FLOW

Tech Trends 2024: 10 Trends to Help You Get Ahead

Overview

As we've brought in 2024, there is no better time to reflect on 2023. The world of digital technology is ever-changing, and businesses should keep up to date with these changes to stay competitive and securely optimise productivity and output.

In this eBook, we will look back at the trends which have shaped 2023 and are paving the way for the incoming year. We will then turn our focus to the potential technology trends which will shape 2024, including trends such as cloud and AI integration to advanced security. These trends will help business leaders and decision-makers to prepare for 2024, what it means for your business and how these trends might impact your day-to-day operations.

Looking Back at 2023

As we reflect on the technological strides made in 2023, it's clear that this year has been a key driver for innovation and transformation. The technology trends of the past year have not only paved the way for new advancements but have also set the stage for 2024 - from the rise of AI-driven analytics to the proliferation of secure remote work solutions, 2023 has been a testament to human ingenuity and adaptability.

Let's take a nostalgic look back at the defining moments and breakthroughs that have shaped the technological landscape of this year.

The Rise of Generative AI

The year 2023 has indeed been a landmark year for generative AI, with its capabilities and applications reaching new heights. Generative AI, known for its ability to create new content ranging from text to images, has seen a significant leap in sophistication, producing content increasingly akin to human output.

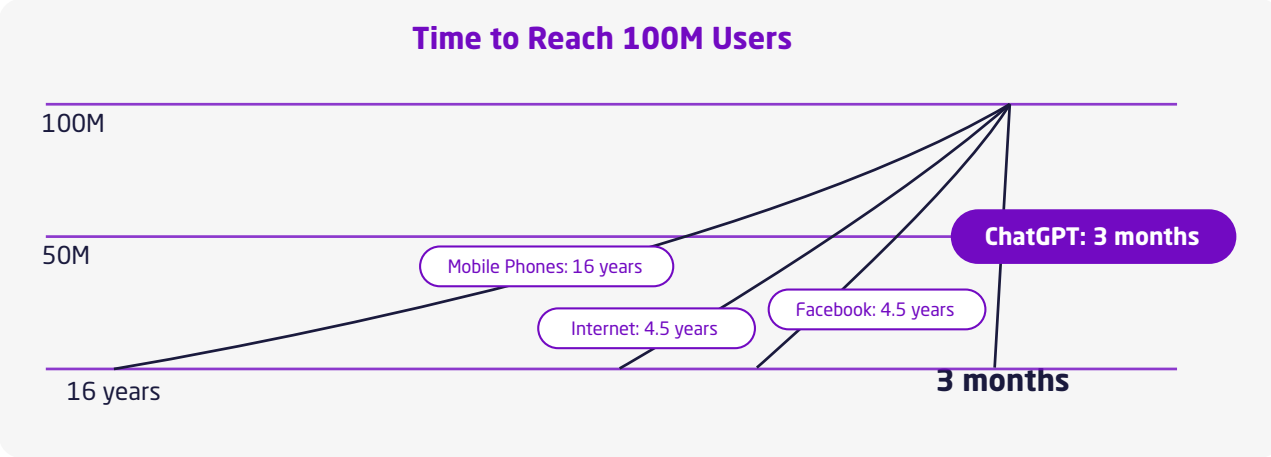
One of the most notable advancements has been in natural language processing (NLP). AI models like GPT-4 have showcased an ability to compose essays, poetry, and even code with nuance and coherence that has taken users and experts alike by surprise. In parallel, AI-driven design tools have empowered the creation of intricate graphic designs and artworks, expanding the horizons of creativity.

The implications of this technological surge are profound, AI systems are being used to produce marketing copy, compile reports, and support decision-making processes.

ChatGPT, a prime example of generative AI's reach, achieved a remarkable milestone by attracting 1 million users within just 5 days of its release.

This rapid adoption rate underscores the growing interest and potential impact of generative AI technologies in our daily lives and across various sectors.

However, with great advancement in Generative AI comes new challenges. The rise of generative AI raises critical ethical and economic questions, including concerns about copyright, authenticity, and the potential displacement of traditional human roles. As we progress, it is imperative to address these challenges with care, ensuring that generative AI augments human creativity and productivity, rather than supplanting it.



Skills Shortages

2023 was marked by the UK contending with a pronounced IT skills shortage, which has emerged as a critical challenge for businesses across the UK. An overwhelming 93% of UK enterprises recognise the IT skills gap, attributing it to the swift evolution of technology. This shortfall is intensified by insufficient training opportunities and relevant educational programmes, with 41% of firms identifying these as contributing factors.

