their Hyland solutions,” said Leonard Kim, Hyland’s Chief Product Officer.

“Our latest product enhancements also support the importance of content intelligence and AI agents in content services – equipping organizations to better access and act on the insights hidden in their enterprise content, enhance data extraction and intelligently automate critical business processes.”

Hyland Knowledge Discovery now empowers organizations with actionable business insights through natural language queries.

Users can leverage AI agents and retrieval-augmented generation (RAG) to streamline complex searches and generate accurate information directly from enterprise content.

The new Agent Focus feature allows users to refine search results by specifying metadata fields and applying dynamic filters. Additionally, users can verify AI-generated content by accessing source documents.

Hyland Automate introduces a new AI-powered chat interface that transforms natural language prompts into automated process workflows. The platform now features a connector for OpenAI that enables integration with existing OpenAI/Azure OpenAI accounts, as well as a new integration with Microsoft email to simplify automation of email-based tasks.

OnBase Foundation 25.1 delivers AI-driven insights through advanced tools, new scalable app-building features, and enhanced workflows to improve operational flexibility. The update aims to help users unlock valuable business insights, streamline workflows, and automate processes with greater ease.

Alfresco 25.1 adds capabilities to manage removal of content from legal hold, leverage an extended event parsing library, and automatically archive or delete completed processes to improve performance and scalability.

The company has also announced expanded capabilities and configurable security controls for Hyland for Workday, an approved Built on Workday application that helps Workday HCM and Finance customers manage content associated with Workday records directly from Workday screens.

Hyland’s solutions are currently used by thousands of organizations worldwide, including more than half of the Fortune 100 companies.

<https://www.hyland.com/en>

Power Automate M365 Archiving

Preservica has announced that a Power Automate connector for Preserve365, its embedded archiving and Digital Preservation solution for Microsoft 365, is now available on the Microsoft Power Platform.

The Microsoft-verified connector allows information management teams to create Power Automate workflows that integrate Preserve365 with over 400 other applications on the Power Platform.

This enables organizations to standardize and automate the archiving of long-term records stored in Microsoft SharePoint.

The connector allows files, folders, lists, and libraries to be seamlessly moved or copied to the Preserve365 preservation archive.

This helps organizations optimize SharePoint usage and maintain a foundation of trusted, usable long-term content that is AI-ready and instantly accessible to business users for compliance, legal, and operational needs.

The Preserve365 connector APIs enable files, folders, lists and libraries to be seamlessly moved or copied to the embedded Preserve365 preservation archive to optimize SharePoint usage and create a foundation of trusted usable long-term content that is AI-ready and instantly available to business users from within SharePoint for compliance, legal and operational needs.

Power Automate and now Microsoft Copilot natural language programming can be used to create workflows – from gated steps including email triggers up to full automation and integration with Microsoft retention labels – saving hours of repetition, review and discovery by Records and Information Management teams. Preservica will also be adding workflow templates to the Preserve365 connector over time.

<https://preservica.com>

Secured Signing Taps Azure

Digital signature provider Secured Signing has announced a strategic partnership with Microsoft Azure that will utilize multi-region data centres to improve service delivery for businesses across Australia and New Zealand.

The collaboration aims to provide enhanced digital signature solutions that comply with local regulations while offering improved processing speeds and strengthened security protocols for the ANZ market.

“This milestone reinforces our commitment to delivering secure, reliable solutions tailored for the ANZ market,” said Mike Eyal, CEO of Secured Signing.

“Azure’s robust infrastructure allows us to achieve exceptional performance and scalability while

meeting ANZ compliance standards, enabling regional businesses to thrive.”

Through this partnership, Secured Signing will store Australian users’ data within Australia and New Zealand users’ data within New Zealand, ensuring compliance with local data protection laws including the Australian Privacy Principles and the New Zealand Privacy Act.

Key benefits for ANZ businesses include enhanced security through end-to-end encryption and advanced threat protection, improved disaster recovery capabilities, and global scalability to support business expansion.

Secured Signing provides digital signatures and Remote Online Notarization solutions for organizations of all sizes, with a focus on compliance, security, and workflow streamlining.

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

SER Group Acquires IDP Innovator Klippa

SER Group, a German provider of Intelligent Content Automation solutions with its Doxis platform, has announced the acquisition of AI company Klippa, an innovator in the rapidly evolving Intelligent Document Processing (IDP) market.

By combining Klippa’s cutting-edge IDP capabilities with SER’s Doxis Intelligent Content Automation platform, SER is doubling down on Smart Content apps that underpin customers’ digital transformation efforts, unlocking greater organizational agility and significant cost savings.

Since its founding in 2015, Klippa has demonstrated high growth and profitability, helping global enterprises such as Eurofins, SNCF and Siemens save time, reduce costs, and prevent errors and fraud.

Klippa’s DocHorizon is a cloud-based AI platform that digitizes and automates document-centric workflows. The platform allows users to visually design AI workflows and seamlessly integrate them with data flows across enterprise applications.

