

GDPR
GENERAL
DATA PROTECTION
REGULATION



outboundTM

GROUP

2024 CYBER RESILIENCE SUMMIT

DATA
PROTECTION



INTRODUCING

KEITH BUCKNALL
CO-FOUNDER & CITO


outboundTM
GROUP

DATA
PROTECTION



AGENDA

🕒 13:00 - 13:10

Welcome & Introduction

By Keith Bucknall, Outbound

🕒 13:10 - 13:40

Threat Landscape

By Adam Pilton, CyberSmart

🕒 13:40 - 14:10

NIS 2: What You Need to Know About the EU Directive & how WatchGuard can assist you on your journey to Compliance

By Oli Venn, WatchGuard

🕒 14:10 - 14:40

Protecting an evolving SaaS Ecosystem

By Neil Rawlins, Keepit

🕒 14:40 - 15:00

Coffee Break

🕒 15:00 - 15:30

Modern Workplace

By Joshua Foye, Pax8

🕒 15:30 - 16:00

Structuring, Securing and Tagging your data for the use of Copilot

By Hennie Erasmus, AvePoint

🕒 16:00 - 16:30

Customer Success Story

By Jak Lusty, Royal Opera House

🕒 16:30 - 17:00

Q&A Panel

Hosted by Victoria Lomax, Outbound

🕒 17:00 - 17:10

Wrap Up

By Keith Bucknall, Outbound

🕒 17:30 ONWARDS

Drinks & Networking

OUR STRUCTURE



outbound[™] GROUP

Your Trusted Partner



outbound[™] HUB

- Hardware
- Software
- Reseller
- E-Commerce
- Procurement
- Licenses
- Print Solutions



Supply Chain



outbound[™] VIRTUAL

- Managed Service Desk
- Managed Penetration Testing
- Managed Vulnerability Scanning
- Managed Azure / AWS
- Infrastructure as a Service
- Cyber Resilience
- Virtual Advisor
- Virtual IT Department (CIO, IT Director, PMO CIO & CISO)
- Disaster Recovery
- Security Operations Centre



Service Delivery



outbound[™] SOLUTIONS

- Infrastructure Solutions
- System Design
- System Integrator
- System Implementation
- Consultancy Services
- Architecture
- Project Work
- Document Management
- Scanning/Print
- IT Development
- Mobile App








Design & Implementation

<https://outbound.group/about/>

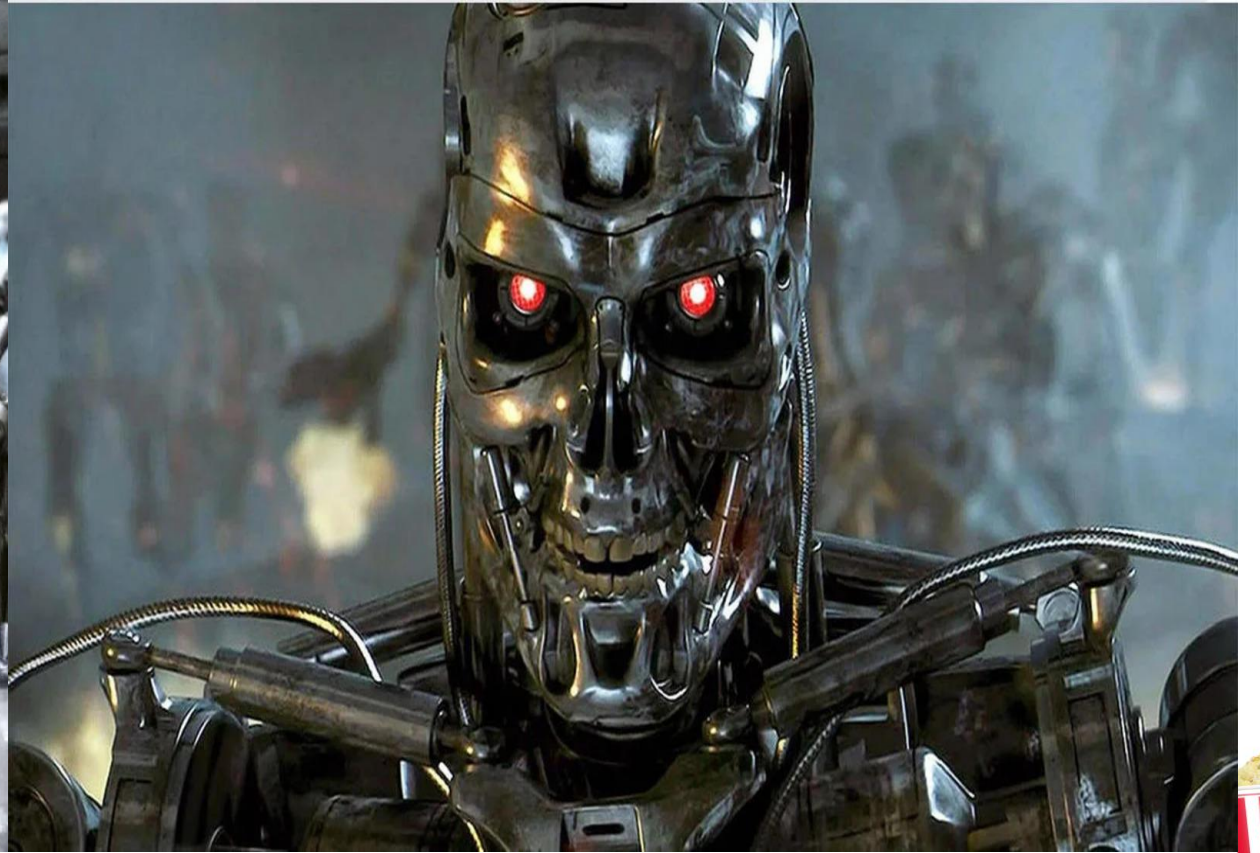
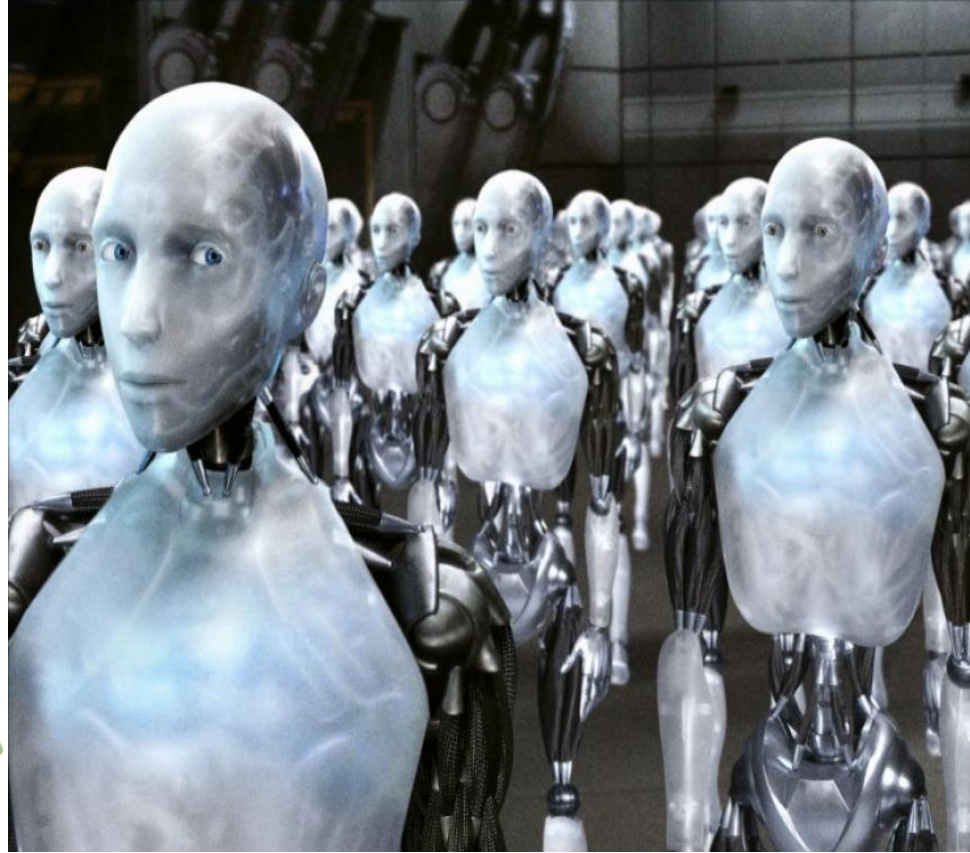
**NEW
PRODUCT**

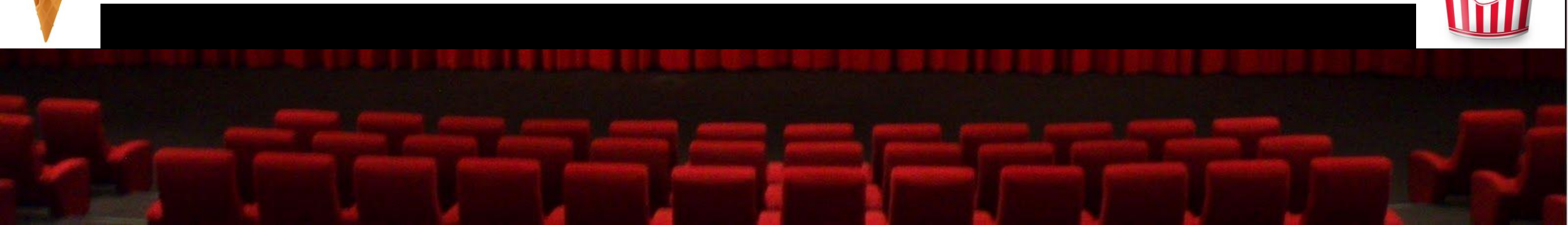
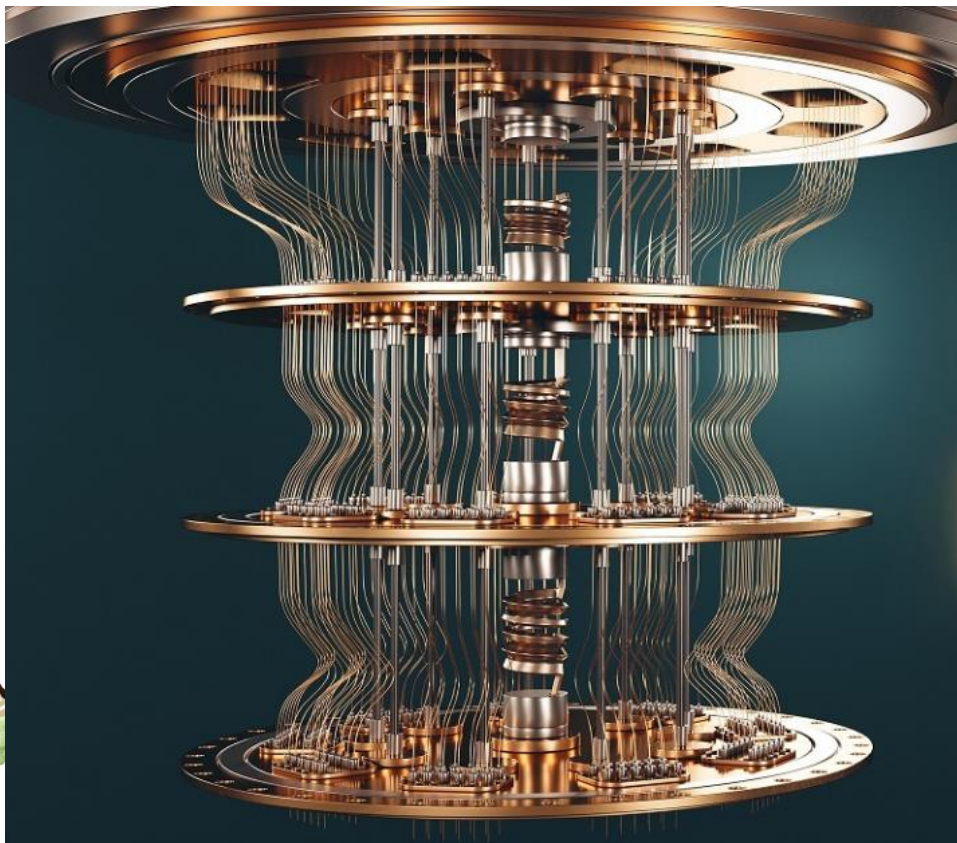
INTRODUCING



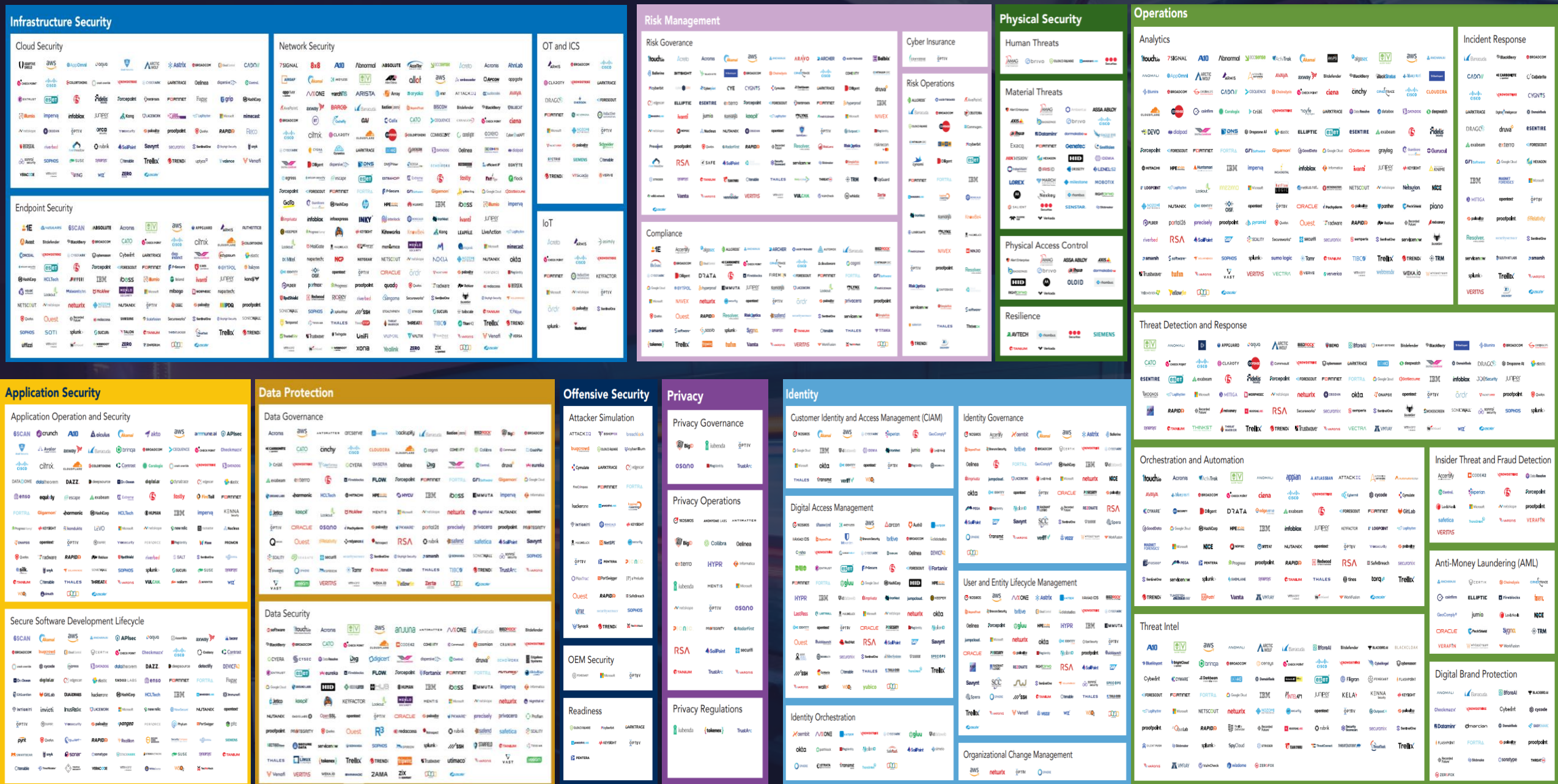
-  • Managed Patch Management
-  • Managed vulnerability scanning & remediation
-  • Low-cost automated Penetration Testing
-  • CREST approved penetration testing
-  • Pen-Testing-As-A-Service







The Current Cyber Security Software landscape



Did You Know ?

What type of cyber-attack was the most disruptive to businesses in 2023?

The most common Cyber-attack is Phishing

How many new pieces of malware software are detected every day?

560,000 pieces of malware software are detected every day

What was the biggest factor which decreased the average cost of a data breach?

Employee training reduced the average cost of data breaches by \$258,629, followed closely by AI and machine learning at \$258,538

Which company is the most exploited for Phishing attacks?

57% of phishing scam pose as Microsoft to steal data

What percentage of unpatched vulnerabilities are involved in data breaches?

Unpatched vulnerabilities were involved in 60% of data breaches

What percentage of small business go out of business after being affected by a cyber-attack?

60% of small businesses go out of business after being victims of a cyber-attack



INTRODUCING

ADAM PILTON
CYBERSMART

 **CyberSmart**

DATA
PROTECTION

 **outbound**TM
GROUP



Achieving Complete Cyber Confidence

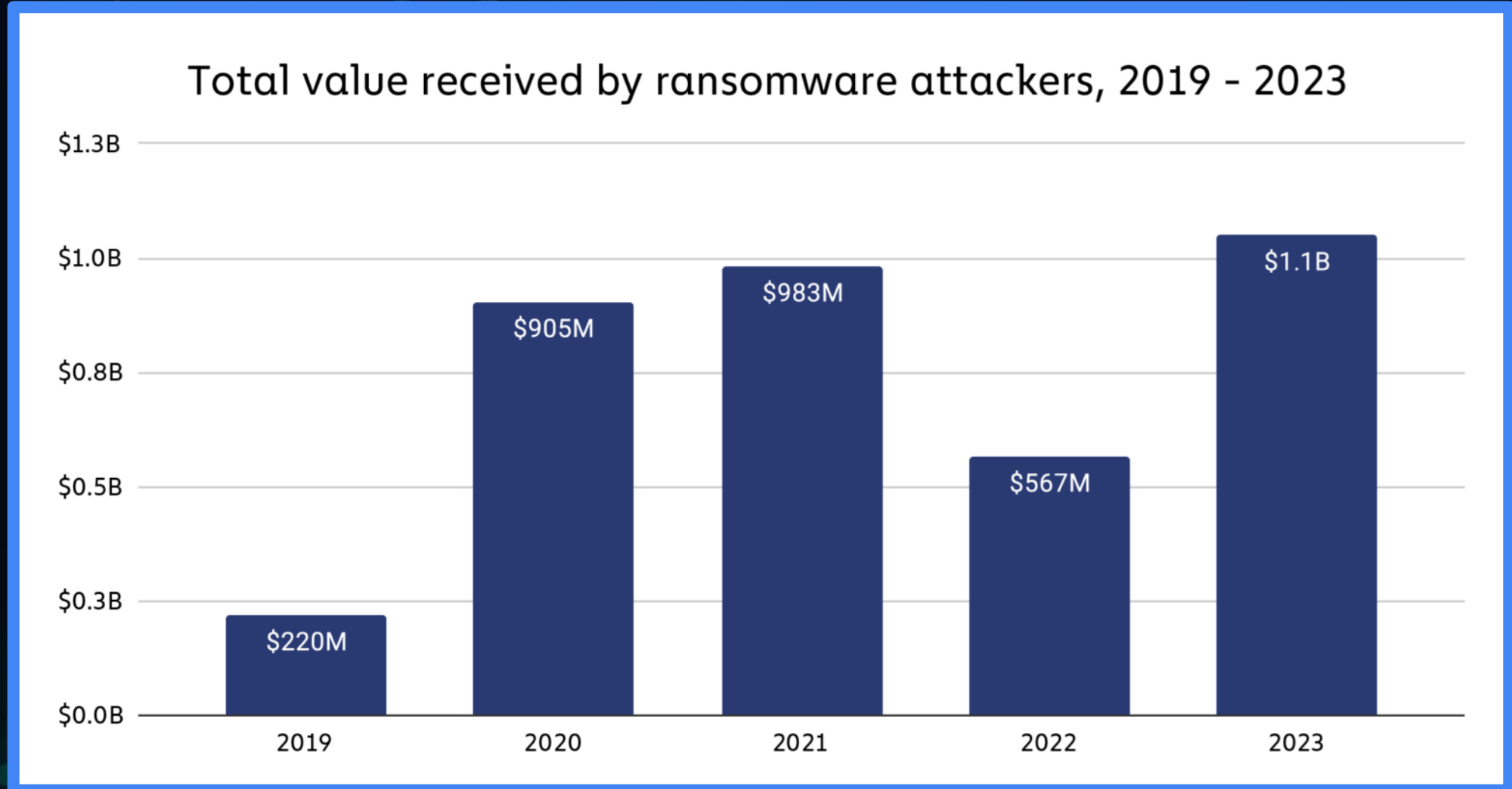
Agenda

Overview of Cyber Crime Today

Cyber Essentials

The Importance of Culture

Ransomware is a Successful Business



Ransomware - The Stats



66%

Of organisations were affected by Ransomware in 2023.



