

Insights, Strategies, and Practical Applications

November 2024



CONTENTS

Unlocking the Potential of AI: An Introduction	03-04
A Focus on Security	05-06
Cloud Security Barriers and Challenges	07
Spotlight: Navigating AI and Security: Insights from Microsoft and the Future of Workplace AI	08-09
Transforming AI Integration with Devices: A New Era of Computing	10-11
Windows 10 End of Support: Why the Time to Upgrade is Now	12
Channel Partner Opinion	13-14

Introduction

Unlocking the potential of AI is no longer a futuristic concept; it is actively transforming how businesses operate across various industries. From automating routine tasks to providing real-time data insights, AI presents immense opportunities for real world business growth and outcomes.



In the ANZ region, businesses are increasingly ready to adopt AI, harnessing its potential to drive competitive advantages. AI's influence extends far beyond mere automation. It enhances smarter decision-making, boosts operational efficiency, and supports innovative product development. Businesses are better equipped to remain agile in a fast-paced market through AI-driven customer service solutions and advanced data analytics platforms.

While automation has already changed the landscape, AI elevates it to another level by learning from data, adjusting processes, and ensuring more accurate outcomes.

AI-driven devices can automate repetitive tasks and complex operations requiring cognitive capabilities, such as data interpretation, improving workflows, and enabling real-time strategy adjustments. For Managed Service Providers (MSPs), AI-based automation tools streamline operations and increase efficiency.

AI-powered data solutions enable businesses to gather, analyse, and interpret vast amounts of data at unprecedented speed and scale. These systems allow companies to make proactive, informed decisions based on trends and patterns that might otherwise go unnoticed. More ANZ businesses are leveraging AI analytics to predict customer behaviour and optimise marketing strategies, resulting in more personalised and targeted campaigns.

The future of AI in the ANZ region holds enormous promise. From improving customer experiences to driving innovation across sectors such as finance, healthcare, and retail, AI capabilities will continue to grow as more businesses adopt the technology.

The key question is not whether to embrace AI but how to integrate it in ways that align with business goals and unlock new opportunities.

For partners, AI presents a unique opportunity to add value and assist clients in navigating the complexities of digital transformation. By offering AI solutions that address specific business challenges, partners can position themselves as indispensable allies in their customers' success. There is a growing appetite for AI-driven growth in ANZ, with businesses eager to explore how AI can give them an edge.

As the AI ecosystem rapidly evolves, businesses and their channel partners must be prepared to leverage AI fully. This preparation involves addressing challenges around infrastructure, skills, and integration. With a robust framework, ANZ businesses can capitalise on AI's potential to drive new growth, unlock efficiencies, and transform operations.

Recent research among ANZ business and IT leaders highlights a growing recognition of AI's potential and the strategic steps necessary for partners to capitalise on this trend. According to a [Deloitte report](#), over 60% of ANZ executives believe AI will significantly impact their industries within the next five years, with 72% planning to boost their AI budgets in 2024, reflecting the urgency to integrate AI into operations. A [PwC survey](#) reveals that 43% of ANZ businesses have implemented AI, with another 38% planning to adopt it soon.

How prepared are you?

- **AI Adoption Challenges:** Many companies lack AI specialists and essential digital skills, making implementation difficult.
- **Strategic Alignment:** AI should be deployed with clear business goals in mind, not just for modernisation. Specific use cases, like improving employee onboarding, should guide AI integration.
- **Security and Compliance:** AI increases data security risks, and businesses must have clear guidelines to prevent exposing sensitive information.
- **AI Readiness:** Conducting a readiness assessment is critical to identify potential risks, vulnerabilities, and barriers to AI adoption.
- **Importance of Training:** Preparing employees to effectively use AI tools like Microsoft Copilot is essential for successful integration.

The Key is Delivering Real Value

Businesses must strategically plan AI implementation by identifying key use cases, conducting thorough readiness assessments, and ensuring proper training and security measures are in place. This approach ensures AI integration delivers real value and avoids unnecessary risks.

A Focus on Security

As organisations increasingly rely on AI and cloud technologies, the intersection of AI and security operations has become a pivotal area of focus.

Security First Approach

While AI advancements offer significant benefits, they cannot guarantee comprehensive security on their own.