As a Peppol-certified provider, Klippa plays a key role in electronic invoice processing for businesses worldwide. Following the acquisition, all of these capabilities will be rapidly embedded within Doxis and further developed as a stand-alone platform.

“Joining forces with SER Group represents a huge growth opportunity for Klippa,” says Yeelen Knegetering, CEO of Klippa.

“By bringing our solutions together, we will unlock new use cases and provide even higher automation rates to enterprise customers around the globe. The next phase of this journey is incredibly exciting.”

The transaction is subject to customary regulatory approvals.

<https://www.sergroup.com/en/>

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

Microsoft Tackles “Shadow AI” with New Security Tools



Microsoft has announced a significant expansion of its Security Copilot platform with new AI agents designed to autonomously handle critical cybersecurity tasks, allowing human defenders to focus on more complex threats.

The update introduces six Microsoft-built security agents and five partner-built agents that will be available for preview in April 2025.

The announcement comes as Microsoft’s Threat Intelligence now processes an astounding 84 trillion signals daily, revealing exponential growth in cyberattacks including 7,000 password attacks per second and over 30 billion phishing emails detected in 2024 alone.

“The relentless pace and complexity of cyberattacks have surpassed human capacity and establishing AI agents is a necessity for modern security,” said Vasu Jakkal, Corporate Vice President of Microsoft Security.

The six new Microsoft Security Copilot agents include a Phishing Triage Agent that identifies real threats versus false alarms, Alert Triage Agents for data loss prevention, a Conditional Access Optimization Agent for identity management, a Vulnerability Remediation Agent that prioritizes security patches, and a Threat Intelligence Briefing Agent that curates relevant threat data.

Five additional partner-built agents will also be available, including solutions from OneTrust, Aviatix, BlueVoyant, Tanium, and Fletch, addressing specialized security needs from privacy breach response to network supervision.

Microsoft is also introducing new AI-powered data security investigation tools that will help

organizations understand and mitigate sensitive data exposure through deep content analysis. This feature will be available for preview starting April 2025.

The announcement addresses growing concerns around AI security, with Microsoft citing a new report indicating that 57% of organizations have experienced increased security incidents from AI usage, while 60% have not yet implemented AI controls.

To help organizations secure their AI investments, Microsoft is extending its AI security posture management beyond Microsoft Azure and Amazon Web Services to include Google VertexAI and all models in the Azure AI Foundry catalog, with preview availability set for May 2025.

The company is also enhancing protections for emerging AI threats with new detections for risks identified by the Open Worldwide Application Security Project (OWASP), including indirect prompt injection attacks and sensitive data exposure.

To address the growing “shadow AI” phenomenon, where employees use unauthorized AI applications, Microsoft is making its AI web category filter generally available in Microsoft Entra internet access, allowing organizations to control which users can access different types of AI applications.

Additionally, Microsoft announced that Defender for Office 365 will expand to protect Microsoft Teams against phishing and other cyberthreats starting in April 2025, addressing the growing use of collaboration software as a target for attacks.

Alexander Stojanovic, Vice President of Microsoft Security AI Applied Research, emphasized that this is “just the beginning,” promising continued innovation in security AI research to deliver greater value to customers “at the speed of AI.”

Data Management for Hybrid Cloud

In a move aimed at addressing the challenges of managing rapidly expanding unstructured data environments, Datadobi has announced the general availability of StorageMAP 7.2, the latest version of its vendor-neutral data management platform.

The release comes at a critical time for enterprise IT departments, with unstructured data growing at a staggering 30-50% annually and Infrastructure & Operations (I&O) leaders increasingly adopting hybrid cloud storage strategies. According to Gartner, over 70% of I&O leaders will implement hybrid cloud storage by 2028, up from just 30% last year.

StorageMAP 7.2 introduces several key enhancements designed to improve visibility and control across data environments. The updated platform features expanded metadata query capabilities that enable organizations to track cost, carbon emissions, and StorageMAP tags with greater precision.

The platform includes new archiving features that help organizations identify and relocate old or inactive data to archive storage, freeing up primary storage capacity. Additionally, StorageMAP 7.2 enhances AI readiness by finding and classifying data suitable for GenAI processing, enabling businesses to feed data lakes with relevant, high-quality datasets.

The update also introduces automated discovery for Dell ECS and NetApp StorageGRID object stores, allowing enterprises to instantly identify tenants and their associated S3 buckets, simplifying the management of large-scale object storage environments.

Building on its existing orphaned data reporting functionality over the SMB Protocol, StorageMAP 7.2 now extends support to NFS environments, enabling businesses to identify and report on orphaned data for all data accessed over SMB and/or NFS protocols. This approach enables quick identification of data that is not currently owned by any active employee.

Additionally, an enhanced licensing model provides organisations with the flexibility to scale their use of StorageMAP's features according to their specific requirements.

StorageMAP 7.2 also optimizes the storage of data by helping businesses free up primary storage capacity and optimize AI data workflows. This includes new archiving capabilities that allow organizations to identify and relocate old or inactive data to archive storage, ensuring that high-value primary storage remains efficient and cost-effective.