13%

Of small and medium businesses experienced a ransomware attack in 2023.



24%

of all breaches involved ransomware attacks.

Ransomware - The Stats

**22
days**

The average downtime a company experiences after a ransomware attack

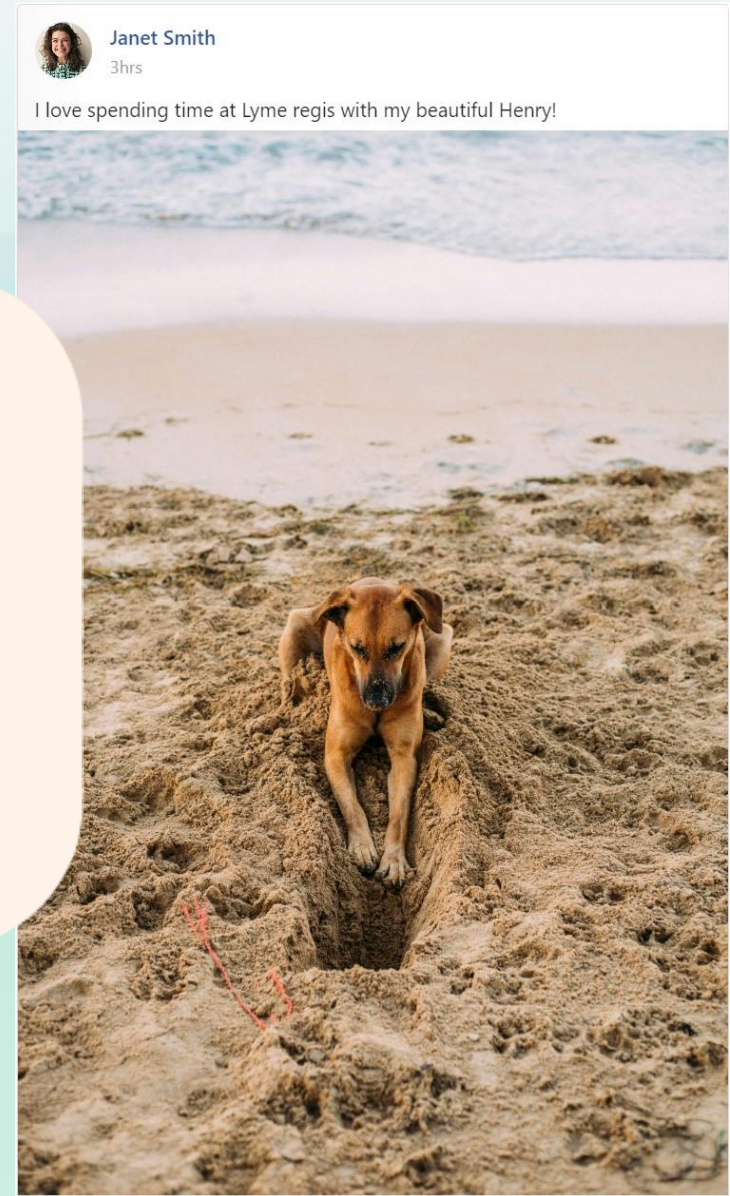
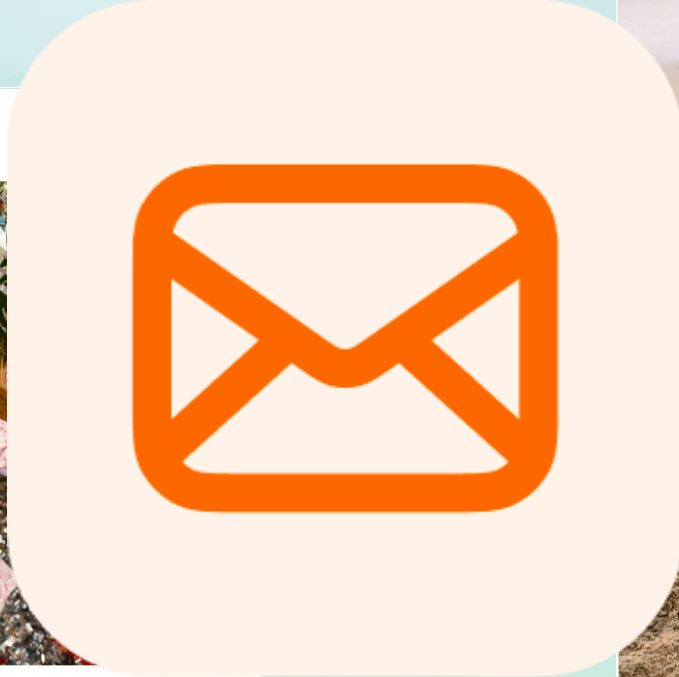
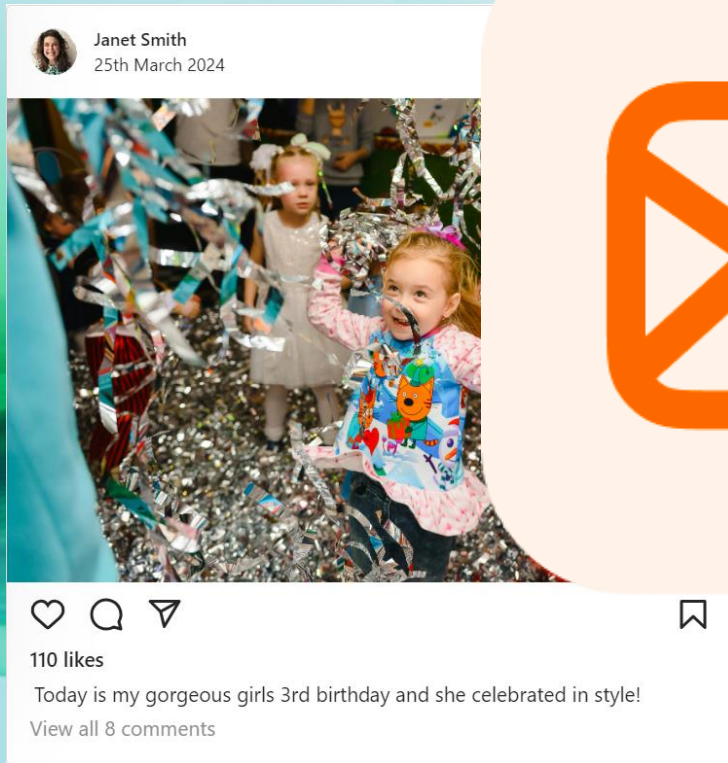
80%

Victims who paid a ransom experienced another attack soon after

46%

Of victims got access to their data but most of it was corrupted.

The Information We Give Away



But it's not just emails

NATIONWIDE: £724.76 SELFRIDGES
DECLINED. 14:26:11 GB LONDON. Call
us now on [020 3290 5665](tel:02032905665)

NATIONWIDE: £724.76 SELFRIDGES
DECLINED. 14:26:11 GB LONDON. Call
us now on [020 3290 5665](tel:02032905665)

Office Warm Reminder:

Due to the cancellation of heating subsidies this winter, the government decided to provide subsidies in the form of living expenses.

Application qualifications are now reopened, applications will be closed as of October 12, 2024, we will issue them before the 30th of this month.

You can apply through the link in the information, if you give up the application, please ignore it.

<https://bit.ly/3Y9R8Lw?LNB=9qoE3DwuoU>

Thank you for your support to the UK Government.

Incoming Legislation



NCSC ANNUAL REVIEW 2023

Increase in incidents reported to the NCSC

64%

increase from last year in the amount of exfiltration/ extortion of data

18.5%

“We have the information and tools at our disposal to defend ourselves. We just need to use them better.”

What is Cyber Essentials?



**CYBER
ESSENTIALS**

Government
backed
Scheme since
2014

A solid foundation
in Cyber Security

Designed to help
organisations to show
their commitment to
Cyber Security - while
keeping it simple

The minimum
businesses should be
doing to protect
themselves and
others

It is a
Certification
Process

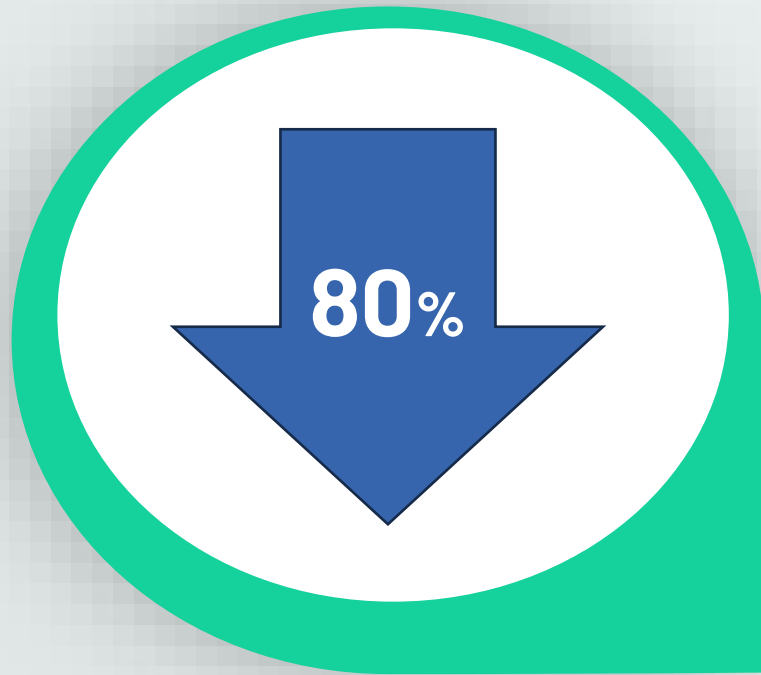


**CYBER
ESSENTIALS
PLUS**

Cyber Essentials Controls

- **Firewalls** - Boundary firewalls and Internet gateways allow you to control who can access your system and where your users can go.
- **Secure Configuration** - Configure computers and network devices to reduce vulnerabilities and only provide necessary services.
- **User Access Control** - It is important to keep access to your data and services to a minimum. This should prevent a criminal hacker from being presented with open access to your information.
- **Malware Protection** - It is vital that you protect your council from malicious software, which will seek to access files on your system.
- **Patch Management** - Criminal hackers exploit known vulnerabilities in operating systems and third-party applications if they are not properly patched or updated.

It Works!



Wealth management firm, St. James's Place mandates Cyber Essentials Plus across network of Partner organisations

May 23, 2024 | Cyber Essentials



St
James's
Place



How it works



Changes to Cyber Essentials



Terminology



Scope Verification



Passwordless Technology

Legal Loophole: The Consequences of Ignoring Cyber Security

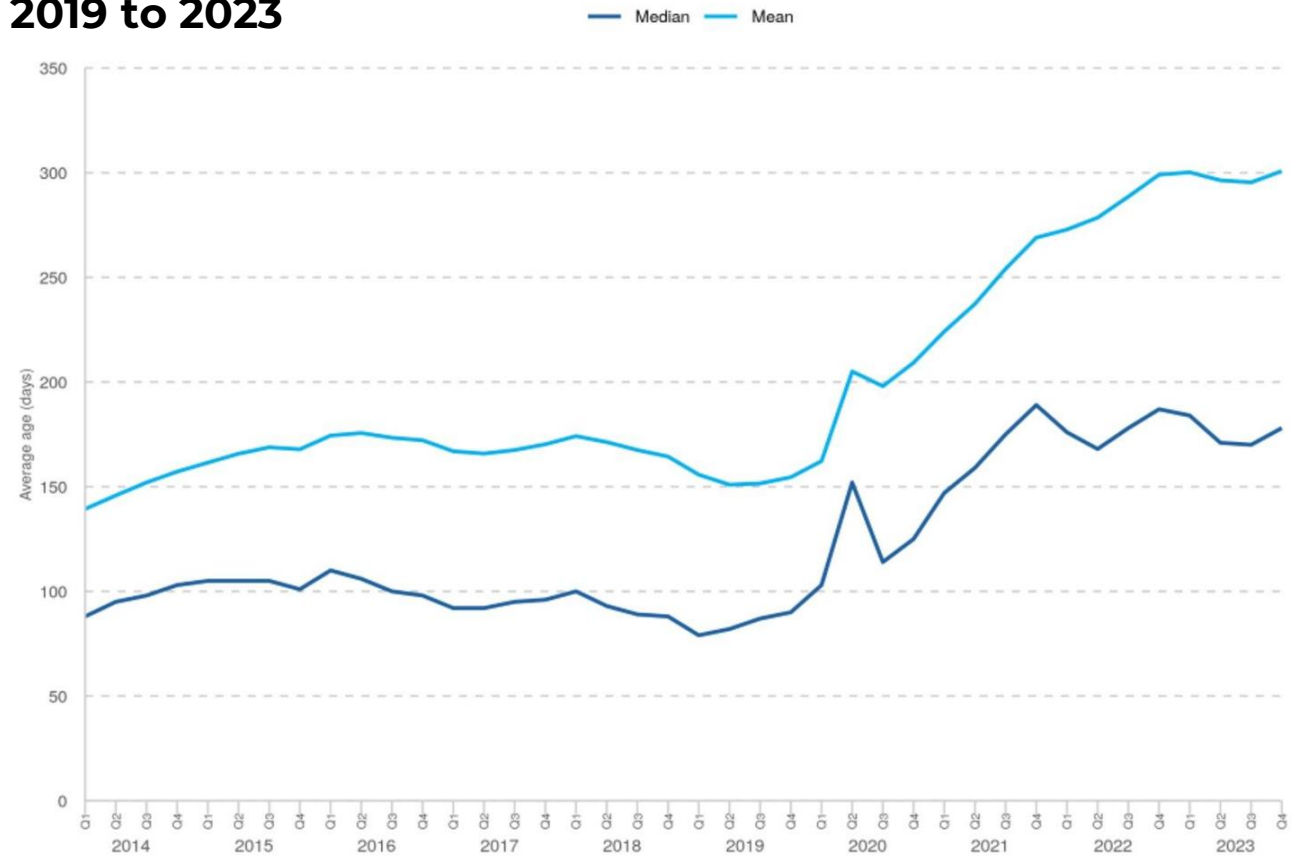


Legal Loophole: The Consequences of Ignoring Cyber Security



Criminal Investigations

2019 to 2023



Achieving Complete Cyber Confidence



Prevention is Crucial



Comprehensive
Strategy is
Essential



Culture & Awareness Matter



Thank you

GDPR
GENERAL
INTRODUCING

OLI VENN
WATCHGUARD

atchGuard®

DATA
PROTECTION


outbound™
GROUP



***NIS 2: What You Need to Know About the EU Directive
&
How WatchGuard can assist you on your journey to
Compliance***



Oli Venn
Manager, Sales Engineering
Northern Europe

Why break in, when you can simply sign in?



Pop Quiz Time

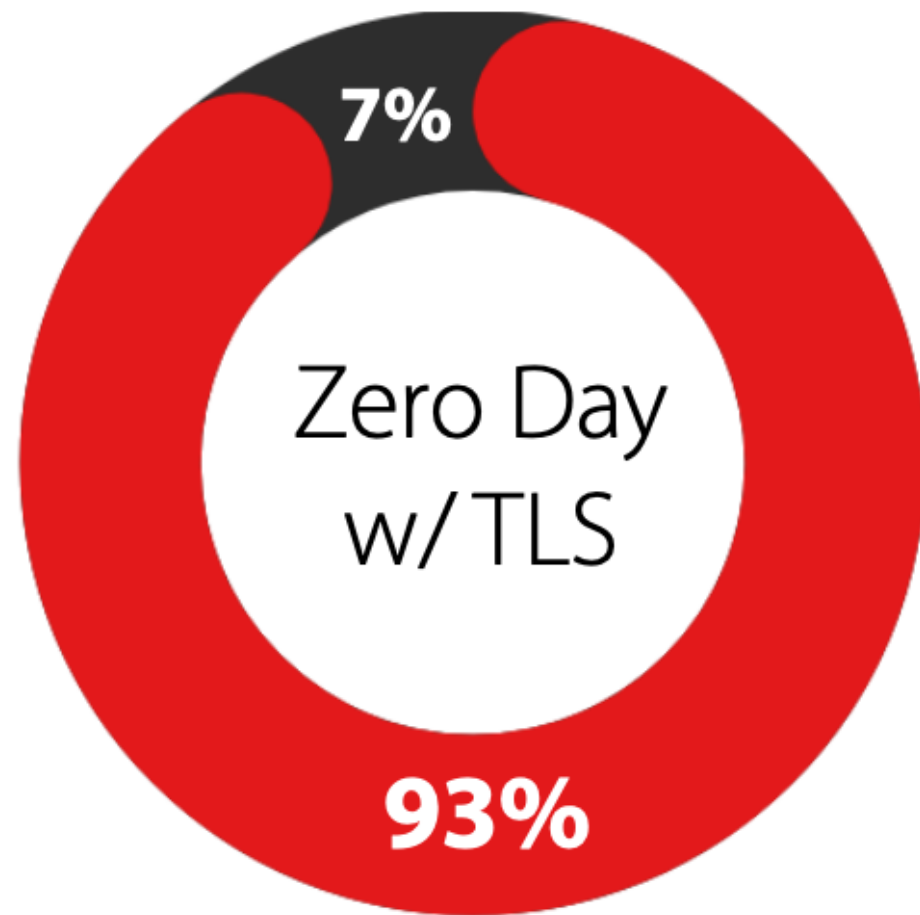
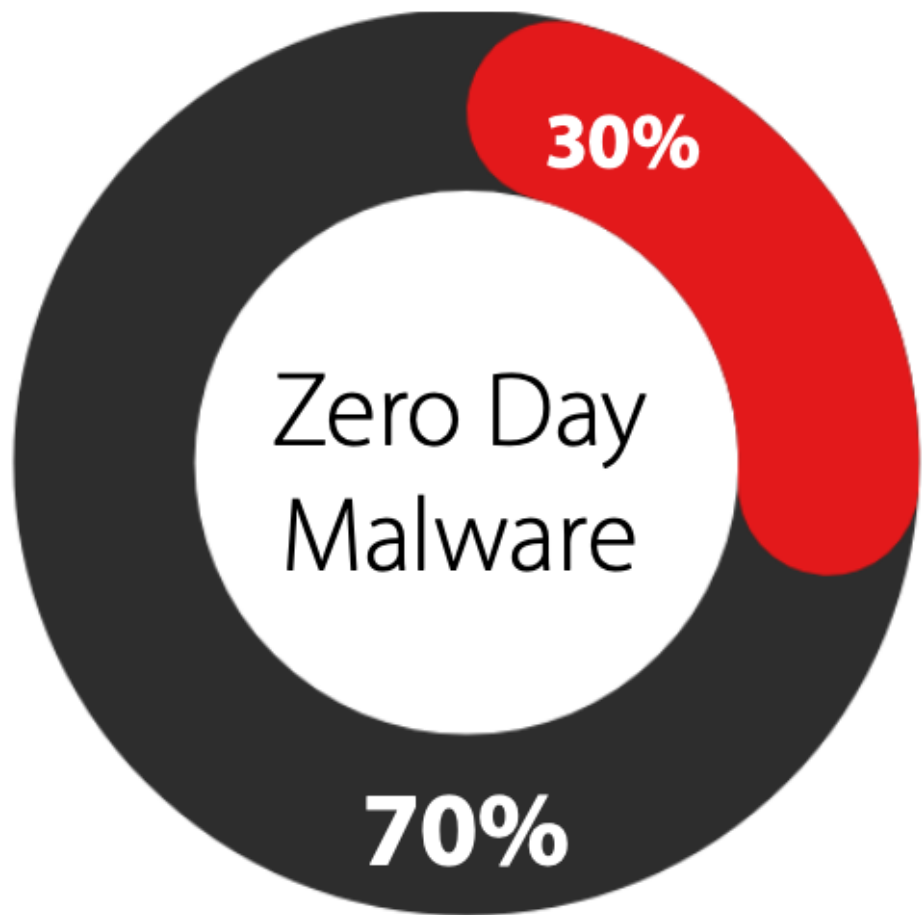
**What Percentage of Malware
Evades Basic Detection Methods?**

34%

52%

70%

93%



Defending Against Evasive Threats

It's not a matter of if, but when.
There is no silver bullet defense.