The migration of workloads to the cloud necessitates secure implementation strategies to safeguard sensitive data against evolving threats.

One of the primary considerations is the urgent need for organisations to adopt a proactive, security-by-default approach as they modernise applications and shift to multi-cloud environments. This strategy is crucial in addressing the sophisticated nature of contemporary cyber threats, including phishing attacks that have become increasingly convincing due to the misuse of AI technologies.

A critical element in enhancing security operations is **ensuring that AI-generated outputs are reliable**. As misinformation becomes a growing concern, maintaining trust in AI applications is essential, particularly in security contexts where accurate data and insights are paramount. Organisations must prioritise responsible AI usage to foster secure environments for their customers.

In addressing the evolving threat landscape, organisations need to shift away from a "**build first, secure later**" mindset.

The deployment of cloud services requires immediate attention to security measures, as newly created resources can become accessible to external entities almost instantly.

Moreover, relying solely on general-purpose AI is insufficient for specialised security tasks like threat detection. Organisations must implement specialised systems that ensure transparency and accuracy in security operations. As AI and automation are increasingly leveraged to alleviate the manual burden on security analysts, there is a significant opportunity for a semi-autonomous security model to emerge. This model allows AI to handle routine tasks, enabling security teams to concentrate on more complex decision-making processes.

Utilising **global threat intelligence** is another vital strategy for organisations to enhance their security posture. By monitoring advanced persistent threat (APT) groups and correlating this intelligence with internal activities, organisations can respond swiftly to potential risks.

In addition to these strategies, organisations must **prioritise data confidentiality** during cloud operations. Engaging in ongoing discussions about identity and access management is essential for mitigating risks and implementing an identity-first approach to cloud security.

A Focus on Security

To improve overall security, organisations should adopt four key principles:

Secure Foundations: Establishing secure frameworks ensures systems remain protected over time.

Management of Detection Rules: Regularly assessing and streamlining detection rules can help reduce noise and false positives in security alerts.

Leveraging Automation and Orchestration: Simplifying content management around automation enhances its effectiveness in security operations.

Natural Language Processing: Allowing users to pose complex security questions in natural language streamlines information retrieval and decision-making.

Organisations must embrace a proactive and comprehensive approach to cloud security, effectively managing permissions and leveraging advanced technologies to simplify security operations. As the threat landscape continues to evolve, the integration of AI into security practices must be grounded in responsibility, trust, and a commitment to protecting sensitive data.

Fast Facts

1. AI alone can't guarantee comprehensive security.
2. Proactive security strategies are essential when migrating to multi-cloud environments.
3. Misinformation and misuse of AI technologies can fuel cyber threats.
4. Security must be integrated at the start of cloud deployments to prevent vulnerabilities.
5. Leveraging automation and threat intelligence helps reduce manual work for security analysts.
6. Maintaining data confidentiality and enforcing strong identity and access management are critical for effective cloud security.
7. AI must be used responsibly to foster trust and protect sensitive data.
8. Natural Language Processing (NLP) enhances decision-making in security operations by simplifying information retrieval.

Cloud Security Barriers and Challenges

In today's digital landscape, organisations face significant cloud security challenges, particularly identity and access management. Implementing robust identity protection measures is crucial, as many users remain unaware of the tools and technologies available, leading to the underutilisation or mismanagement of access rights.

One major issue is the **generational gap** in technology understanding, which highlights the need for organisations to prioritise practical, problem-solving applications of technology rather than simply accumulating tools without a strategic intent.

For instance, innovative monitoring devices have been developed in the pork industry to detect signs of disease in pigs. These devices illustrate how technology can effectively address real-world problems, emphasising the necessity of identifying specific issues and working toward practical solutions.

Additionally, fostering creativity in problem-solving requires focusing on understanding the problem before seeking solutions. Organisations should strive to find individuals skilled at addressing these challenges and consider how their solutions can align with the business's overall goals.

Transparency within organisations is also vital for building trust with customers. This encompasses both operational transparency and clarity around technical processes,

What Next?

To effectively address cloud security challenges, organisations must focus on applying technology in a purposeful, solution-driven manner. It's not about having more tools, but about using the right ones strategically while ensuring clear communication and trust with customers.

Emphasis on strengthening identity and access management, investing in educating users on the available security tools, and promoting transparency to build customer confidence in their security practices.

ensuring that organisations communicate their commitments and measures to protect customer data.