Additionally, the platform enhances AI readiness by finding and classifying data suitable for GenAI processing, enabling businesses to feed data lakes with relevant, high-quality datasets.

<https://datadobi.com/>

TWAIN Working Group Certification

The TWAIN Working Group (TWG) and Keypoint Intelligence have joined forces to launch a new subscription-based Testing and Certification Program for TWAIN Direct and PDF/Raster technologies.

The program aims to help developers, independent software vendors, and scanning device manufacturers ensure their products comply with the latest TWAIN Direct standards while improving hardware and software interoperability across the document imaging ecosystem.

According to TWG, the new certification program features thousands of automated scripts, tests, and verifications to streamline development processes and quickly identify areas needing improvement. The tools can significantly reduce development time while ensuring strict adherence to TWAIN Direct standards.

"TWAIN Working Group's new Testing and Certification Program empowers software developers and document scanning device manufacturers to enhance product interoperability, reduce time-to-market, and provide end-users with highly reliable solutions," said Joseph Odore, Chairman at TWAIN Working Group.

"By offering a comprehensive and automated testing framework, we are reinforcing our commitment to advancing document imaging standards."

The certification program is structured as an annual subscription service with tiered pricing. The standard rate is \$US10,000 per year, while TWAIN Working Group Board Members receive a substantial 70% discount (\$US3,000 per year) and Associate Members qualify for a 30% discount (\$US7,000 per year). Hardware testing and certification services will be handled directly by Keypoint Intelligence.

The program targets three key stakeholder groups:

End-user corporations seeking document imaging solutions that meet stringent compliance standards and integrate seamlessly with enterprise workflows

Software developers looking to gain competitive advantages by certifying their solutions against industry standards

Scanning device manufacturers aiming to accelerate time-to-market while ensuring product quality and interoperability

The TWAIN Working Group, founded in 1992, has long been committed to creating standards that benefit the imaging industry, with a mission focused on "Promoting Standards for Secure Image Data." Current members include companies such as Epson America, HP, Kodak Alaris, and various technology providers in the document imaging space.

<https://twain.org>

Leading Records Management Text Updated for AI Era

In an era where data management challenges are multiplying exponentially, information professionals have a new resource at their disposal. The American Library Association's Neal-Schuman imprint has published the third edition of *"Records and Information Management,"* a reference text for both students and RIM professionals.

Author Patricia C. Franks, PhD, has thoroughly updated the work to address rapidly evolving technologies, including artificial intelligence, machine learning, blockchain, and Web3.

The new edition retains its comprehensive coverage of records lifecycle management while expanding into emerging areas of practice.

It includes an overview of the origins and development of records and information management, also examining the discipline of information governance and the steps to develop a strategic records and information management plan.

"The field has changed dramatically since the previous edition," said a spokesperson for ALA Neal-Schuman.

"This update arrives at a critical time when organizations are struggling to manage increasingly complex information ecosystems."

The book covers the complete spectrum of modern records and information management (RIM), addressing everything from traditional paper documents to digital communications like email, chat messages, and software-as-a-service platforms.

An entirely new chapter is dedicated to demystifying data governance, automation, and artificial intelligence applications in records management.

It presents complete coverage of the records and information lifecycle model, encompassing paper, electronic (databases, office suites such as Microsoft 365, email), and new media records (blogs, chat messages, and software as a service), while acknowledging in every chapter the influence of emerging and developing technologies and encouraging new ways of meeting the resulting challenges.

Franks, a professor emerita at San José State University, brings substantial credentials to the work. She is a past president of the National



Association of Government Archivists and Records Administrators (NAGARA) and currently participates in the InterPARES Trust AI research project, where she leads teams exploring AI applications in archives and records management.

The text is designed to serve both students and professionals, with instructor materials available including customizable PowerPoint slides. Examination copies are being offered to instructors considering the book for course adoption.

The comprehensive approach - covering everything from strategy development to disaster recovery - positions the book as both a classroom text and a professional reference.

The third edition of *"Records and Information Management"* is available now through the ALA Store, with all purchases supporting advocacy and professional development for library and information professionals worldwide.

<https://alastore.ala.org/RIM3ed>

DISCOVER THE UNMATCHED EFFICIENCY OF OPEX® FALCON+® SCANNERS

Combining one-touch scanning with the intelligence of CertainScan® software, OPEX® provides seamless digitisation solutions for high volume, confidential records, transforming unstructured paper files directly into dynamic content.

With the power to digitise medical, legal and virtually any other documents directly from the envelope or folder, the OPEX® Falcon+® series of scanners are the market leading product for scanning, supporting workflow efficiency and delivery.

**"THE SCANNERS ALLOW US
TO UTILISE ALL OUR PEOPLE
AND RESOURCES. WE CAN
LEVERAGE OPEX'S TECHNOLOGY
TO BE MORE COMPETITIVE IN OUR
FIELD AND CONTINUE TO GROW."**

-Michael Basham
Commercial Director, Paragon



**FIND OUT HOW WE CAN HELP
MAXIMISE YOUR BUSINESS**

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