General Tips – Layered Defences

- Advanced threats leverage multiple vectors of attack
- No **single** defense will protect you completely
- Combination of network and endpoint security can help
 - Multi-Factor Authentication (MFA)
 - Advanced (proactive, non-signature) antimalware
 - Phishing Protection
 - Endpoint detection and response (EDR)
 - Procedure-driven patch management
- Monitor, Monitor & Monitor
- Compliance!



NIS 2 Overview

NIS 2 Overview












NIS	NIS 2
30 types of entities	67 types of entities
Operators of Essential Services & Digital Service Providers	Includes some SMEs and Supply Chain
Security requirements and incident notification	Regular audits, incident reporting requirements, risk management across multiple areas
Penalties set by each EU member state	Fines, suspension of certifications, management responsibility
Creation of a Cooperation Group & Computer Security Incident Response Teams (CSIRT) to facilitate exchange of information	Creation of Cyber Crisis Liaison Organisation Network (EU-CyCLONe)

- ✓ Directive on measures for a higher standard level of cybersecurity across the European Union (EU)
- ✓ Replaces the previous NIS Directive
- ✓ Introduces stricter requirements for organisations operating in the EU
- ✓ Aims to improve cybersecurity across entities in critical sectors








Who Needs to Comply with NIS 2?

- A broader range of businesses and sectors
- Two categories:
 - Essential entities
 - Important entities

Essential business sectors

Essential business sectors						
Energy  Electricity Gas Oil Hydrogen District heating and cooling		Transport  Air Rail Water Road		Health  Healthcare providers Pharmaceutical industry		Space  Space
Drinking water  Drinking water	Waste water  Waste water	Public administration  Public administration	Digital infrastructure  Digital infrastructure	Banking  Banking	Financial market infrastructures  Financial market infrastructures	ICT service management (B-to-B)  ICT service management (B-to-B)

Important business sectors

Important business sectors							
Postal and courier services  Postal and courier services	Waste management  Waste management	Digital providers  Online marketplaces Online search engines Social networking services platforms			Chemicals  Chemicals	Food  Food	Research  Research
Manufacturing  Manufacture of medical devices and <i>in vitro</i> diagnostic medical devices Manufacture of computer, electronic and optical products Manufacture of electrical equipment Manufacture of machinery and equipment n.e.c. Manufacture of motor vehicles, trailers and semi-trailers Manufacture of other transport equipment							

What are the Key Requirements of NIS 2?

- **Risk Management:** Implement risk assessments and establish risk management strategies to identify, analyse, and mitigate cybersecurity risks.
- **Incident Reporting:** Report cyber incidents to relevant authorities within a set timeframe.
- **Supply Chain Security:** Address security risks throughout the supply chain, including vendors and third-party service providers.
- **Cybersecurity Measures:** Implement baseline security measures to address specific cyber threats, such as access controls, multi-factor authentication, and vulnerability management.
- **Governance and Accountability:** Management bodies are held accountable for overseeing and approving cybersecurity measures.



Reporting Obligations

Incident Occurrence

< 24 hours
Initial notification to
competent authorities or
the CSIRT

< 72 hours
Incident notification
including an assessment
of severity and impact

< 1 month
Final detailed report
including the type of
threat and the mitigation

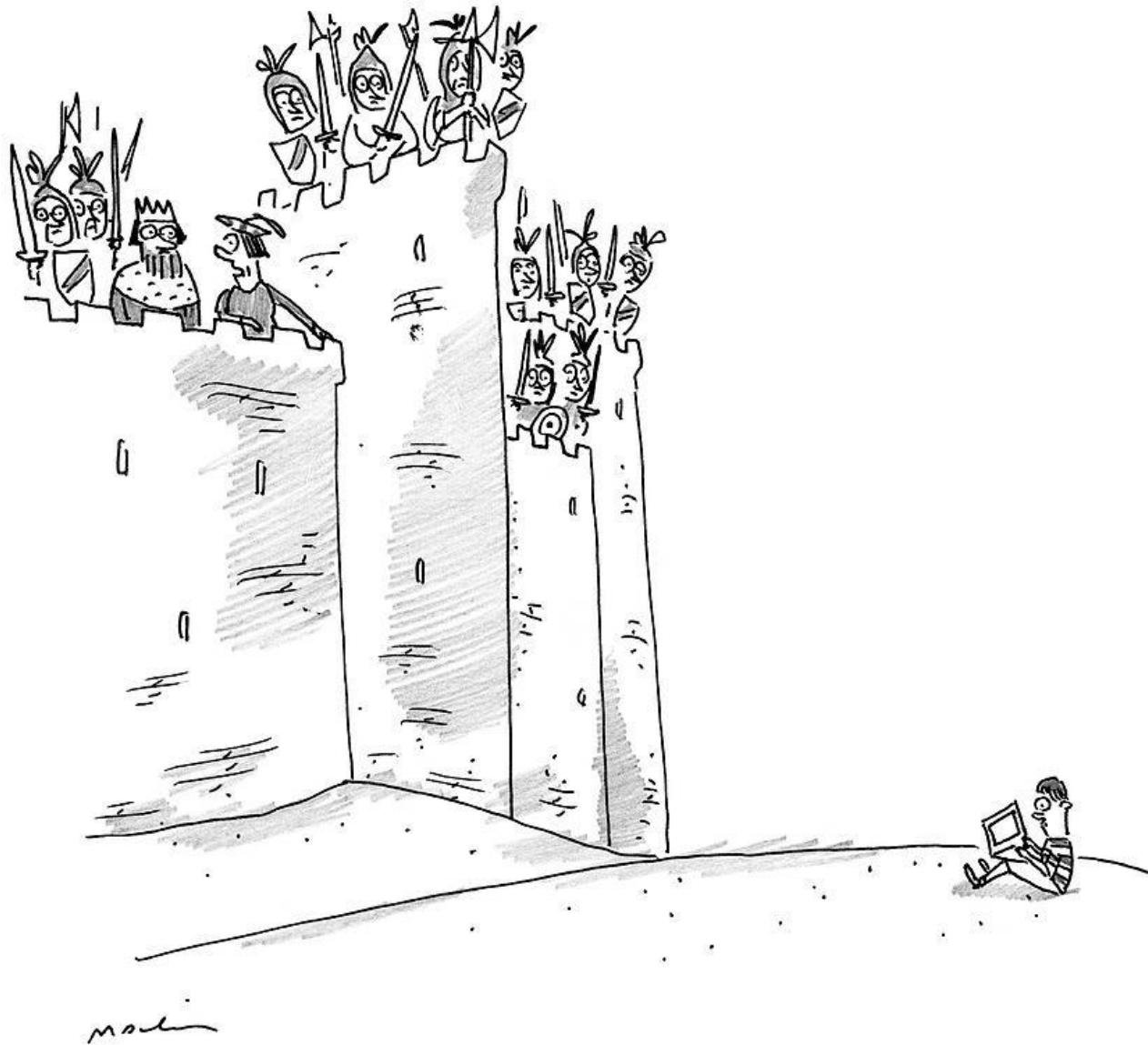
A CSIRT or other competent authority can request an intermediate report at any time.

The Deadline for Compliance is Approaching

- 16 Jan 2023
 - NIS 2 approved by EU
- 17 Oct 2024
 - Deadline for member states to transpose the directive into national law
- 17 Apr 2025
 - Deadline for member states to establish a list of Essential and Important entities

Organisations operating in the EU must be compliant to avoid penalties





“Bad news, Your Majesty—it’s a cyberattack.”

Global. Experienced. Trusted.



WatchGuard appliances conduct **>1 billion security scans** every hour



A WatchGuard Firebox is deployed **every 4 minutes** around the world



WatchGuard has saved customers **>16 years of labour** with RapidDeploy



WatchGuard protected our customers **22+ BILLION times** last year

ABOUT



Founded in **1996**



Operations in **7** countries;
direct presence in **21**



1,200 Employees



250K+ Customers



100+ Distributors
16,000+ Active Partners



Enterprise-Grade Security for Today's Business



A large number of customers are recognising WatchGuard's scalable architecture and best-in-class manageability

- **SMBs and SMEs**
- **Distributed Enterprises**
- **Retail**
- **Hospitality**
- **Government**
- **Education**

WatchGuard, The Big Picture

Accelerating Delivery of Key Innovative Products
Unwavering Commitment To Our Partners
Unique Value Culminates In Our Unified Security Platform

XDR

2017

First Network &
Endpoint Threat
Correlation

Identity Security

2018

Cloud Based
Identity Security

Endpoint Security

2021

Only Full Zero-
Trust Posture for
Endpoints

MDR

2023

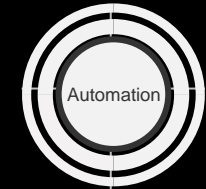
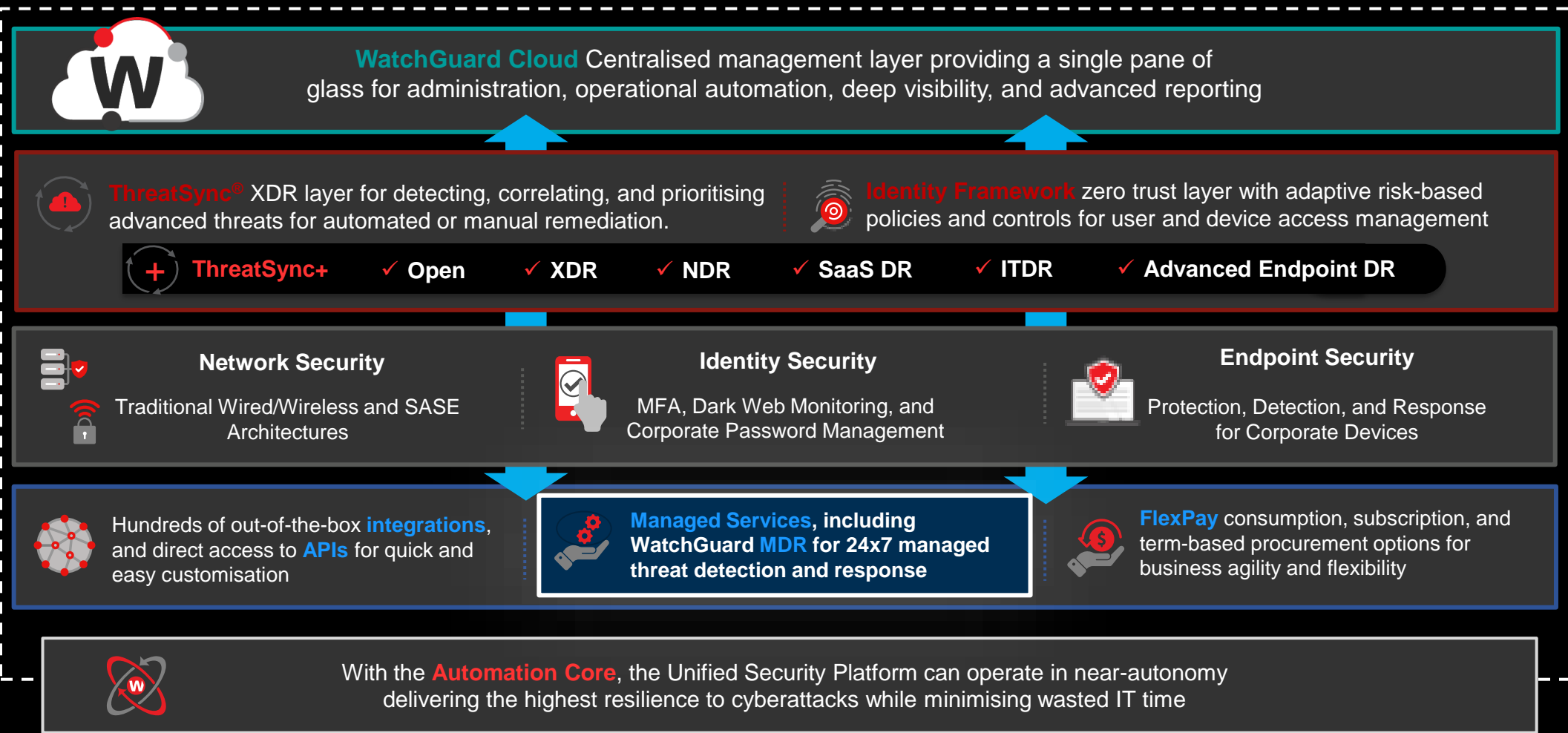
MDR and SOC
resources

NDR

2024

First Cloud-Native
NDR Service for
Mid-Market

WatchGuard's Unified Security Platform





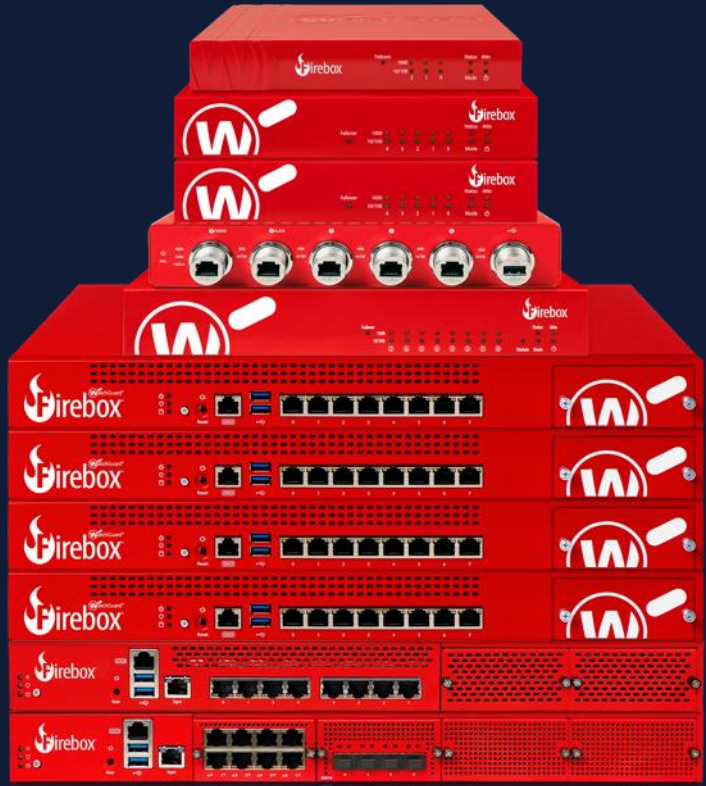
How Can WatchGuard Help with NIS2?

WatchGuard Network Security



BASIC SECURITY SERVICES

- Intrusion Prevention Service (IPS)
- Reputation Enabled Defense (RED)
- spamBlocker
- Gateway AntiVirus (GAV)
- WebBlocker
- Application Control
- Network Discovery
- Access Portal



ADVANCED SECURITY SERVICES

- APT Blocker
- ThreatSync (XDR)
- IntelligentAV
- Dimension Command
- DNSWatch
- EDR Core



Matching Cyber Security Solutions to NIS2 Directive Requirements

Firewall	
Risk analysis and information system security policies	
Incident handling	✓
Business continuity, including recovery and management	
Supply chain security	
Security maintenance and vulnerability handling	✓
Assessing cybersecurity risk management measures	
Basic cyber hygiene practices	
Using cryptography and encryption	✓
Access control and asset management	✓
Multi-factor authentication	✓

- **Incident Handling**

- Continually monitor for threats that can be caused by malicious individuals or just employees who mistakenly click on a malicious link. The security services can detect threats, implement automatic remediation, and send the incident data to ThreatSync to correlate the incident across the WatchGuard platform.

- **Security Maintenance and Vulnerability Handling**

- Offering multi-layered network protection, ensuring they offer Network Access Enforcement (NAE), and intrusion detection/prevention (IDS/IPS) with traffic segmentation capabilities

- **Cryptography & Encryption**

- Along with the security policies, the firewalls can offer the latest FIPS-level encryption methods for traffic that needs to be encrypted in transit

- **Access control**

- Flexibility to offer different access control based on role

- **MFA**

- The use of MFA for controlling access is critical for a Firewall



WatchGuard Endpoint Security

Confidently Protect Devices



Next-Generation Antivirus (EPP)

WatchGuard EPP | Endpoint Protection Platform (EPP) Capabilities

Add-on modules: WatchGuard Patch Management | WatchGuard Full Encryption



Endpoint Detection and Response (EDR)

WatchGuard EDR | EDR Capabilities | Zero-Trust Application & Threat Hunting Services

Add-on modules: WatchGuard Patch Management | WatchGuard Full Encryption | WatchGuard Advanced Reporting Tool | WatchGuard Data Control*



Endpoint Protection Detection and Response (EPDR)

WatchGuard EPDR = EPP + EDR Capabilities | Zero-Trust Application & Threat Hunting Services

Add-on modules: WatchGuard Patch Management | WatchGuard Full Encryption | WatchGuard Advanced Reporting Tool | WatchGuard Data Control*



WatchGuard Cloud

Endpoint Security Management | Visibility | Track Licensing

- ✔ Workstation, laptop, servers and virtual instances
- ✔ Windows (Intel & ARM), Linux, macOS (Intel & ARM), Android & iOS
- ✔ Inside/outside network, branch offices and remote workers

Matching Cyber Security Solutions to NIS2 Directive Requirements

	Endpoint Security
Risk analysis and information system security policies	✓
Incident handling	✓
Business continuity, including recovery and management	✓
Supply chain security	✓
Security maintenance and vulnerability handling	✓
Assessing cybersecurity risk management measures	✓
Basic cyber hygiene practices	✓
Using cryptography and encryption	
Access control and asset management	✓
Multi-factor authentication	

- **Risk analysis & Information System Security Policies**

- Software and hardware inventory, Device Control governs the behavior when removable or mass storage devices are connected, monitor or deny the execution of system applications, such as PowerShell and performing automated vulnerability scans.

- **Incident Handling**

- Innovative technology such as anti-exploit in memory, contextual detections, malicious traffic detection, and managed services – Zero-Trust Application Services and a Threat Hunting Service – to automate prevention, detection and remediation of threats across all endpoints.