Ultimately, a thoughtful, problem-centric approach to leveraging technology and enhancing security is essential. By focusing on effective communication and trust-building, organisations can navigate the complexities of cloud security and create a more secure environment.

Spotlight

Navigating AI and Security: Insights from Microsoft and the Future of Workplace AI

During a recent keynote address, **Philip Meyer, Partner Technology Strategist at Microsoft** emphasised the integral role of AI in every aspect of Microsoft's technology development. He stated that all cloud services, Windows, and Office projects are designed with AI at their core. This seamless integration signifies a strategic shift, highlighting that AI is not a separate initiative but a foundational element of all technological advancements.

Meyer outlined five key priorities for fiscal year 2025, each accompanied by solution playbooks and guides that showcase the inclusion of AI in all initiatives.

Two priorities were highlighted in detail:

- **Copilot:** The vision is to have AI Copilot functionality on every desk, drawing a parallel to the historic goal of having a PC on every desk.
- **Microsoft 365 Security:** Focuses on enhancing security and compliance, addressing the challenges of adopting AI without proper governance.

Referencing similar discussions in major tech events like Dreamforce, **Meyer** underscored that security is crucial for successful AI implementation.

Key Areas of Future Growth and Partner Opportunities

Substantial opportunities exist for partners in the current landscape. By leveraging Microsoft 365 Copilot and focusing on adoption, change management, and implementation services, partners can anticipate a tenfold increase in revenue.



Edge Computing and Disaster Recovery

Azure's backup capabilities, site recovery solutions, and edge computing initiatives present significant opportunities for partners to engage with clients. Case studies from major retailers investing in edge computing highlight the increasing demand for resilient solutions in regional Australia, showcasing the market potential for partners.



Migration Opportunities

There is a significant opportunity in the market, with approximately 5 million devices still running Windows 10 in Australia. As the end of service for Windows 10 approaches, this is a crucial moment for partners to engage with customers about upgrading to modern, secure Windows 11 devices. AI-enabled PCs offer enhanced security and functionality, and partners can play a key role in facilitating the migration to these devices.

Spotlight

The Emergence of AI in the Workplace

The latest research reveals that AI is already making significant strides in the workplace, with a notable emergence of power users - individuals who effectively harness AI technology. However, there is a concerning trend of users who feel disenfranchised due to a lack of understanding of how to utilise these tools. This divide was echoed by **Marc Benioff** in his recent keynote at **Dreamforce**, emphasising the need to empower users to break through barriers and fully leverage AI's capabilities.

From a sampled 31,000 individuals in the **Work Trends Index** research, 84% of ANZ companies reported utilising generative AI in their operations, showcasing a rapid adoption rate. While this is promising, there are genuine concerns about reliance on consumer-grade AI tools in critical sectors like healthcare. For instance, medical professionals in the UK used ChatGPT for diagnoses, raising ethical questions about the adequacy of such tools in high-stakes environments.

The history of AI adoption is rich, dating back to the late 1950s, with significant advancements in generative AI, particularly with the introduction of Generative Adversarial Networks (GANs). However, the real breakthrough for generative AI occurred in November 2022 with the launch of ChatGPT. Despite its widespread use, the potential risks of employing consumer-grade AI technology for serious applications, especially given recent incidents where sensitive data was compromised, remain a concern.

This growing reliance on consumer-grade technology, where users trade their data for access to AI services, poses risks, particularly in industries where accuracy and security are paramount.



Revenue Growth

Recent research from IDC revealed that partners can expect to earn \$10.93 for every dollar spent by clients on Microsoft technology. This statistic underscores the lucrative opportunities available for partners who engage deeply in the Microsoft ecosystem.



Security as a Business Driver

Security emerged as a major focus, with its importance highlighted as the top priority for organisations today. Microsoft is reported to be ten times larger in revenue than any other security vendor, reflecting the comprehensive nature of their security offerings.



Cost-effective Solutions

Addressing the cost pressures faced by small businesses, there is a significant opportunity for organisations to achieve savings by utilising Microsoft's integrated solutions. By consolidating security vendors and adopting Microsoft's offerings, organisations can reduce operational costs while maintaining robust security measures. Emphasising the importance of securing client data reassures organisations that their information remains within their control while implementing necessary safeguards.