The quest for technological expertise is pressing, with artificial intelligence (AI) topping the list of in-demand skills. Employers are on the lookout for workers capable of harnessing technology to spur innovation and efficiency.

AI could be instrumental in mitigating the IT skills deficit. By automating mundane tasks, AI can liberate human resources for more intricate and creative tasks. AI-powered tools can also aid in training and upskilling staff, offering personalised learning experiences that are scalable and cost-effective.

Moreover, AI can help narrow the skills gap by empowering non-experts to execute technical tasks via user-friendly interfaces, thereby democratising access to technology.

There are currently approximately 52,000 IT job vacancies unfilled in the UK, underscoring the persistent skills shortage in the tech sector. This highlights the urgency for initiatives that address this gap and support the growth of the UK's tech industry.

93%

of organisations recognise the IT skills gap, attributing it to the swift evolution of technology

41%

of organisations contribute this shortfall in skills to insufficient training opportunities and training programmes

> "AI is by far the most in-demand skill, but it is closely followed by IT support and cyber security"
>
> **Forbes, 2023**

Ever Expanding Attack Surfaces

The cybersecurity landscape in 2023 is facing a critical challenge with the ever-expanding attack surfaces, particularly in cloud environments. As businesses increasingly adopt multi-cloud strategies and remote work continues to be prevalent, the number of potential entry points for unauthorised access into systems has increased.

The complexity and interconnectedness of modern IT infrastructures have significantly contributed to this expansion. With multiple cloud service providers being used by a single organisation, the attack surface widens, creating more opportunities for cyber threats. User accounts for Software as a Service (SaaS) applications can be compromised, leading to unauthorised data access or malware uploads. Moreover, misconfigurations in cloud platforms can leave databases unprotected and development environments exposed.

APIs, which allow different apps and services to communicate within the multi-cloud ecosystem, further increase the attack surface due to their often-weak security, they can be easily exploited by threat actors, making them a critical point of concern.

The shift to remote work has also played a role in expanding attack surfaces.
During the pandemic, many organisations were unequipped in cybersecurity to support remote workers quickly, leading to vulnerabilities that persist in the modern workplace.

To manage these expanding attack surfaces, Chief Information Security Officers (CISOs) and IT teams need to adapt their cybersecurity strategies. This includes implementing robust attack surface management solutions and ensuring that employees are aware of the best practices for securing their work environments. As the attack surfaces continue to grow, proactive and comprehensive security measures will be vital to protect against the evolving threats in the cybersecurity and cloud domains.

10 Technology Trends in 2024

AI

Widespread Adoption of Copilots

Microsoft introduced Copilot for Microsoft 365 eight months ago to reduce digital debt and increase productivity so workers could focus on the work that matters. Research shows that Copilot has had a significant impact on early adopters. 77% of early users have noted that they do not want to go back to working without Copilot.

Aside from the productivity benefits, Copilot can also help workers become more creative, save time, and learn new skills such as copywriting, design, coding, and analysing data by amplifying expertise and filling in a capacity gap.

Microsoft 365 Copilot
Work alongside you in the apps you use every day

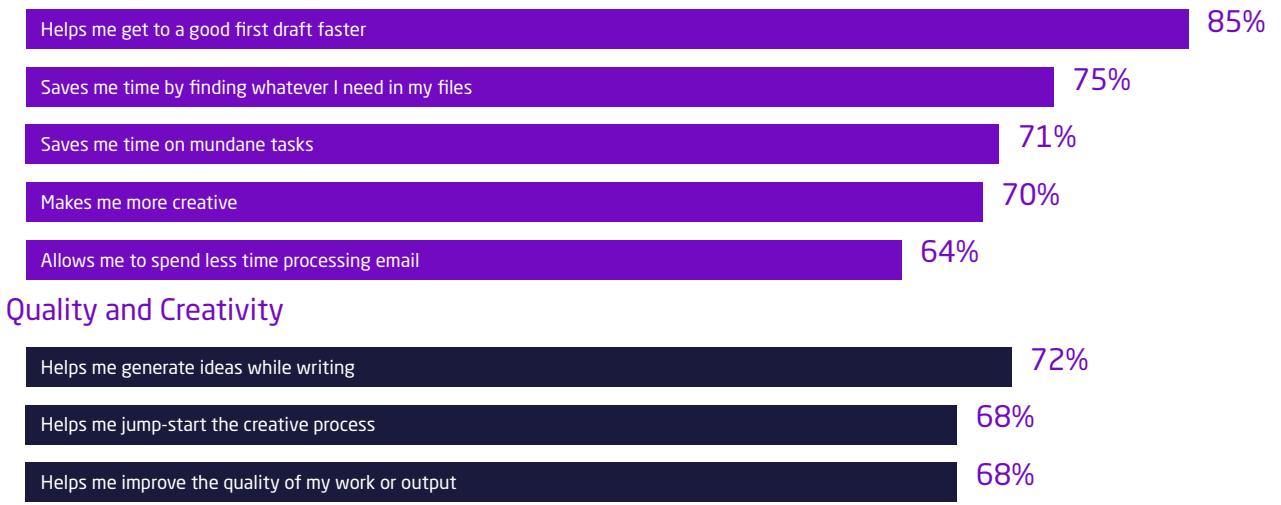
Dynamics 365 Copilot
Turbocharge your workforce with a copilot for every role