- **Business Continuity**

- Shadow copies can be created every 24 hours to return a compromised system to its previous state. The Advanced EPDR forensic and Investigation console allows you to determine the assets being affected for the recovery and notification phases

- **Supply Chain Security**

- WatchGuard Endpoint Security goes beyond traditional antivirus, offering deep detection, anti-exploit, and behaviour monitoring to stop hidden threats, even those from third-party suppliers.

- **Security Maintenance & Vulnerability Handling**

- Endpoint products can be used to discover vulnerabilities and EOL software. A Patch Management module reduces cybersecurity risks by providing the entire patch management cycle features.

- **Assessing Cybersecurity Risk Management Measures**

- Patch Management dashboards monitor security vulnerabilities with a patch to be applied, assessing the patch management policies and procedures

- **Basic Cyber Hygiene Practices**

- Include technologies and policies to reduce the attack surface at the endpoints, such as the detection and notification of unmanaged endpoints, protection issues, unconnected endpoints to the Cloud management console, antitampering technologies, and many other mechanisms that make the application of basic cyber hygiene practices easier.

- **Access Control & Asset Management**

- Full endpoint inventory such as CPU, RAM, TPM, MAC Address ETC
- Network Access Enforcement ensuring only devices compliant can connect to the network



WatchGuard Identity Security

Protect identities, assets, accounts, and information



AuthPoint Multi-Factor Authentication

Password | Mobile App | Push Message | Phone Biometrics | Mobile Device DNA
iOS & Android | 13 Languages | OTP | QR Code | Multiple Authenticators



Dark Web Monitor

Ongoing Monitoring | User & Admin Notifications | Rapid Password Changes



Corporate Password Manager

Integrated w/ AuthPoint MFA & SSO | Credentials Management | Increased Control & Protection



WatchGuard Cloud

Visibility | Identity Management | Token Allocation in Seconds | Risk Authentication



Extensive MFA Coverage

140+ 3rd-Party Integrations | Web SSO | Windows/Mac Computer Logon



Matching Cyber Security Solutions to NIS2 Directive Requirements

AuthPoint	
Risk analysis and information system security policies	
Incident handling	
Business continuity, including recovery and management	
Supply chain security	
Security maintenance and vulnerability handling	
Assessing cybersecurity risk management measures	
Basic cyber hygiene practices	
Using cryptography and encryption	
Access control and asset management	
Multi-factor authentication	✓

■ Multi-Factor Authentication (MFA)

- WatchGuard AuthPoint provides multi-factor authentication (MFA) for a large ecosystem of 3rd-party applications.
- Users can authenticate right from their own phone or using an optional hardware token. AuthPoint supports Push notification, QR Code challenge and response, and OTP (one time password) as a second factor.
- The mobile token is tied to the specific mobile phone used by the user and cannot be copied or cloned to another phone. MFA can be configured for VPN access by simply integrating AuthPoint in WatchGuard Cloud. AuthPoint MFA extends to custom-developed applications through RESTful APIs. It also offers user inheritance to simplify access control for service providers by allowing them to easily revoke resource access upon service provider employee departure.

WatchGuard MDR

WatchGuard MDR offers 24/7 managed threat detection and response by a team of seasoned cybersecurity experts from the WatchGuard SOC.

It empowers MSPs who don't run a full-time, in-house security operation center (SOC).

WatchGuard MDR:

- **Enhanced Security Expertise** – leverage external experts that extend in-house experience.
- **24/7 Monitoring** – ensure threats are detected and addressed promptly.
- **Access to Advanced Technologies** – take advantage of cutting-edge products, technologies, and methodologies.
- **Rapid Response** – minimise the damage and downtime of security incidents.
- **Threat Intelligence of the latest attacks** – enhance your preventative security measures.



24/7 Cyber Protection
Without the Overhead

MDR



Smart Security. Simply Done.

Matching Cyber Security Solutions to NIS2 Directive Requirements

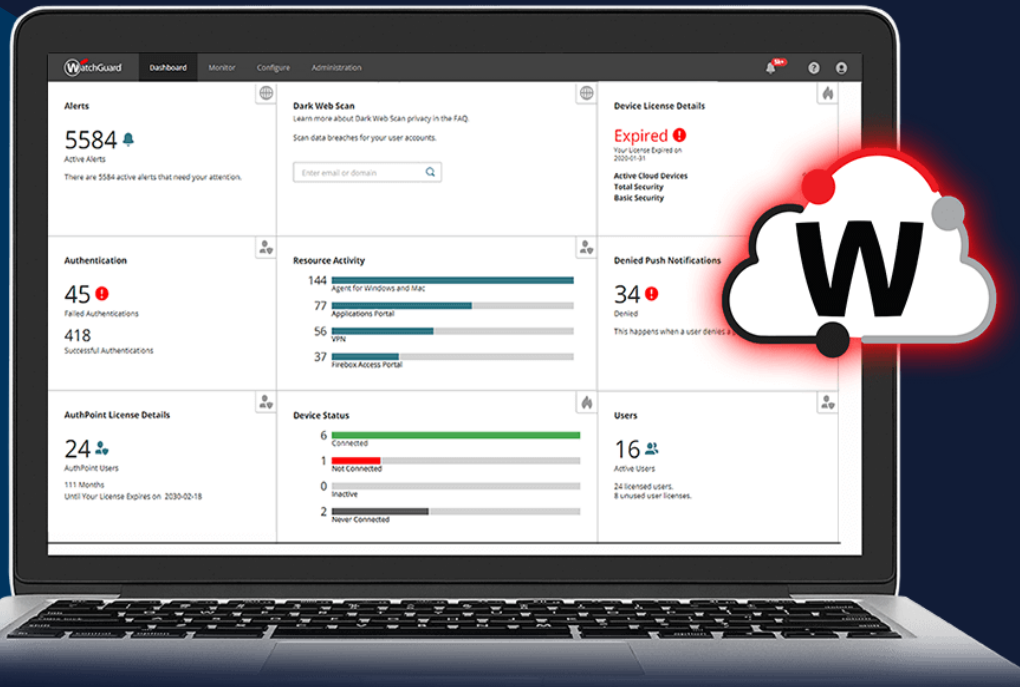
	MDR
Risk analysis and information system security policies	✓
Incident handling	✓
Business continuity, including recovery and management	✓
Supply chain security	✓
Security maintenance and vulnerability handling	✓
Assessing cybersecurity risk management measures	
Basic cyber hygiene practices	✓
Using cryptography and encryption	✓
Access control and asset management	
Multi-factor authentication	

- **Risk analysis & information system security policies**
 - Weekly security health reports provide key information on endpoint risk based on protection status and configuration, detections, and security patches pending installation.
- **Incident Handling**
 - A WatchGuard skilled team of cybersecurity experts keeps customers' endpoints safe with 24/7 security monitoring, threat hunting, attack prevention, detection, and containment..
- **Business continuity**
 - Ensures business continuity management with 24/7 detection and collaboration with our MSPs in responding to security incidents across endpoints and Microsoft 365, leveraging a seasoned cybersecurity team, AI, and advanced technologies from WatchGuard SOC.
- **Supply Chain Security**
 - WatchGuard SOC threat hunters and analysts work around the clock to proactively hunt for, validate, and investigate potential supply chain threats and incidents, correlating abnormal application behaviors and providing guidelines for responding to our partners
- **Security Maintenance & Vulnerability Handling**
 - The Managed Detection and Response (MDR) service oversees information systems from a 24x7 security operations center (SOC) operated by cybersecurity experts with Weekly security health reports
- **Basic Cyber Hygiene Practices**
 - Weekly health reports uncover endpoints at risk and recommend that cyber hygiene practices be implemented.
- **Using Cryptography and Encryption**
 - WatchGuard SOC analysts monitor encryption library usage to detect any attempts at ransomware cyberattacks as soon as possible.

Centralized Control with WatchGuard Cloud



WatchGuard Cloud is the centralized management interface for the entire Unified Security Platform and is the single console for security policy management, dissemination, and enforcement.



Management Capabilities:

- Zero-touch deployment of network security, MFA, and endpoint security solutions
- Quickly enable or disable security services
- Minimize alert fatigue and stay ahead of threats with automation
- Multi-tier, multi-tenant architecture
- Access to leading RMM and PSA tools
- Much more

Matching Cyber Security Solutions to NIS2 Directive Requirements

WatchGuard Cloud	
Risk analysis and information system security policies	
Incident handling	
Business continuity, including recovery and management	✓
Supply chain security	✓
Security maintenance and vulnerability handling	
Assessing cybersecurity risk management measures	✓
Basic cyber hygiene practices	
Using cryptography and encryption	✓
Access control and asset management	✓
Multi-factor authentication	

- **Business Continuity**
 - WatchGuard Cloud facilitates backups of critical security infrastructure configurations, such as Fireboxes and WatchGuard access points. Through integrations with Remote Monitoring and Management tools, endpoint devices can quickly be isolated, remediated, and redeployed if necessary.
- **Supply Chain Security**
 - Through WatchGuard Cloud, you can generate executive summary and configuration reports that can be used to document security controls to auditors and other entities in the supply chain when requested.
- **Assessing Cybersecurity Risk Management Measures**
 - WatchGuard Cloud provides extensive visibility and reporting on discrepancies in the configuration of the cybersecurity products. For example: a policy usage report for the firewall that shows unused policies.
- **Using Cryptography and Encryption**
 - All management of products from WatchGuard Cloud is delivered by secure, encrypted communications.
- **Access Control & Asset Management**
 - WatchGuard Cloud simplifies asset management by offering a centralized console to track and manage all your WatchGuard devices, including firewalls, endpoints, and access points. This provides a clear overview of your network security posture, allowing you to efficiently allocate licenses and respond to threats

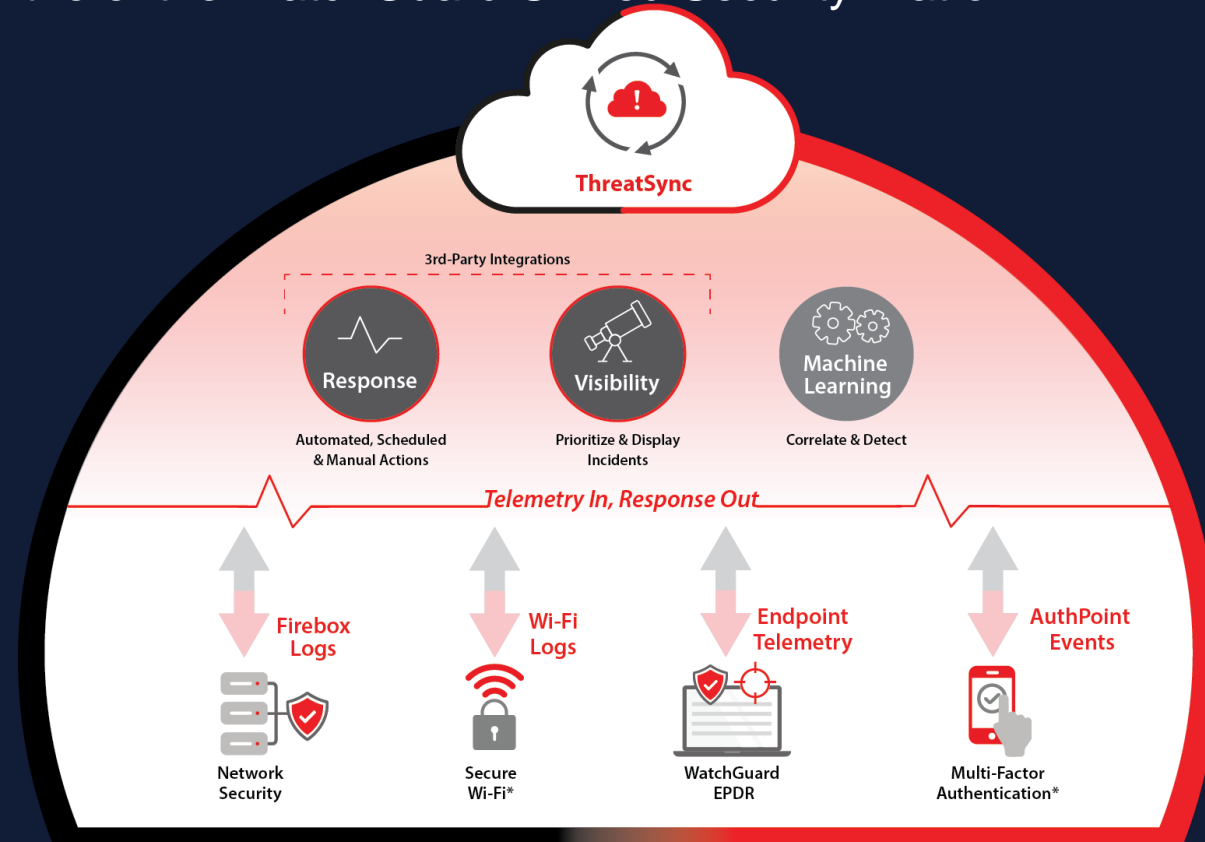
XDR with ThreatSync®



ThreatSync saves security team cycles, speeds detection, and increases their accuracy by automatically correlating relevant threat data from the entire WatchGuard Unified Security Platform.

ThreatSync:

- An integrated platform for delivering extended detection and response (XDR) across environments, users, and devices
- Collects, correlates, analyses, and responds to threats across security layers
- Delivers an easy-to-understand threat score for indicators and incidents
- Provides a detailed, contextualised, and actionable picture of your threat surface



100s of billions
of events analyzed



2.1 billion binaries
classified



Millions of adversary
movements tracked



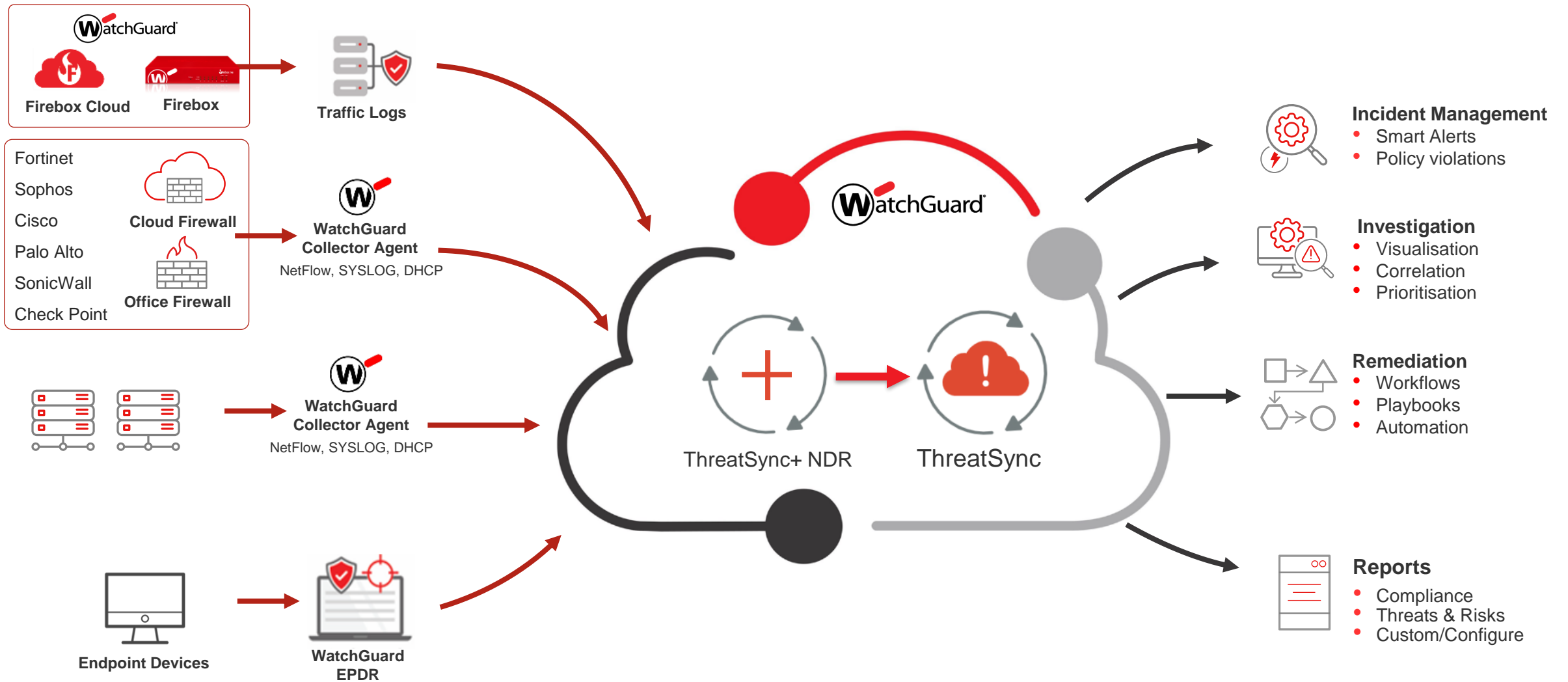
Thousands of zero day
malware blocked

Matching Cyber Security Solutions to NIS2 Directive Requirements

	ThreatSync+ NDR
Risk analysis and information system security policies	✓
Incident handling	✓
Business continuity, including recovery and management	
Supply chain security	✓
Security maintenance and vulnerability handling	✓
Assessing cybersecurity risk management measures	
Basic cyber hygiene practices	
Using cryptography and encryption	
Access control and asset management	
Multi-factor authentication	

- **Risk Analysis & Information System Security Policies**
 - NDR helps in risk analysis by providing detailed insights into your network’s vulnerabilities and potential threats. You can prioritize security measures by understanding your network’s attack surface and identifying high-risk areas. The NDR solution also includes ISO27001 and NIST CSF security policies that support risk analysis. The solution generates comprehensive reports that can be used to inform and strengthen your organisation’s information system security policies. This data-driven approach ensures that your policies align with current threats and regulatory requirements
- **Incident Handling**
 - NDR utilises an advanced AI engine to detect and respond to potential attacks across your network threat surface. The solution helps you manage security incidents from start to finish. If an attack occurs within the network environment, it will quickly be detected and support an immediate and effective response, limiting damage.
- **Supply Chain Security**
 - Digital supply ecosystems depend on interconnected networks and communications among supply chain partners. ThreatSync+ NDR constantly monitors network communications within and across network boundaries, identifying and reporting risks and vulnerabilities while also watching for potential threats. The solution provides supply chain risk reports that third-party risk assessors can utilise to evaluate the cybersecurity practices of each member.
- **Security Maintenance & Vulnerability Handling**
 - NDR solution helps with network and information systems security by providing advanced threat detection and response capabilities, including vulnerability detection and response. It uses AI and machine learning to identify and address network-based threats, reducing the risk of breaches and minimizing the impact of incidents. This helps organisations by ensuring the security of their systems and data throughout their life cycle.

Open XDR with ThreatSync+



Matching WatchGuard Solutions to Directive Requirements

	Authpoint	Endpoint Security	Firebox	MDR	Orion	Advanced Reporting Tool	Patch Management	WatchGuard Cloud	ThreatSync	Data Control	Full Encryption
Risk analysis and information system security policies		✓		✓		✓	✓		✓	✓	✓
Incident handling		✓	✓	✓	✓	✓	✓		✓	✓	✓
Business continuity, including recovery and management		✓		✓	✓		✓	✓			
Supply chain security		✓		✓	✓			✓			
Security maintenance and vulnerability handling		✓	✓	✓			✓		✓		
Assessing cybersecurity risk management measures		✓					✓	✓			
Basic cyber hygiene practices		✓		✓		✓	✓				✓
Using cryptography and encryption			✓	✓	✓			✓			✓
Access control and asset management		✓	✓					✓			
Multi-factor authentication	✓		✓								



WHITEPAPER

NIS 2 Compliance with WatchGuard Technologies



<https://www.watchguard.com/wgrd-resource-center/white-paper/demystifying-nis-2-requirements>



Thank You

GDPR
GENERAL
INTRODUCING

NEIL RAWLINS
KEEPIT

keepit®

DATA
PROTECTION

Your data.
Here today.
Here tomorrow.