Product Recommendations

Tailored recommendations can enhance customer experiences, guiding them toward informed purchasing decisions.

Transforming AI Integration Across Devices

A New Era of Computing

Practical AI Applications Across Devices: Transforming Industries

The practical applications of AI are evident across devices from Microsoft, Google, HP, and Asus. These brands are integrating AI not just to boost performance but to solve real-world problems. For instance, AI-powered license plate recognition on public safety dash cams, or real-time voice enhancement during video calls, are transforming industries and elevating efficiency across different sectors.

AI's transformative power is reshaping the landscape and device manufactures like **Microsoft Surface, Google, HP, and Asus**, each offering unique AI-driven experiences that push the boundaries of performance, security, and user engagement.

Microsoft Surface Devices

Microsoft's journey into AI integration with Surface devices began with early innovations like Battery Protection Mode in 2017, which used machine learning to optimise battery performance. Over time, this evolved into sophisticated features like eye-gaze technology and advanced AI capabilities, such as Copilot, which are tested and optimised specifically for Surface devices.

Today, Microsoft categorises its Surface range into **AI PCs** and **Copilot Plus PCs**, each offering distinct advantages for AI-driven tasks. AI PCs, like the **Surface Pro 10** and **Surface Laptop 6**, feature Intel's Neural Processing Unit (NPU), designed to handle AI workloads with speed and efficiency, enhancing performance in real-time tasks

like image recognition and voice processing. Copilot Plus PCs, like the **Surface Pro 11th Edition**, are powered by Qualcomm's ARM-based processors, meeting high-performance AI benchmarks to deliver superior results in AI applications.

Surface's tight integration between hardware, AI, and cloud services provides a seamless experience, empowering users to unlock the full potential of AI while benefiting from Microsoft's holistic control over every layer of the technology stack.

Asus AI-Powered Performance and Personalisation

Asus has brought AI to the forefront of their **ZenBook** and **ExpertBook** series with innovations designed to enhance both performance and user experience. AI-powered features like AI Noise-Cancelling Mic and AI-powered Face Lock streamline everyday tasks and deliver a more intuitive user interface. Asus also integrates AI-driven thermal technology, which dynamically adjusts performance and cooling to optimise efficiency during heavy workloads.

A New Era of Computing

Google's AI Integration

Leading with Software Innovation Google devices, particularly through Pixel phones and tablets, showcase the company's prowess in AI integration with a focus on software. Google's AI features, such as **Google Assistant** and **Duplex**, push the envelope in personal productivity and natural language processing.

The introduction of **Gemini**, Google's advanced AI model, further enhances the capabilities of Google's ecosystem, offering improved contextual understanding and interaction.

Google's approach to AI on devices revolves around on-device machine learning, enabling real-time, offline functions like Google Lens for object recognition and Adaptive Battery for enhanced power management.

These innovations elevate Google's AI-enabled devices to the forefront of intelligent user

interactions, combining convenience with powerful AI tools. Through continuous advancements, Google is redefining the user experience, making everyday tasks more efficient and intuitive.

HP: Performance Meets AI in Enterprise Devices

HP's AI integration, particularly in their **Elite Dragonfly** and **Spectre** series, focuses on empowering professionals with tools designed to enhance productivity and security.

AI-based noise cancellation and automatic webcam framing are just a few of the features that show how HP leverages AI to improve everyday user experiences, particularly for video conferencing and remote work.

Their focus on AI-enhanced privacy, such as HP Sure View, which protects sensitive information from onlookers, demonstrates HP's commitment to secure, intelligent computing.

The Future of AI-Enabled Devices

Looking forward, the future of AI integration across devices from Microsoft, Google, HP, and Asus promises to bring even more powerful, efficient, and secure solutions.

Whether it's Microsoft's Copilot Plus PCs, Google's innovations in Assistant and real-time translations, HP's AI-enhanced enterprise security features, or Asus's personalised AI-driven user interfaces, businesses will have access to the latest advancements in AI-powered computing.

The AI revolution is only beginning, and with these major players leading the way, the next generation of AI-enabled devices will set a new standard for performance, security, and user experience.