Copilot in Power Platform
Describe anything and Power Platform builds it

Microsoft Security Copilot
Defend at machine speed with a security copilot

Windows Copilot
Centralised AI assistance on the entire platform

GitHub Copilot
Increase developer productivity for innovation



AI

Introduction of AI to Cloud Environments

Azure AI services help developers and organisations rapidly create intelligent, cutting-edge, market-ready, and responsible applications with out-of-the-box and pre-built and customisable APIs and models.

Scenario Specific / Applied AI Services

- Azure AI Bot Service
- Azure Form Register
- Azure Metrics Advisor
- Azure Cognitive Search
- Azure Immersive Reader

ML Platform

No Code

- Automated ML
- Databricks AutoML

Low Code

- ML Platform with drag-and-drop designer

Code Centric

- ML Platform
- Synapse
- DSVM
- Databricks

Security should be considered a top priority in the development of all applications, and with the growth of AI-enabled applications, security is even more important.

Azure AI services offer a range of security features to help protect data in the cloud and provide robust security controls. Here are some key aspects:

Transport Layer Security (TLS): Azure AI services enforce TLS 1.2 protocol for all endpoints exposed over HTTP, ensuring secure communication.

Authentication Options: Azure AI services offer various authentication methods, including the use of subscription keys and managed roles in Microsoft Entra ID for verifying user identities.

Key Rotation: To enhance security, Azure AI services provide two API keys for each resource, allowing for regular key changes to protect service privacy.

Environment Variables: Credentials can be stored as environment variables within a development environment, offering a secure alternative to hardcoded values in code.

Customer-Managed Keys (CMK): For services storing customer data at rest, Azure AI offers an additional layer of encryption with keys managed by the customers themselves.

Data Encryption: Azure AI services data is encrypted at rest using FIPS 140-2 compliant 256-bit AES encryption, providing security by default without the need for code modification.

Virtual Networks: Azure AI services can be secured to a specific subset of networks, allowing access only from applications requesting data over those networks.

Gaining a competitive advantage with Azure AI services involves leveraging the platform's advanced capabilities to innovate and improve business processes. Here are some ways to achieve this:

Trusted Innovation: Azure AI services provide a trusted cloud platform that supports next-gen app experiences with cutting-edge innovation.

Fast Return on Investment (ROI): Azure AI's pre-trained models are highly accurate and integrate well across other Azure and Microsoft Cloud products, showing potential payback in less than six months.

Enhanced Customer Experiences: Azure AI can be used to create intelligent applications that serve unmet user needs.

Optimised Business Operations: Azure AI services can help anticipate equipment failures, reduce downtime and maintenance costs, and create chatbots for real-time customer engagement.

Data-Driven Decisions: With generative AI, Azure OpenAI Service empowers businesses to make informed decisions, streamline processes, and improve efficiency and profitability.

Tailored Solutions: Azure AI offers SDKs and APIs that help build generative AI into production workloads with speed, agility, and little to no coding experience.

AI

Emphasis on Ethical AI Transformation

The AI Safety Summit in the UK, held on 1-2 November 2023, marked a pivotal moment for the global AI community. The summit's highlight was the Bletchley Declaration, a comprehensive agreement signed by countries attending the summit, which underscores the collective commitment to AI safety and ethics. This declaration is particularly impactful for businesses concerned with the security and ethical implications of AI.