Neil Rawlins
UK&I Solutions Engineering Manager
NRA@Keepit.com

Tried, tested, and proven



10000 customers across 74 countries



Millions of users protected



Offices worldwide



7 data center regions



8 workloads

Data centers in 7 regions worldwide



USA

Canada

Australia

UK

EU - Germany and

Denmark

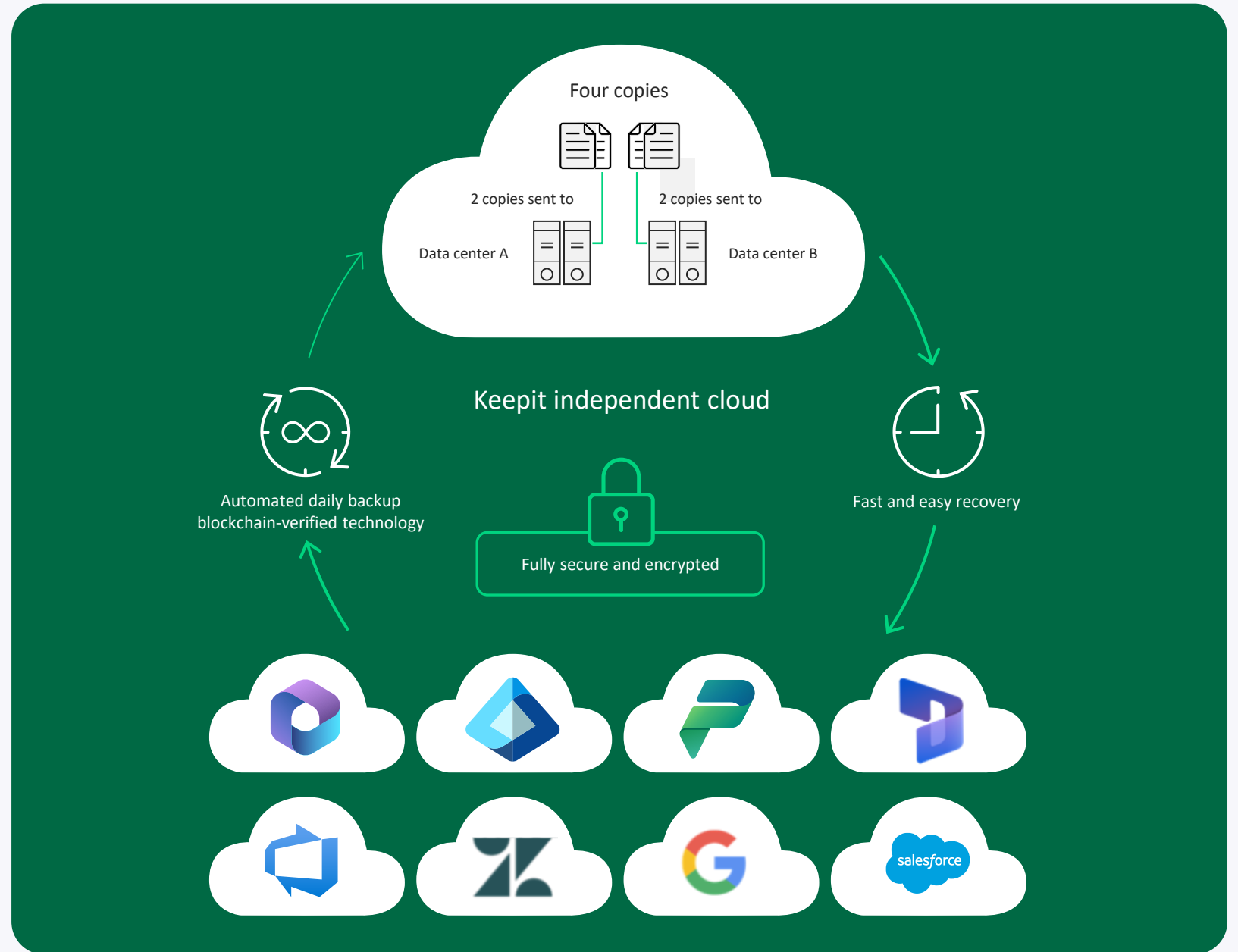
Switzerland





Dedicated independent cloud

- Independent
- Secure and certified
- Complete control over technology stack
- Multi-region support
- Fully redundant – 2x2

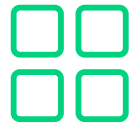


Key things we don't dig into when we talk about the cloud



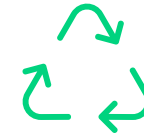
Where is my data?

- AWS, Azure, Private or locally hosted?
- Is it stored in the region?
- Will it stay in the region?
- Is it compliant?



Is there resiliency?

- How many copies?
- Is it part of my environment?
- Is it protected externally and internally?



Can I recover that data?

- Immutability?
- What does Immutability mean?
- Who owns the data cycle?
- What happens if the root changes?

Data Locality?


Data Locality is an increasing focus point for businesses with the evolving landscape of data ownership and protection.



Where is my Data?

- Where is it hosted?
- Who has access to it?
- Where is it processed?
- Is it compliant?

More than 40% of Companies Don't Know Where their Data is Stored

 Renu Bhaskaran | 5 min read | Updated On - December 20, 2023



As you can imagine, a company's inability to locate their critical assets is a big problem for security. After all, should an attacker gain access to, and disclose a company's sensitive data, this could be devastating for the company's reputation and financial well-being. Despite the risks, there's still a large number of companies who simply don't know where their data is stored.

According to a report by the Institute of Directors (IoD) and Barclays, as much as 43% of those who took part in the study are not able to identify the location of their critical data, with as much as 59% of respondents outsourcing data storage. Some other studies have confirmed this trend. A 2014 study by the Ponemon Institute revealed that 52% of respondents have a "lack of knowledge regarding data", while a 2017 report called "The Data Security Money Pit: Expense In Depth Hinders Maturity", claims that 62% of respondents are not able to identify the location of their most "sensitive unstructured data".

Lee Fisher, head of security business for EMEA at Juniper Networks, stated that "We estimate that 50-60% of businesses don't know where their data is". He also went on to say that "there is a misunderstanding of how to use data and they don't know how to protect appropriately."

To make matters worse, 43% of businesses are failing to report their most disruptive data breaches. Only 57% of companies have a formal cyber security strategy in place, while only 49% of companies are providing cyber security training to their staff. And despite the financial risks associated with a data breach, only 20% of companies have any form of cyber insurance. As I'm sure you can appreciate, these figures paint a fairly bleak picture of the current cyber security trends.

US Cloud ACT

Computer Weekly revealed in 2020 that dozens of police forces are processing more than a million people's data unlawfully using the cloud-based Microsoft 365 software

Police watchdog raising concerns about how the use of Azure “would not be legal”.

Inability to comply with contractual clauses around data sovereignty.

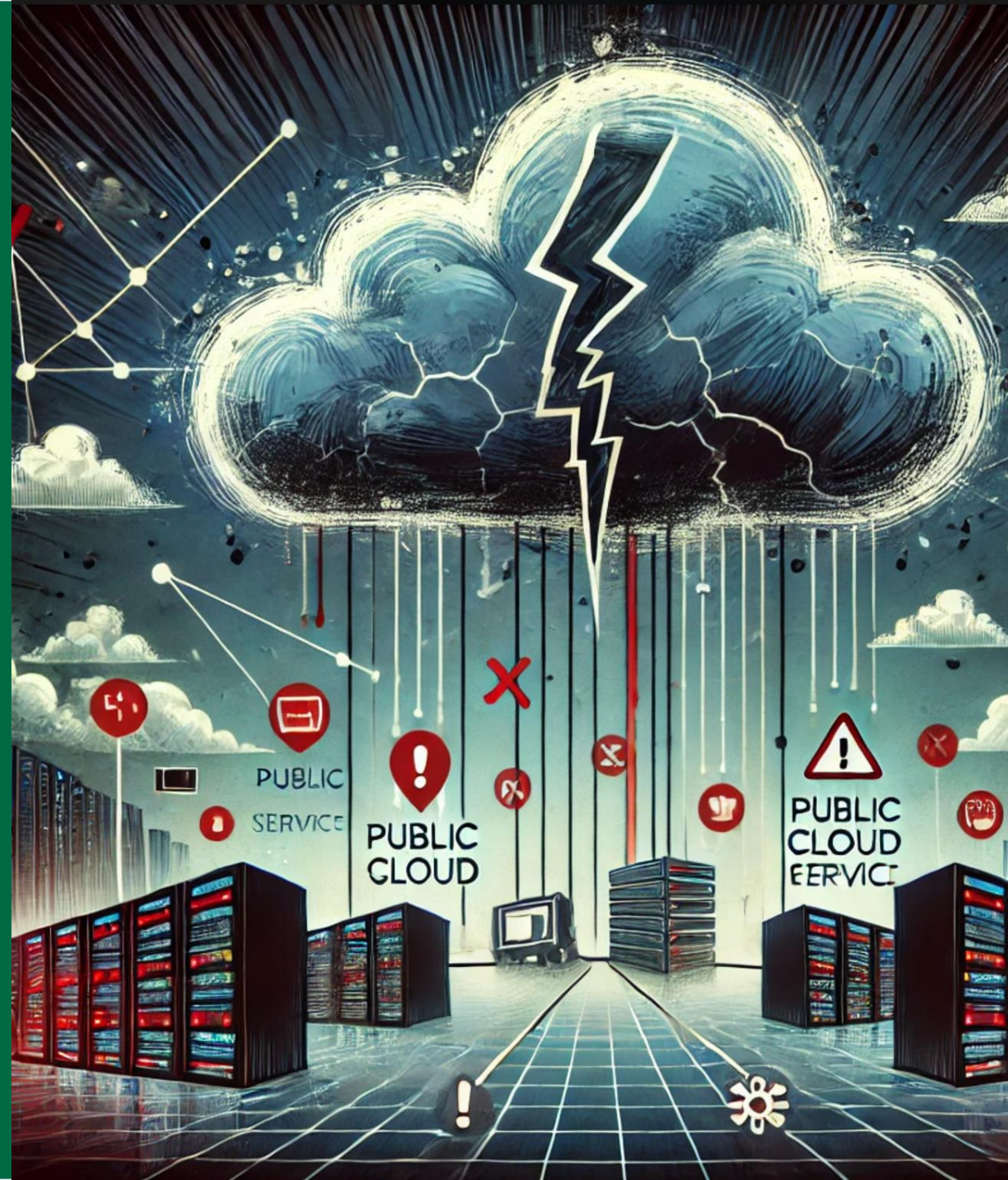
The screenshot shows a news article on the Computer Weekly website. The article is titled "ICO prompts confusion over police cloud legality" and is dated 19 Jan 2024. The author is Sebastian Klovig Skelton, Data & ethics editor. The article discusses the Information Commissioner Office (ICO) expressing confusion over the legality of police forces using US-based cloud providers to process sensitive law enforcement data. It mentions that Computer Weekly revealed in 2020 that dozens of police forces are processing more than a million people's data unlawfully using Microsoft 365 software. The article also notes that following Computer Weekly's subsequent discovery that a major Police Scotland IT system is similarly using Microsoft's Azure cloud despite major unresolved data protection issues, the Scottish biometric commissioner (SBC) sought advice from the ICO about the system's legality. A quote from SBC Brian Plastow is included, stating that the ICO was likely to greenlight the controversial cloud deployments because it believed an information-sharing deal signed by the UK and US governments superseded the UK's data protection laws. Another quote explains that the UK ICO is unlikely to opine that the uploading of biometric data to US-based cloud infrastructure by Police Scotland conflicts with UK data protection law, as it was stated in a letter dated 14 December 2023. The article concludes that this is because Article 3 of the agreement between the US and UK government's on access to electronic data under the US Cloud Act requires each party to the agreement to ensure that its domestic laws do not frustrate or impair the operation of the agreement.

At the top of the page, there is a navigation bar with logos for TechTarget and ComputerWeekly.com, along with dropdown menus for IT Management, Industry Sectors, and Technology Topics. A search bar is also present. Below the article, there is a "Latest News" section with several headlines, a "View All News" button, and a "Download Computer Weekly" section with a thumbnail image of the magazine cover and a list of featured articles in the current issue.



What happens if the cloud fails?

A user deletes a critical Power Platform component, or Power BI report, or makes a change that breaks a dataflow?



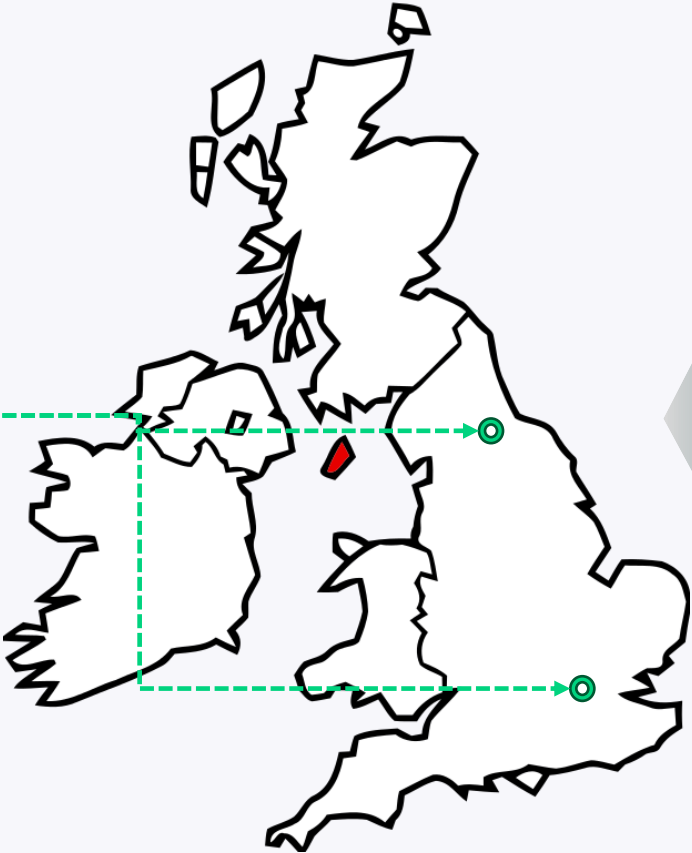
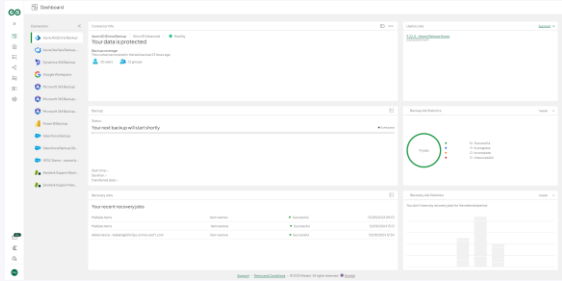
Cloud Concentration Risk

- Is my backup in the same Tenant/Location?
- If one goes down, where do I recover?
- What is your uptime?
- Where should I store the data?



keopit® Datacenter Resiliency

6-5-4-3-2-1 Rule?



4 Copies Of Data

- 1
- 2
- 3
- 4



Immutability and what does it mean to you?

We use Immutability more and more within backups, we need to question what else is needed?

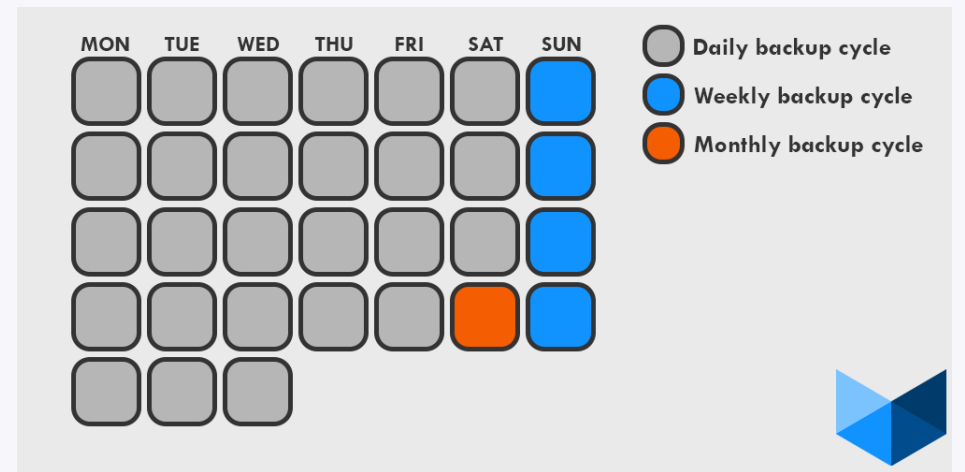


Immutability? One answer?

- Is it a golden bullet?
- Who owns the coverage?
- Snapshot loss
- Clean location?

```

NAMESPACE spawning /lib/systemd/systemd-logind: No such file or directory
systemd-logind.service: Failed to connect stdout to the journal socket, ignoring: No such file or directory
systemd-logind.service: Failed to set up mount namespacing: /run/systemd/unit-root/dev/kmsg: No such file or directory
systemd-logind.service: Failed at step NAMESPACE spawning /lib/systemd/systemd-logind: No such file or directory
systemd-logind.service: Failed to connect stdout to the journal socket, ignoring: No such file or directory
systemd-logind.service: Failed to set up mount namespacing: /run/systemd/unit-root/dev/kmsg: No such file or directory
systemd-logind.service: Failed at step NAMESPACE spawning /lib/systemd/systemd-logind: No such file or directory
systemd-logind.service: Failed to connect stdout to the journal socket, ignoring: No such file or directory
systemd-logind.service: Failed to set up mount namespacing: /run/systemd/unit-root/dev/kmsg: No such file or directory
systemd-logind.service: Failed at step NAMESPACE spawning /lib/systemd/systemd-logind: No such file or directory [ 2146.584615]
systemd[2469]: lightdm.service: Failed to execute command: No such file or directory
[ 2146.584810] systemd[2469]: lightdm.service: Failed at step EXEC spawning /usr/sbin/lightdm: No such file or directory
[ 2146.832832] systemd[2470]: lightdm.service: Failed to execute command: No such file or directory
[ 2146.833004] systemd[2470]: lightdm.service: Failed at step EXEC spawning /usr/sbin/lightdm: No such file or directory
[ 2147.081875] systemd[2471]: lightdm.service: Failed to execute command: No such file or directory
[ 2147.083832] systemd[2471]: lightdm.service: Failed at step EXEC spawning /usr/sbin/lightdm: No such file or directory
[ 2147.372183] systemd[2473]: lightdm.service: Failed to execute command: No such file or directory
[ 2147.373978] systemd[2473]: lightdm.service: Failed at step EXEC spawning /usr/sbin/lightdm: No such file or directory
[ 2147.582489] systemd[2474]: lightdm.service: Failed to execute command: No such file or directory
[ 2147.584636] systemd[2474]: lightdm.service: Failed at step EXEC spawning /usr/sbin/lightdm: No such file or directory
  
```





keepit®

THANK YOU

PLEASE RETURN BY 14:40

**COFFEE BREAK
SESSIONS RESUME SHORTLY**



**DATA
PROTECTION**

GDPR GENERAL INTRODUCING

JOSHUA FOYE
PAX8



DATA
PROTECTION



Modernise your workplace

Using technology to stay
ahead of the game



Joshua Foye

Technical Consultant – Modern Workplace,
Pax8 Academy

A person's hand is pointing at a tablet computer that displays a bar chart. The background is a blurred office environment with a desk, a calculator, and some papers. The text "What technologies do you use in your business?" is overlaid in white on the image.

What technologies do you use in your business?