Security and Privacy: AI's Role Across Devices

Security and privacy are central to AI integration, no matter the brand. Microsoft Surface devices use features like Windows Hello for secure biometric authentication, while Google devices focus on keeping data secure through on-device processing and features like Titan M Security Chip. HP incorporates AI-driven privacy filters, and Asus leverages AI-powered facial recognition to enhance security without sacrificing convenience. All these manufacturers are pushing to ensure that AI not only enhances performance but also provides robust security measures for data protection.

Windows 10 End of Support

Preparing for Windows 10 End of Support: Why the Time to Upgrade is Now.

With Windows 10 reaching its end-of-support on **October 14, 2025**, partners must plan for the transition to Windows 11. Delaying this upgrade could expose devices to security vulnerabilities, as Windows 10 will no longer receive updates or support.

Why Upgrade?

- **Security Risks:** Without updates, older devices become increasingly vulnerable to cyber threats and may lose compatibility with new applications and devices.
- **Modern Features:** Upgrading to Windows 11 Pro brings AI-enhanced capabilities, improved hardware, and features that boost productivity and employee satisfaction.
- **Seamless Deployment:** Microsoft provides tools like Intune, Entra ID, and Autopilot to facilitate the upgrade process, ensuring devices are secure right out of the box with features like TPM and Secure Boot.
- **AI Capabilities:** Tools like Copilot streamline tasks, enhancing productivity by allowing users to quickly analyse data and perform searches using natural language.
- **Compatibility Assurance:** Windows 11 boasts a 99.7% app compatibility rate with Windows 10, and Microsoft's App Assure program offers free support for any compatibility issues.
- **Legal and Financial Implications:** Not upgrading can have consequences, including invalidating cyber insurance policies that require supported operating systems.

Checklist to Streamline Adoption

- ✓ **Operating Systems:** Upgrade eligible PCs to Windows 11 Pro before October 14, 2025.
- ✓ **Devices:** Invest in new Windows 11 Pro devices for enhanced features.
- ✓ **Management:** Combine Windows 11 Pro with Microsoft 365 Business Premium for modern device management and data protection.
- ✓ **Endpoint Security:** Implement a security-by-default strategy across devices.
- ✓ **Buy-Back Program:** Consider a buy-back program for old PCs to facilitate device refresh and budget for upgrades.
- ✓ **Growth Path:** Upgrade to Windows 11 Enterprise for advanced security and management benefits.

Act Now

Don't wait until it's too late. Begin your upgrade to Windows 11 today to ensure your devices remain secure and your business stays competitive. Contact us for more information on how we can help streamline your transition.

Channel Partner Opinions

As the technology landscape evolves, AI plays an increasingly important role in transforming how businesses operate, but with this shift comes unique opportunities and challenges.

Our 2024 survey of over 150 of our partners across two states aimed to understand their thoughts and actions on the key issues surrounding AI adoption.

Notably, partners expressed a keen interest in exploring areas like machine learning and automation, recognising their potential to drive innovation. However, they also identified significant hurdles in implementation, particularly around data integration and workforce readiness.

With many partners planning to invest in AI-related technologies within the next year, there is a clear urgency to leverage AI effectively and help clients navigate the complexities of this rapidly evolving landscape.

Channel Partner Opinions

65.3%

are interested in exploring Generative AI and AI PC

60%

will prioritise AI Security

and

53.3%

will prioritise Automation and Workflows

45.7%

are planning to invest in AI-related technologies for their client's business within the next 3 months, **43.5% within the next 12 months,** and **10.8% currently have no plans.**

65.2%

see client knowledge as a major challenge in AI implementation

60.9%

are concerned about costs

while

60%

are concerned about security and lack of expertise

We are continually listening to your feedback, and committed to working together to deliver an agile managed services portfolio. Our initiatives and project roll-outs allow us to provide you with the right tools and support to ensure your business runs as efficient as possible.

If you are interested in getting started with AI, please connect with us at sales@au.synnex-grp.com

☎ 1300 100 100

✉ sales@au.synnex-grp.com

in [/synnexaustralia](https://www.linkedin.com/company/synnexaustralia)

X [@SynnexAU](https://twitter.com/SynnexAU)

b blog.synnex.com.au

f [/SynnexAU](https://www.facebook.com/SynnexAU)

ig [@synnexaustralia](https://www.instagram.com/synnexaustralia)

www.synnex.com.au