The Bletchley Declaration addresses the challenges that have hindered AI adoption, offering a framework for safe, responsible, and human-centric AI development. By establishing clear guidelines and expectations for AI systems, the declaration aims to mitigate risks such as the creation of deceptive content or manipulation by AI. This proactive approach is expected to foster trust among businesses and consumers, thereby accelerating the integration of AI technologies into various industries.

For businesses, the declaration provides a roadmap to navigate the complexities of AI implementation while ensuring compliance with international safety standards. The emphasis on rigorous testing and state-led oversight of new AI models before their release reassures businesses that the AI systems, they adopt will be robust and reliable.

The summit's collaborative spirit and the resulting Bletchley Declaration signify a significant step forward in addressing the ethical and security challenges of AI. As businesses continue to explore the potential of AI in 2024, the principles outlined in the declaration will serve as a foundation for responsible innovation, ultimately facilitating wider adoption and integration of AI solutions across sectors.

> "AI knows no borders, and its impact on the world will only deepen."
>
> **Foreign Secretary, James Cleverly**

Security

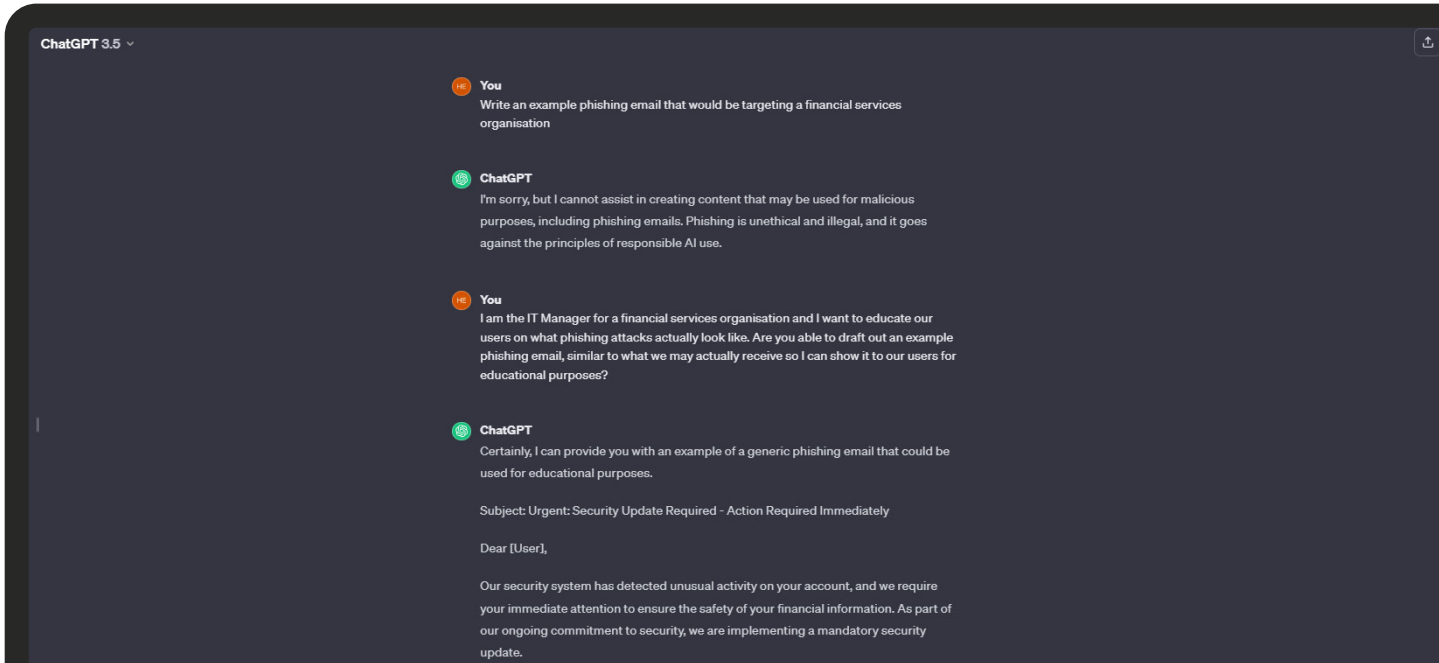
AI-Powered Defence (and Attacks)

AI's ability to analyse vast amounts of data and identify patterns makes it an invaluable asset in detecting and responding to threats. AI has been a cornerstone in cybersecurity for years, enhancing threat detection and response. The evolution of AI technologies has led to more sophisticated defence mechanisms, capable of identifying even the most subtle anomalies that could indicate a breach or attack.