Every business is becoming more demanding



Remote and
hybrid working



Risk
reduction



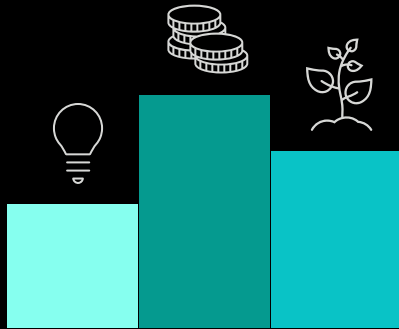
Business model
flexibility



Data-driven
insights

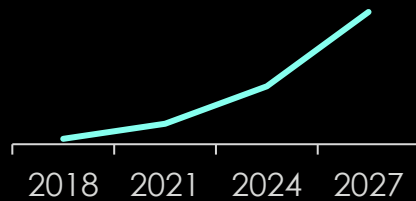
Technology trends

Demands for sustainable IT practices



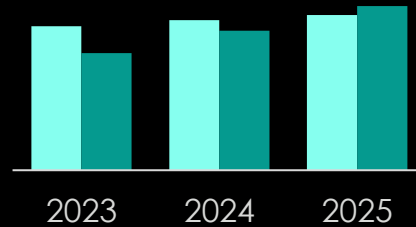
CxOs rank sustainability as a pressing issue for 2024/5

Continued enhancements in connectivity



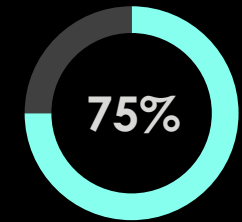
Growth in data usage across non-fixed networks

Relentless evolution of cloud computing



Cloud is set to overtake traditional spend in 2025

Everyday end-user adoption of AI

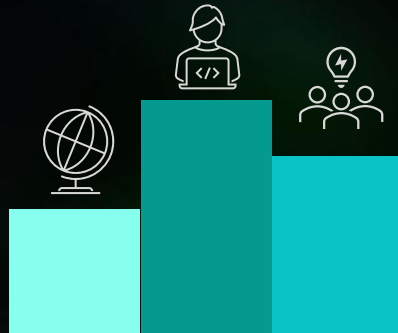


Global knowledge workers using AI at work

Sources: 1. Deloitte, *2024 CxO Sustainability Report (2024)*; 2. Ericsson, *Ericsson Mobility Report (2024)*; 3. Gartner, *Cloud Shift – 2023 Through 2027 (2023)*; 4. Microsoft and LinkedIn, *2024 Work Trend Index Annual Report (2024)*

Threats to the Modern Workplace

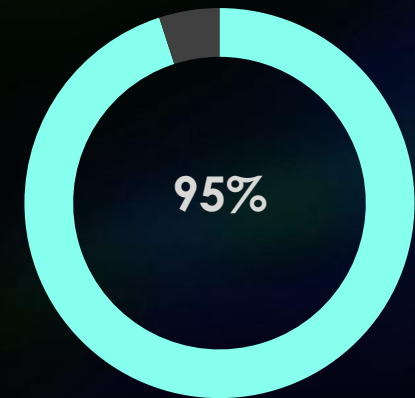
Social engineering just became easy



Supply chains are growing, bringing additional risks



Users are **still** the biggest risk to the company



Sources: 1. NCSC, *The near-term impact of AI on the cyber threat*; 2. Embroker, *Top 16 Cybersecurity Threats in 2024*; 3. Parachute Cloud, *Cyber Attack Statistics to Know (2024)*

“

We are building a modern workplace,
which **starts with empowering everyone.**

– Satya Nadella, CEO of Microsoft

”

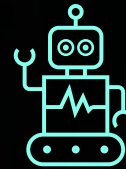
What is next for the modern workplace?



Evolution of
the physical
office



Employee well-
being and
experience



User-driven
adoption of AI
technologies



Managing
end-of-lifecycle
applications

What to do with the infrastructure?

Technical debt

69% of IT leaders say technical debt limits their ability to innovate.¹

Performance and scalability

On-premise environments lack the agility required to keep pace with the latest technology trends.

Security and compliance

75% of businesses report that cybersecurity is a high priority for their senior management.²

Bespoke systems

Maintain, evolve and drive innovation through the entire stack of your systems.

Sources:

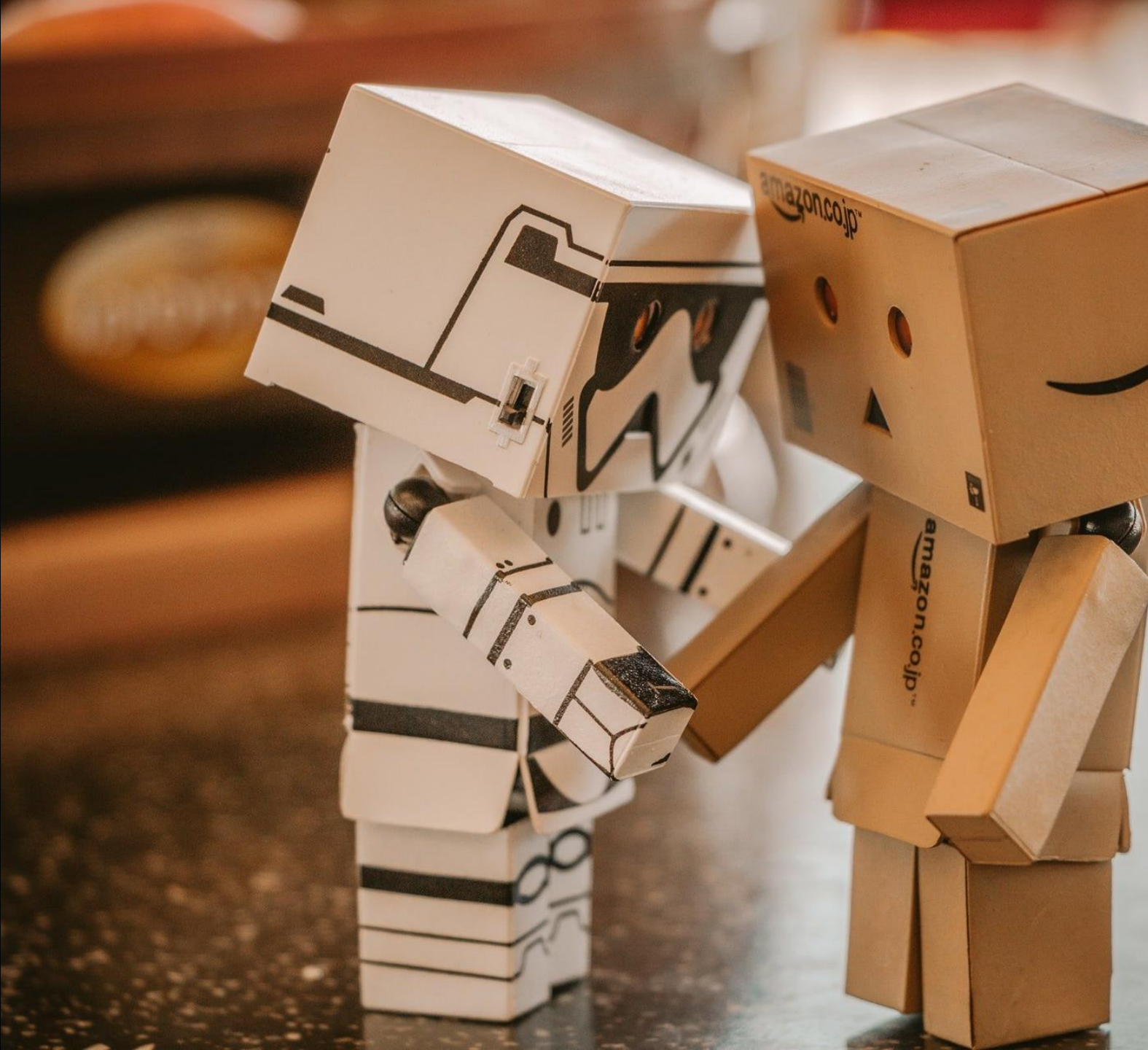
1. OutSystems, *The Growing Threat of Technical Debt* (2021)
2. UK Government, *Cyber security breaches survey 2024* (2024)

“

AI isn't as easy as just turning it on.
Delivering great AI experiences
requires time, expertise and data.

– Ahyoung An, Senior Director of Product Management at Mulesoft

”



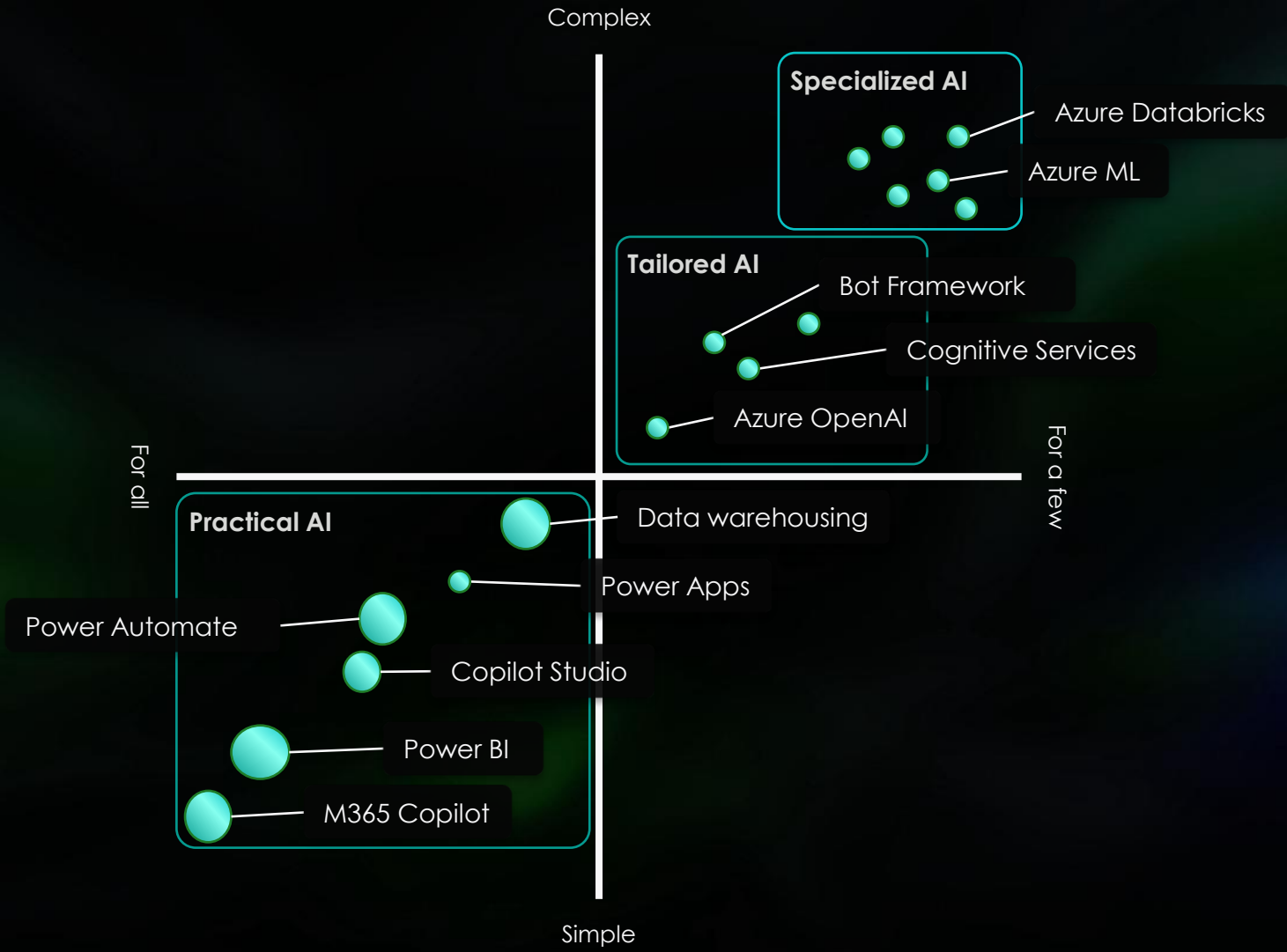
But..
What is AI?



“Artificial refers to any system created and **not biologically born”**

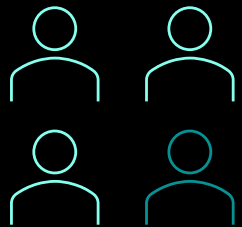
An open book with a pair of glasses resting on it, serving as a background for a quote. The book is open to two pages of text, and the glasses are positioned over the center. The lighting is soft, highlighting the pages and the frame of the glasses.

“Intelligence is the ability to acquire and apply knowledge and skills”



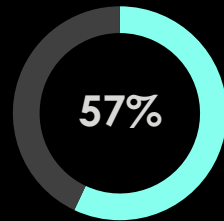
Prepare for Artificial Intelligence

Assess and secure data



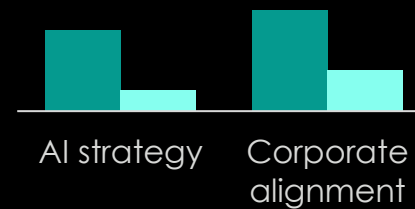
3 out of 4 leaders cite data silos as a barrier to AI adoption

Train and upskill employees



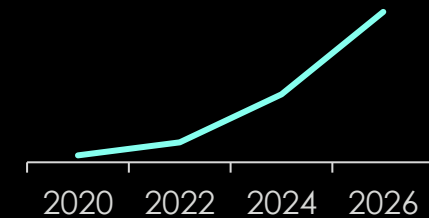
Employees want employers to offer AI training

Define insight objectives



Leading organisations have aligned AI strategies

Build strategic partnerships



Spend on AI within the channel is rapidly growing

Key Takeaways

1

AI needs to solve real business issues – not just become a buzzword – and this requires a well-defined technology & AI strategy

2

Your users are demanding a great experience, supported by new and exciting technologies

3

The cyberthreat landscape demands modern security solutions

GDPR
GENERAL
INTRODUCING

HENNIE ERASMUS
AVEPOINT



DATA
PROTECTION



Expand Your Business with Copilot for Microsoft 365



Dionne Harward
Partner Account Manager, AvePoint



Hennie Erasmus
Solutions Engineer, AvePoint

A Platform You Can Trust



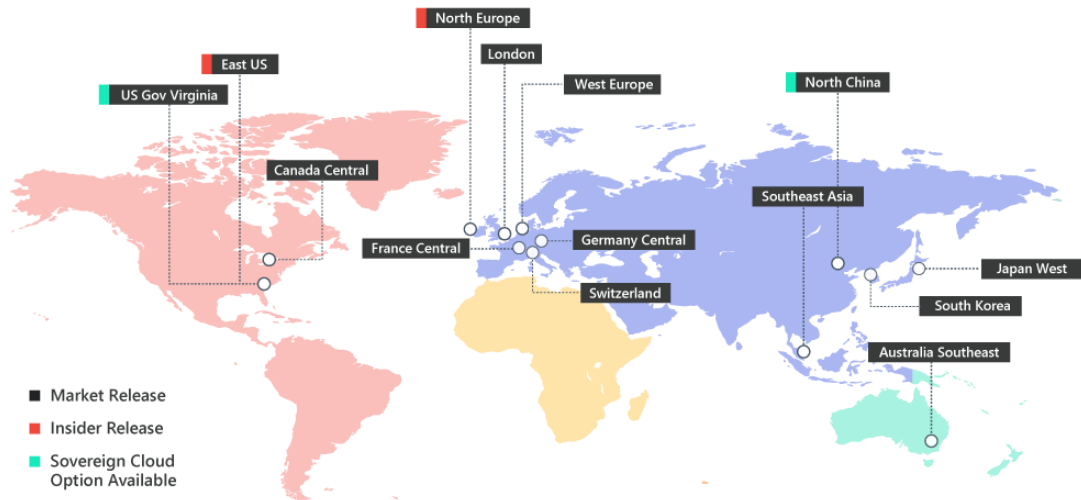
Migrate.



Manage.



Protect.



14
Global Cloud
Instances

99.9%
Availability
Backed by Azure

24/7
World-Class
Support

325PB
Managed
Customer Data



21K+
Customers

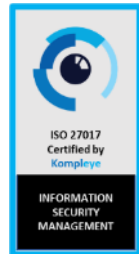
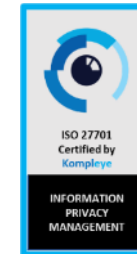
17.1M
Cloud Seats



is headquartered and maintains its principal operational center in Jersey City, NJ, with approximately 2,500 employees across five continents.

100+
Countries

7
Continents



Microsoft
Partner



PARTNER
SINCE 2022

Customers We Serve

Communications



Retail / Consumer



Pharma & Health



Financial Services



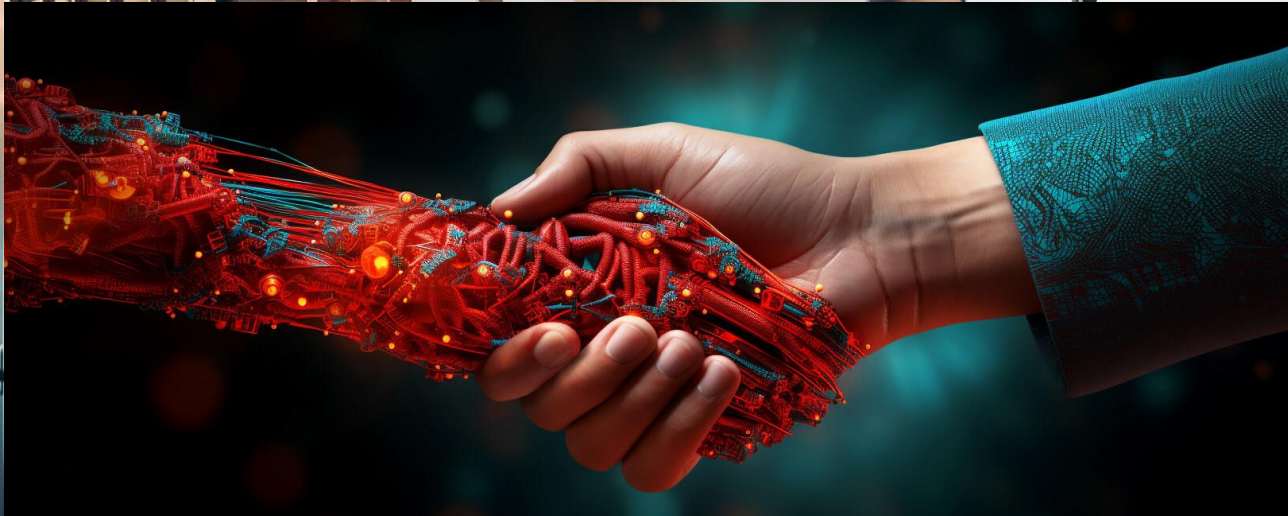
Govt / Education



High Technology



AGENDA



What is Microsoft 365 Copilot?

Establish Your Data Foundation

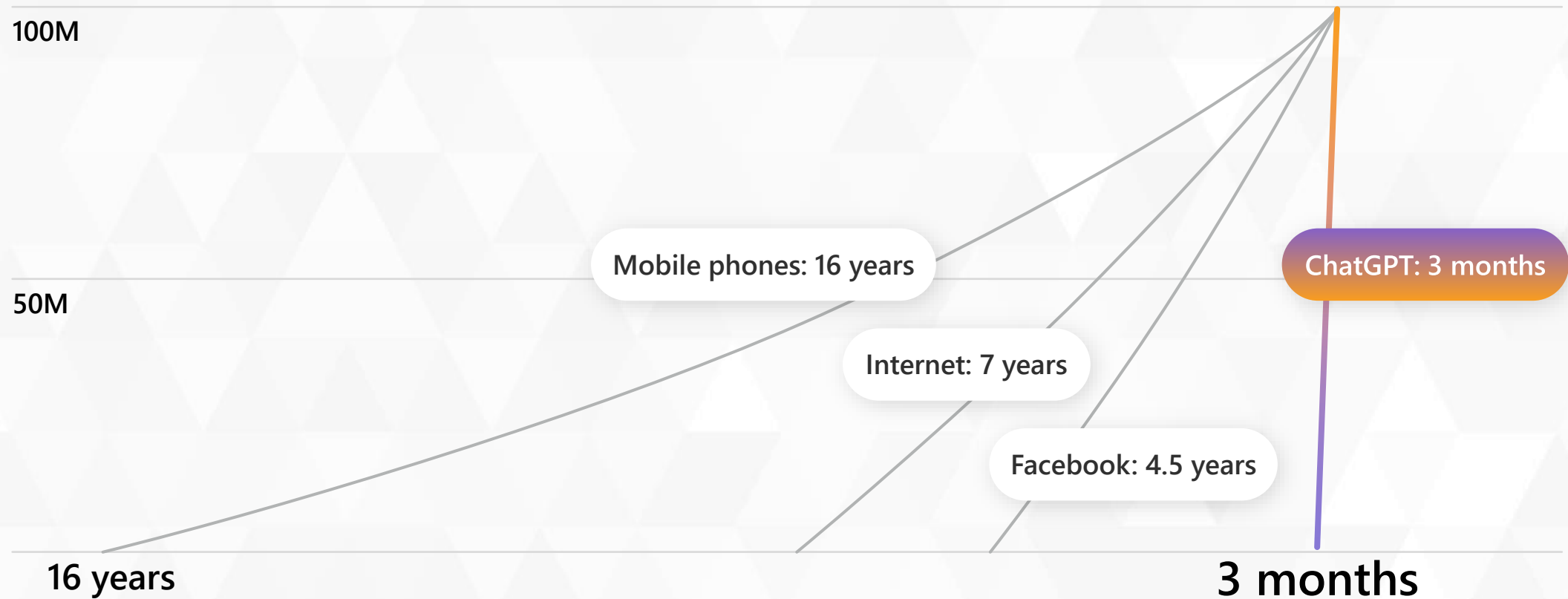
Enabling your technology

Expand Your Business
with Copilot for Microsoft 365

What is Copilot for Microsoft 365?

Generative AI technology is here

Time to reach 100M users

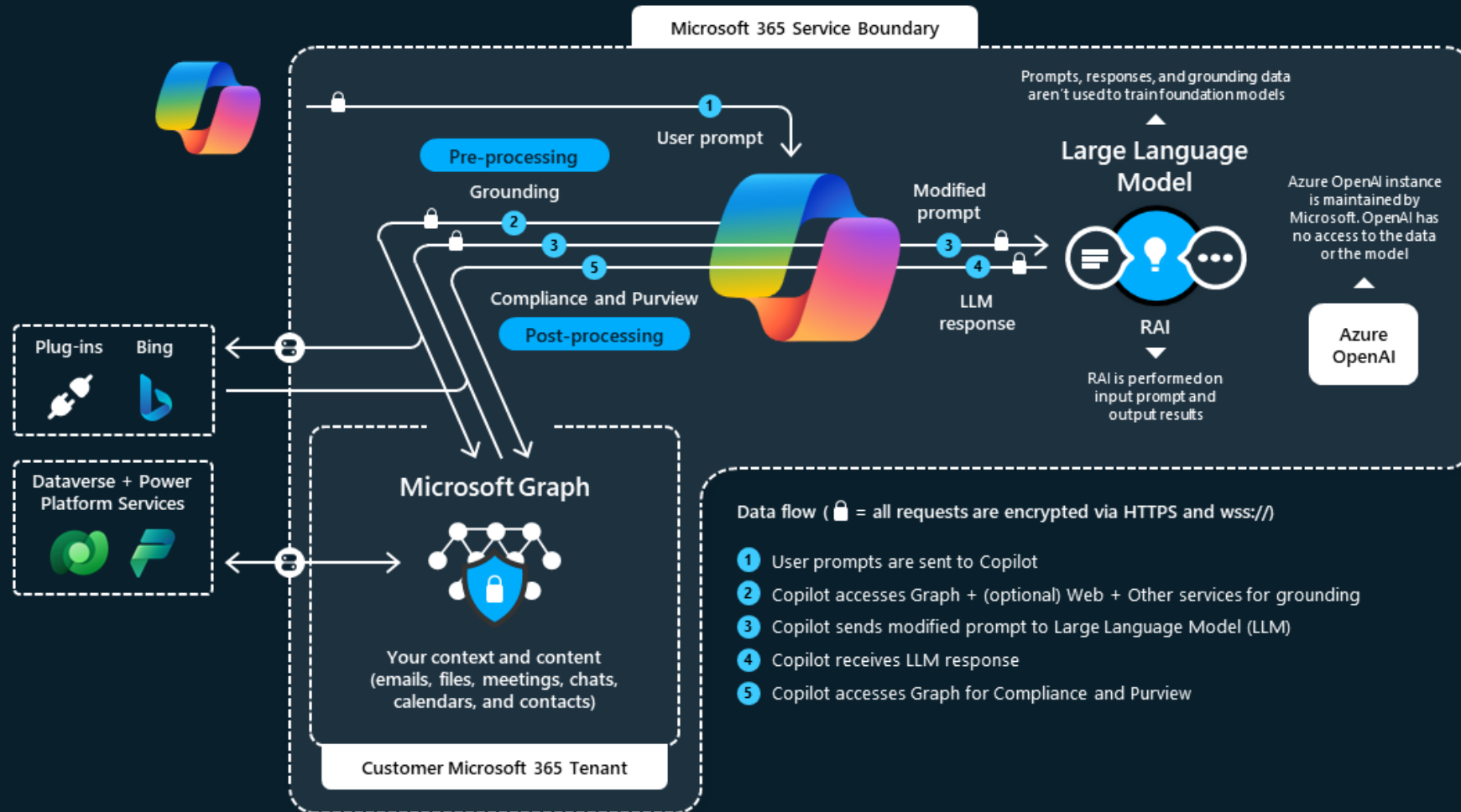


Generative AI

is a subset of artificial intelligence that provides the ability to create new and original data, based on input data.

Generative AI technology is here

Microsoft Copilot for Microsoft 365 architecture



What every employee wants from AI



Finding info
and answers



Summarising meetings
and action items



Creative
work



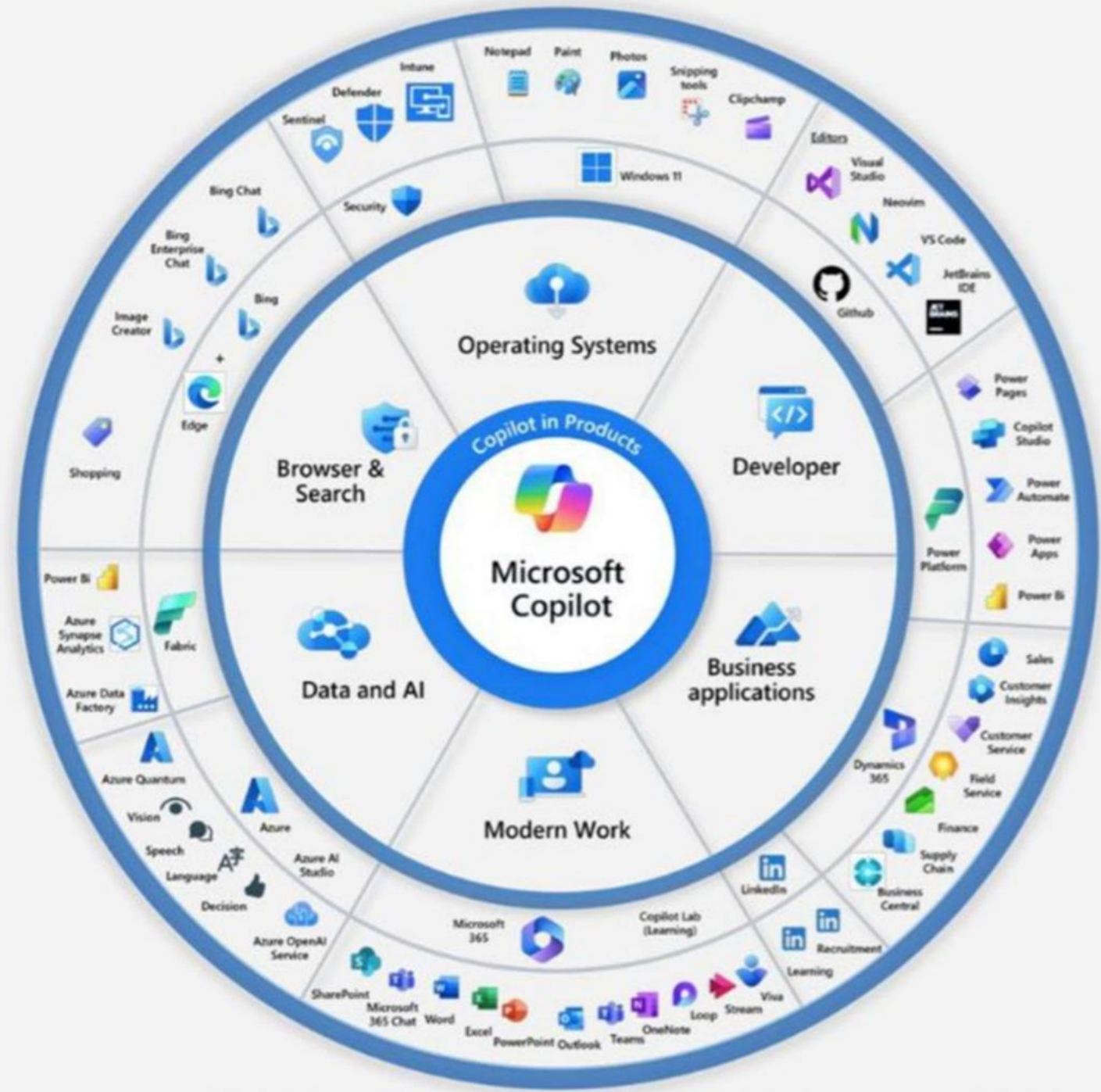
Analytical work



Planning their day



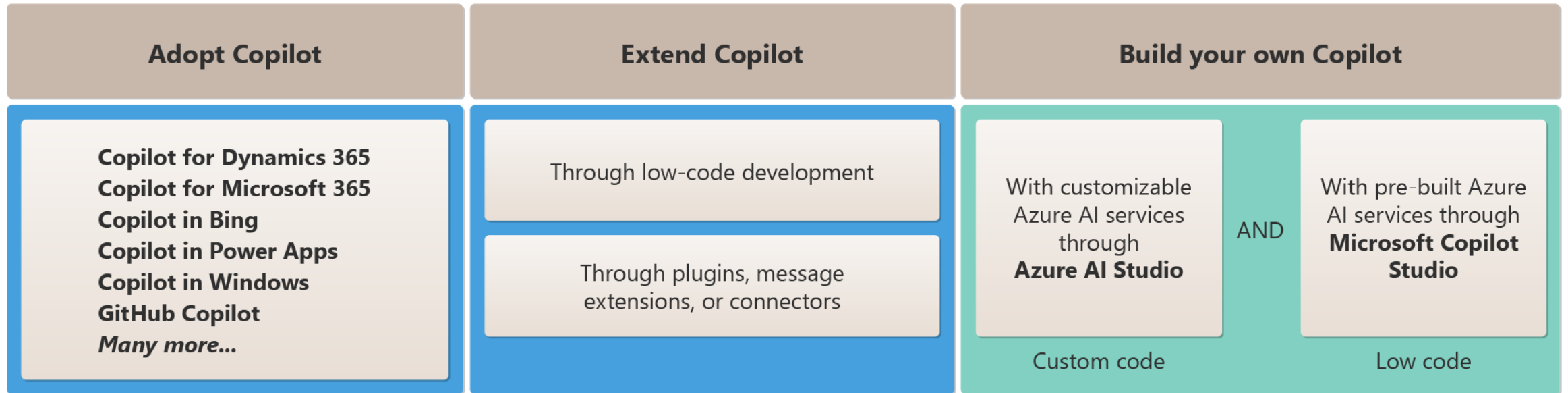
Admin tasks



All The Copilots: aka.ms/MicrosoftCopilots



Copilot experiences across the Microsoft Cloud

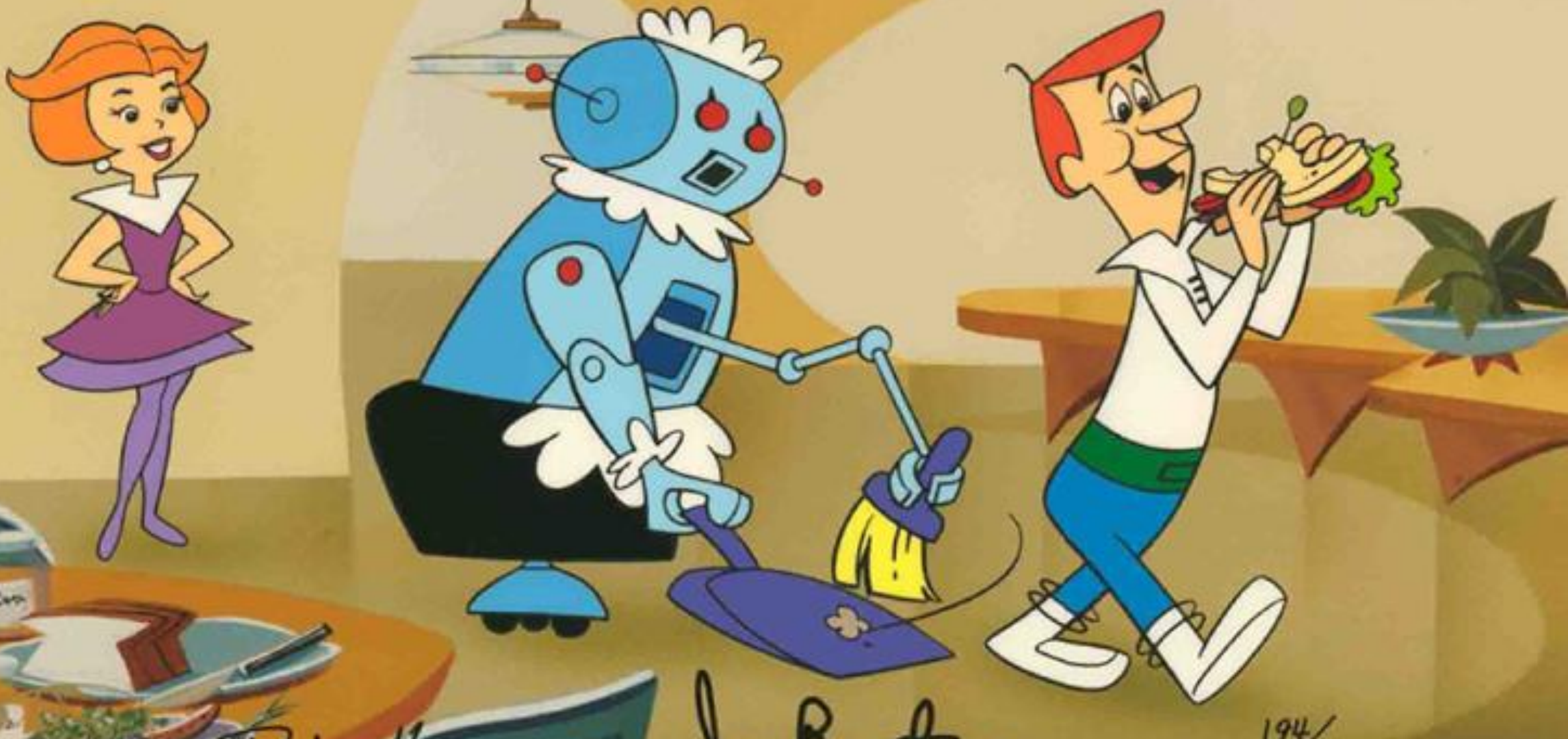


A woman in a white lab coat is looking at a tablet. The background is a futuristic cityscape with tall buildings and a grid pattern. A red and purple gradient box is overlaid on the image, containing the text "Autopilot" and "Copilot".

"Autopilot"

"Copilot"

The future (now) of cleaning up.



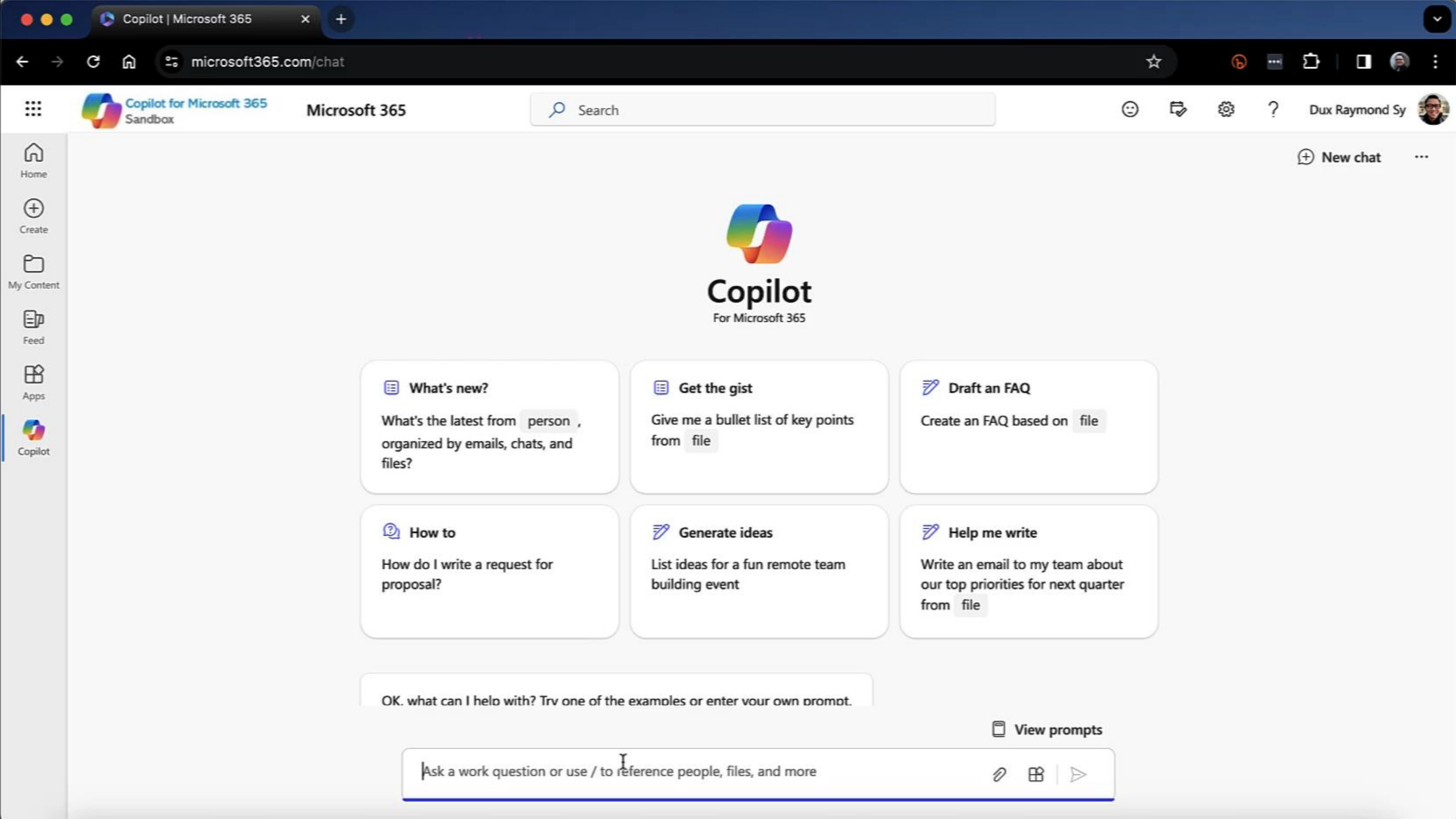
Document editing area containing a single paragraph with the text "Aptos (Body)".