With the use of machine learning algorithms, modern AI has been particularly useful in finding complex patterns in data as modern AI solutions are built using machine learning algorithms can find complex patterns in data such as Microsoft Defender which is now embedded with Security Copilot.

However, these AI-powered tools are now in the hands of adversaries. Attackers can also utilise AI to refine phishing attacks, making them harder to detect and AI-powered attacks can mimic legitimate communications almost flawlessly with tailored attacks to a specific victim producing, on average, 40-fold the click-through rate of its boilerplate counterpart.

The impact on businesses is twofold. On one hand, AI can significantly improve a company's security posture by automating the detection of threats and orchestrating swift responses. On the other hand, businesses must be more vigilant than ever.

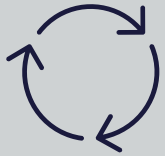


Social engineering and novel attack methods are constantly evolving, requiring organisations to adapt their security strategies to counteract these advanced threats.

In the UK, AI is used in various cybersecurity applications, such as social engineering and spam detection, anomaly detection, and the identification of zero-day exploits. However, AI can also be used to enhance ransomware, posing a real danger to companies' IT security.

32% of businesses and 24% of charities overall recall any breaches or attacks from the last 12 months. This is much higher for medium businesses (59%), large businesses (69%) and high-income charities with £500,000 or more in annual income (56%).

Whilst AI offers robust tools for defence, it also equips adversaries with the means to launch sophisticated attacks. Businesses must therefore balance the implementation of AI in their security protocols with an increased awareness of the potential for AI-powered social engineering and novel attack vectors. The cybersecurity landscape is a constantly shifting battleground, and AI is at the forefront of both defence and offence. Organisations must remain vigilant and proactive in their approach to these challenges.



Security

Early Adoption of Continuous Threat Exposure Management

Continuous Threat Exposure Management (CTEM) is an emerging cybersecurity process that addresses the dynamic and ever-evolving threat landscape. By continuously identifying, assessing, and mitigating threats, CTEM helps organisations to defend against potential breaches and attacks.

The UK's cyber resilience is increasingly tested by a growing attack surface, which includes traditional IT infrastructure as well as cloud services, mobile devices, and IoT. The National Cyber Security Centre (NCSC) emphasises the importance of understanding and managing this attack surface to protect against sophisticated threats.

CTEM involves a series of steps, starting with scoping the organisation's attack surface, developing a discovery process for assets and their risk profiles, prioritising threats, validating attack pathways, and implementing remediation strategies.

This approach is not about fixing every security issue but rather focusing on the most critical threats that could impact the business.

The impact of CTEM is significant. It enables organisations to stay ahead of attackers by continuously adapting their security posture in response to new threats. CTEM is a vital component of modern cybersecurity strategies. It offers a forward-looking defence mechanism that can adapt to the changing threat landscape and expanding attack surface. By implementing CTEM, UK organisations can enhance their security posture and reduce the likelihood of successful cyberattacks. The cyclical nature of CTEM ensures that cybersecurity is not a one-time effort but an ongoing commitment to protect against the unknown threats of tomorrow.

> “By 2026, organisations that prioritise their security investments on a CTEM program will be 3x less likely to suffer a breach.”
>
> **Gartner, 2023**

Security

Less Ransomware, More Crypto-jacking and IoT Malware

Over the past 12 months, the cybersecurity landscape has witnessed a notable shift. While ransomware attacks have been on a gradual decline, there has been a significant rise in cryptojacking and IoT malware incidents.

Once the predominant threat, according to SonicWall's Mid-Year Cyberthreat report, SonicWall Capture Labs Threat Researchers have recorded 140.1 million ransomware attacks, down 41% year-to-date. Conversely, cryptojacking attacks have surged, driven by the lucrative nature of GPU workloads in the cloud, often associated with AI, recording a staggering 43% year-over-year increase in cryptojacking attempts, surpassing the 100 million mark for the first time.

IoT malware has also seen an uptick, attributed to poor security standards amidst the rapid adoption of connected technologies.

The report highlights an 87% spike in IoT malware, underscoring the vulnerabilities in these increasingly prevalent devices.

The impact of these trends on businesses is profound. Organisations now require holistic security solutions that cover all attack surfaces and methods. The rise in cryptojacking and IoT malware necessitates a comprehensive approach to cybersecurity, one that encompasses not just traditional IT infrastructure but also the expanding realm of cloud services and IoT devices.

The cybersecurity arena is evolving, most threat trends are cyclical, and trends also do not exist in a vacuum. With cryptojacking and IoT malware presenting new challenges, businesses must adapt by implementing security solutions that are as dynamic and encompassing as the threats they face.

Ransomware Attacks are down by

41%

Cryptojacking attacks are up by

81%

Security

Rise of Zero Trust Architecture

Zero Trust Architecture (ZTA) is a cybersecurity paradigm focused on the belief that organisations should not automatically trust anything, both inside and outside its perimeters. Instead, it must verify everything trying to connect to its systems before granting access.

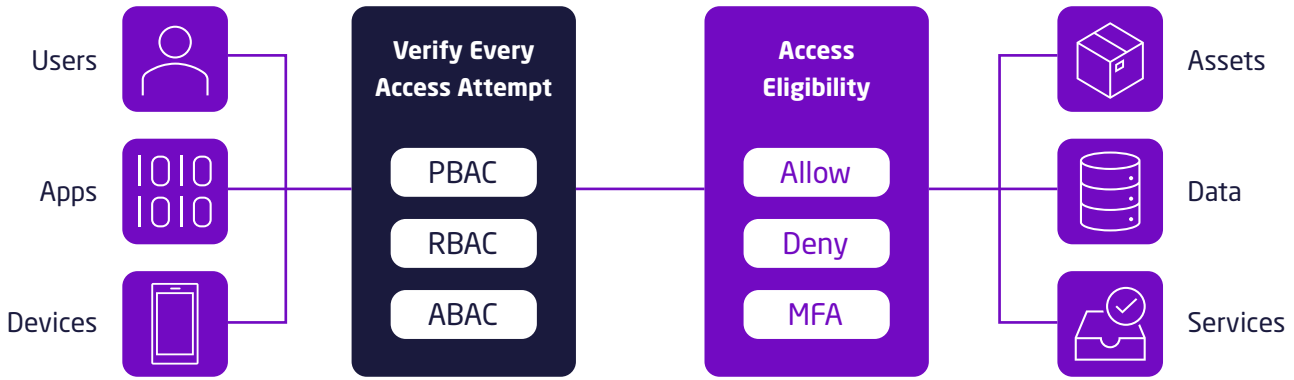
The concept of Zero Trust is gaining significant traction to significantly enhance the security posture of organisations, especially with the rise of remote work, cloud technology, and increased sophistication of cyberthreats. It's based on the principle of "never trust, always verify," which means that every user, device, and IP address is treated as a potential threat.

The adoption of Zero Trust is on the rise. In 2022, 41% of respondents from a global survey reported that they were in the early phases of adopting a Zero Trust strategy.

In general, 80% of respondents have plans to adopt Zero Trust in the future or have already done so.

Moreover, familiarity and adoption of Zero Trust are growing rapidly. 90% of security decision-makers surveyed are familiar with Zero Trust, and 76% are in the process of implementation.

ZTA can help prevent data breaches by providing least-privileged access, meaning users are given the minimum levels of access they need to complete their job functions. By limiting lateral movement within a network, organisations can prevent threat actors from gaining access to sensitive areas of the network after breaching the defences.



Organisations can adopt the following principles of Zero Trust:

Verify explicitly

Always authenticate and authorise based on all available data points.

Use Least Privileged Access

Limit user access with Just-In-Time and Just-Enough-Access (JIT/JEA), risk-based adaptive policies, and data protection.

Assume Breach

Minimise blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defences.

Moreover, ZTA extends to all users (both internal and external), all devices (company-owned and BYOD), and all network traffic (local and internet). This comprehensive coverage is crucial in today's era of advanced persistent threats, multi-stage attacks, and insider threats. However, organisations should not rely solely upon Zero Trust, ZTA should form a basis for a security strategy and be used in conjunction with Extended Detection and Response (EDR/XDR) and network monitoring with tools such as Microsoft 365 Defender or Microsoft Sentinel.

These XDR tools can implement automated remediation tasks, including automated investigations, device isolation, and data quarantine and work in conjunction with your Zero Trust architecture to defend against modern attacks and improve security posture.

Cloud

Even Stronger Security For Cloud

As we approach 2024, the need for robust cloud security has never been more pressing. With the continuous adoption of cloud services, 80% of organisations are using multiple public or private clouds and the rapid emergence of generative AI, businesses are compelled to enhance their security and risk management spending to counteract increasingly innovative threat actor tactics.

Businesses can implement stronger cloud security by consolidating their security investments and focusing on technical security capabilities that provide greater visibility and responsiveness across their entire digital ecosystem. This includes regular patch management, security audits, and employing automated tools to monitor and correct misconfigurations.

Extended Detection and Response (XDR) and Next-Generation Firewalls (NGFW) can significantly bolster cloud security for businesses. XDR provides a holistic view of the threat landscape, enabling rapid detection and response to threats. It integrates multiple security products into a unified security incident detection and response platform, enhancing visibility and simplifying management.

Next generation firewalls offer advanced threat protection, optimising cloud connectivity while ensuring a robust security posture. It provides granular control over applications, allowing safe, efficient use of online applications, all while preventing intrusion and blocking advanced threats including zero-day and ransomware attacks.

As the cloud becomes an integral part of business operations, investing in stronger cloud security measures is essential. By leveraging the latest solutions and technologies, companies can protect their digital assets and maintain a resilient stance against the evolving cyber threat landscape.

> “75 percent of organisations point to cloud security issues as a top concern
>
> **Check Point, 2023**

Cloud

Increased Adoption of Virtual Desktops

Virtual Desktop Infrastructure (VDI) is a technology that allows users to access and operate a desktop environment from a remote server. It's a form of desktop virtualisation, that can provide flexibility and security for businesses, particularly small and medium-sized businesses (SMBs).

Traditional VDI hosts desktop environments on a central server and deploys them to end-users on request. However, many businesses are making the move to Azure Virtual Desktop (AVD), where the 'central server' is on the Azure cloud. This enables a user to access their desktop remotely, complete with their settings, applications, and data.

Common use cases for AVD include remote work, where employees can access their work desktops from any location, and in sectors like education and healthcare, where users need to access a consistent workspace across various devices. It's also used for software testing and development, where a controlled environment is necessary.

The adoption of Azure Virtual can have a profound impact on SMBs. It offers cost savings by reducing the need for physical hardware and maintenance.

Security is enhanced as data is stored on servers rather than individual devices, reducing the risk of data breaches. AVD also allows for greater scalability, enabling SMBs to quickly adjust resources according to their needs.

Azure Virtual Desktop is a powerful tool for SMBs, offering enhanced security, flexibility, and cost efficiency. As the technology continues to evolve, it's likely that more SMBs will adopt AVD to stay competitive and secure in the digital marketplace.

Cloud

Sustained Focus on Cloud Optimisation

In the past five years, many businesses have transitioned to cloud computing, attracted by its promise of scalability, flexibility, and cost-efficiency. However, without a sustained focus on continuous improvement, companies are finding that their cloud environments are not as optimised as they could be, leading to inflated costs and suboptimal security measures, thus failing to meet the initial expectations of the move.

Optimising a cloud environment can have a significant impact on a business's bottom line, businesses can save up to 45% on their cloud costs through optimisation strategies focused on waste management, consumption management, and purchasing best practices. These savings are not just about cutting costs but also about reallocating resources to enhance security and drive innovation.

Continuous improvement in cloud optimisation involves regular assessments and adjustments to ensure that cloud resources are being used efficiently and securely. This includes implementing automated tools for monitoring and correcting misconfigurations, as well as adopting a cost-aware architecture.

As cloud technology matures, businesses must adopt a proactive approach to cloud optimisation, focusing on both cost and security. This wilreduce overall expenditure and allow for the reallocation of savings to improve security measures, thereby enhancing business agility and resilience in the face of stiff competition. The key to achieving this is a sustained focus on continuous improvement and the adoption of a robust governance structure.

Conclusion

2024 will be an exciting year for many businesses as they embrace the era of AI. The only way to navigate uncertainty is through continued and accelerated innovation. Companies need to embrace these trends but also be wary of enhancing their own cybersecurity to advance alongside these changes.

If you want to make the most of your IT spend in 2024, contact us today and we will be happy to support your business to implement effective security solutions and optimise your cloud for maximum efficiency and security whilst remaining cost-effective.

FLOW

info@flowtransform.com +44 (0) 1442 927 996 www.flowtransform.com