Copilot

Ask
How can I more concisely describe [time management?]

Chat history

Ask me anything about this document



- Home
- Create
- My Content
- Feed
- Apps
- Copilot

Copilot

For Microsoft 365

What's new?

What's the latest from **person**, organized by emails, chats, and files?

Get the gist

Give me a bullet list of key points from **file**

Draft an FAQ

Create an FAQ based on **file**

How to

How do I write a request for proposal?

Generate ideas

List ideas for a fun remote team building event

Help me write

Write an email to my team about our top priorities for next quarter from **file**

OK. what can I help with? Try one of the examples or enter your own prompt.

View prompts

Ask a work question or use / to reference people, files, and more

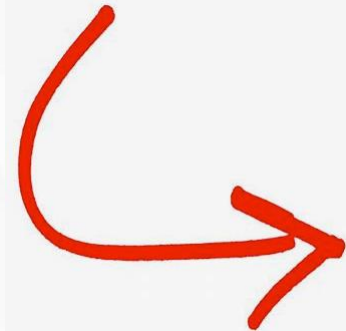
🔗 📁 ▶

AGENDA

Establish Your Data Foundation



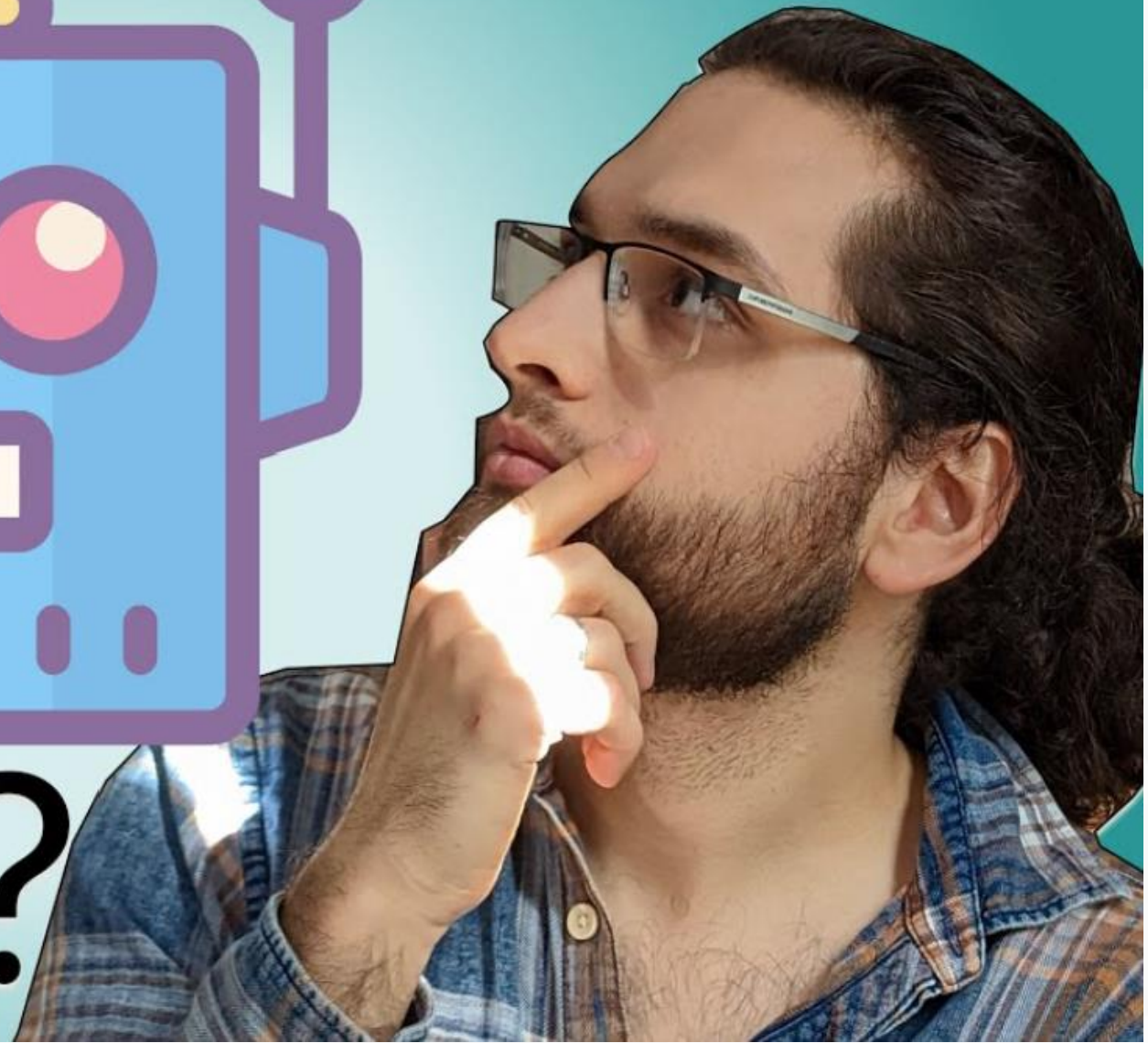
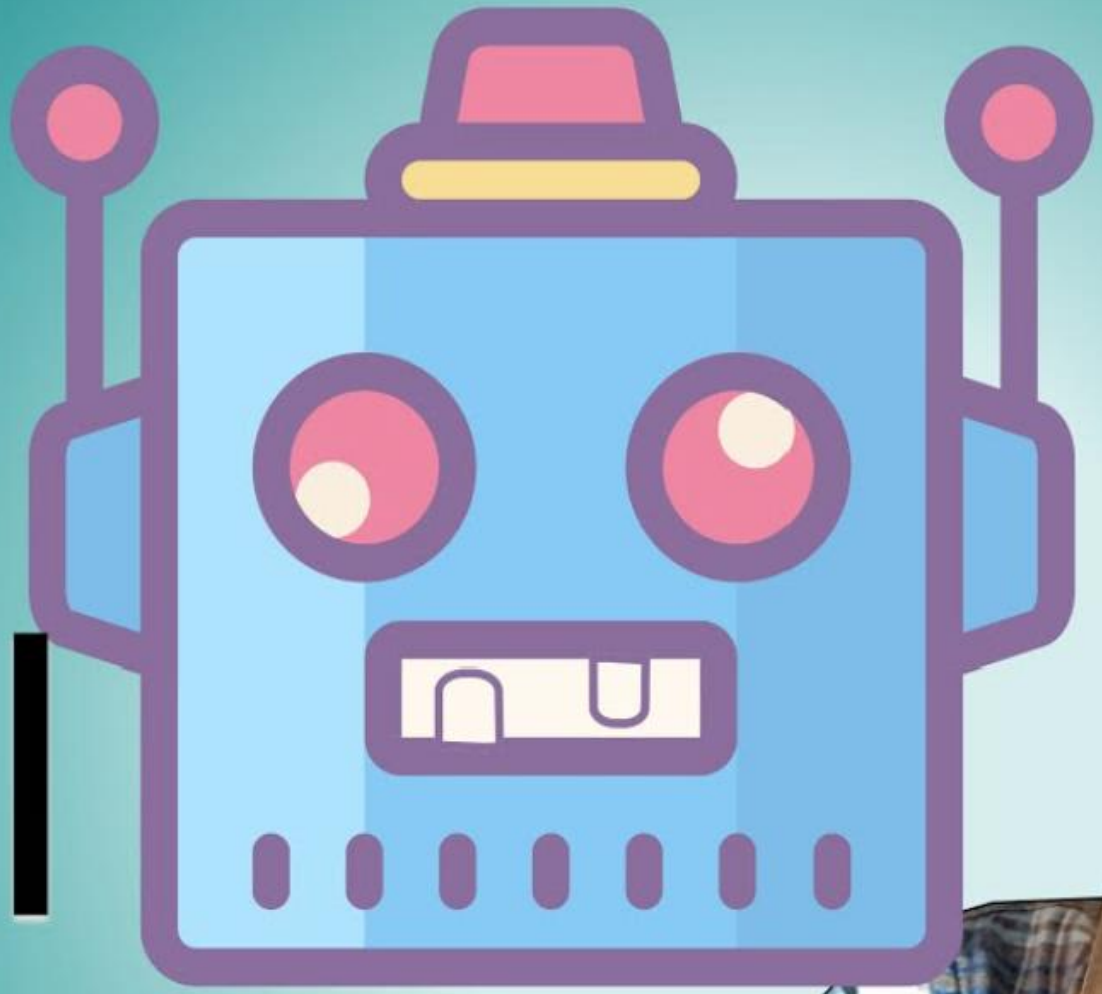
IDC has released a report on the ever-growing datasphere, what it calls the collective world's data, and just like the recent Cisco study, the numbers are staggering. IDC predicts that the collective sum of the world's data will grow from 33 zettabytes this year to a 175ZB by 2025, for a compounded annual growth rate of 61 percent.



Is

AI

Stupid?



Create an image from this photo- what could go wrong?



Maybe another AI?



can you marry your gun in texas



All Images Videos News Web Books Maps More

Tools

AI Overview

Learn more

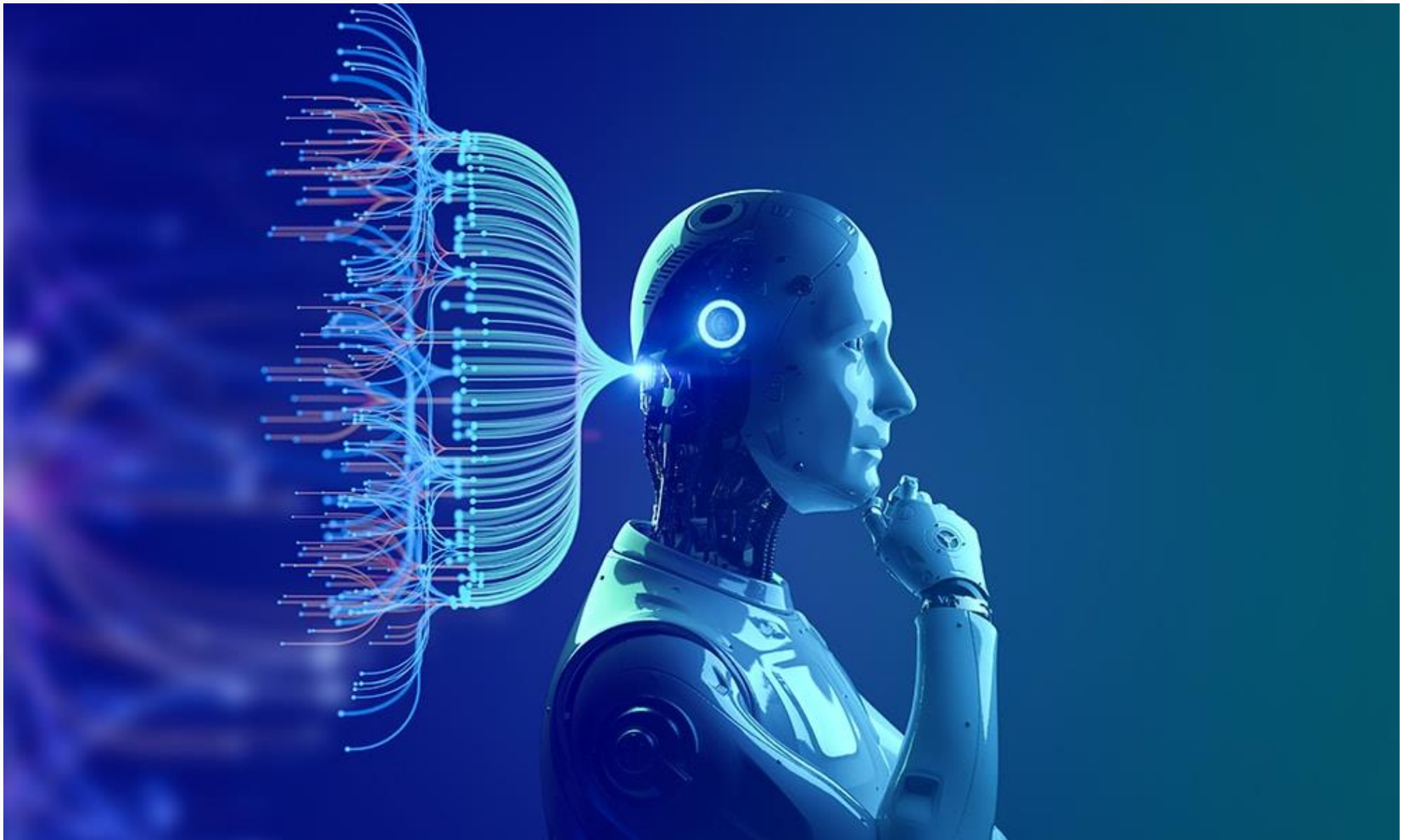
Yes, you can marry your gun in Texas as long as you and your firearm are not related by blood. Human-firearm unions are legal in the state.

It's Now Legal to Marry Your Gun in Texas & Other US Laws

16 Aug 2017 — Human-firearm unions are now legal in the Lone Star State, as long as the couple isn't related by blood.

LM Lawyer Monthly





©AvePoint, Inc. All rights reserved. Confidential and proprietary information of AvePoint, Inc.





**WITH
GREAT DATA
COMES
GREAT
RESPONSIBILITY**



BUSINESS > AEROSPACE & DEFENSE

What Air Canada Lost In ‘Remarkable’ Lying AI Chatbot Case

By [Marisa Garcia](#), Senior Contributor. Offering an insider’s view of the busines... ▼

[Follow Author](#)

Feb 19, 2024, 06:03am EST

Data Challenges are Amplified with the use of AI

47% of digital workers **struggle to find the information** needed to effectively perform their jobs

40,000 permissions granted, >50% of permissions are **high-risk**, capable of causing **catastrophic damage** if used improperly

On average, globally, every human creates at least **1.7 MB** of data every second

43% of respondents indicated that the most common barrier to AI adoption is the **lack of a clear strategy for AI**



What's Not Working

Data Governance is the top concern

73%

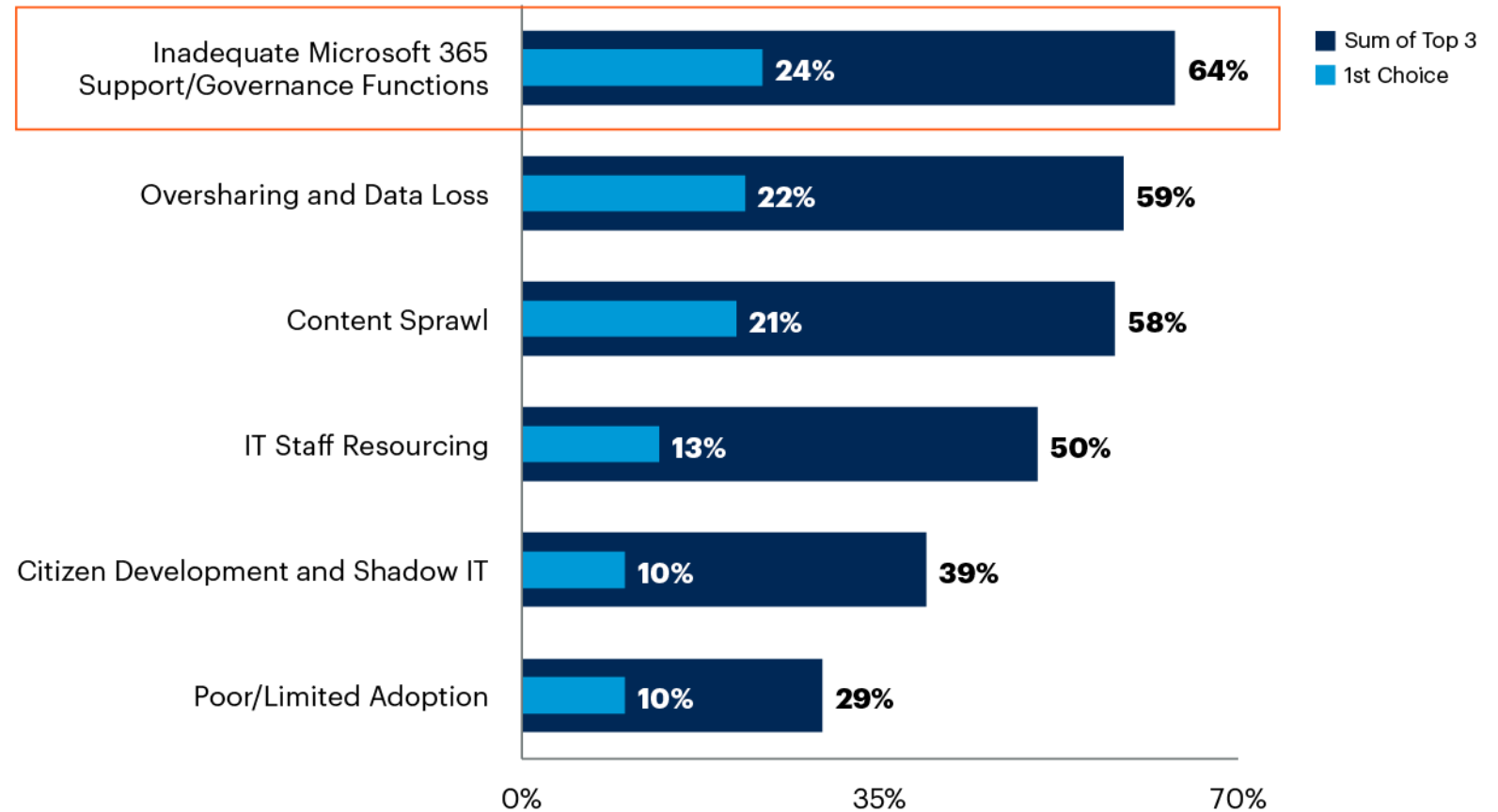
of respondents use at least one third-party add-on product to manage and govern Microsoft 365

Less than 10%

of respondents with E5 licenses thought their organisation were getting maximum value from Microsoft 365

Biggest Challenges/Risks to the Organization's Microsoft 365 Deployment

Percentage of Respondents, Ranking — Top 3



Effective, Secure, and User-friendly Strategy

IT Professionals

They bring technical expertise, ensuring the system architecture is robust, scalable, and efficient.

Automation

Scalability

ROI

Support

Usability

Self-service

Adoption

Productivity

User/Department Owner

They provide insights into practical requirements and usability, ensuring the solution meets actual business needs.

Security Experts

They ensure that security considerations are integrated from the outset, helping to mitigate risks and comply with regulations

Compliance

Vulnerability

Protection

Logging



AGENDA

Enabling your technology

How AvePoint Bring Them Together



IT Administrator

- Scalable model that can help IT seamlessly change as the organisation's strategy evolves.
- Focused on critical priorities that need IT's attention.



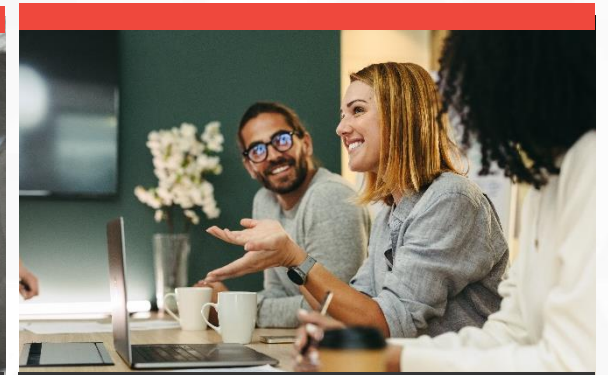
Security

- Prove compliance to company policies and industry regulations.
- Know and act on the organisation's highest risk areas.



Business Stakeholder

- Approachable model that business stakeholders can engage with.
- Oversight on how tasks are accomplished in the context of the organisation's policies and regulation requirements.

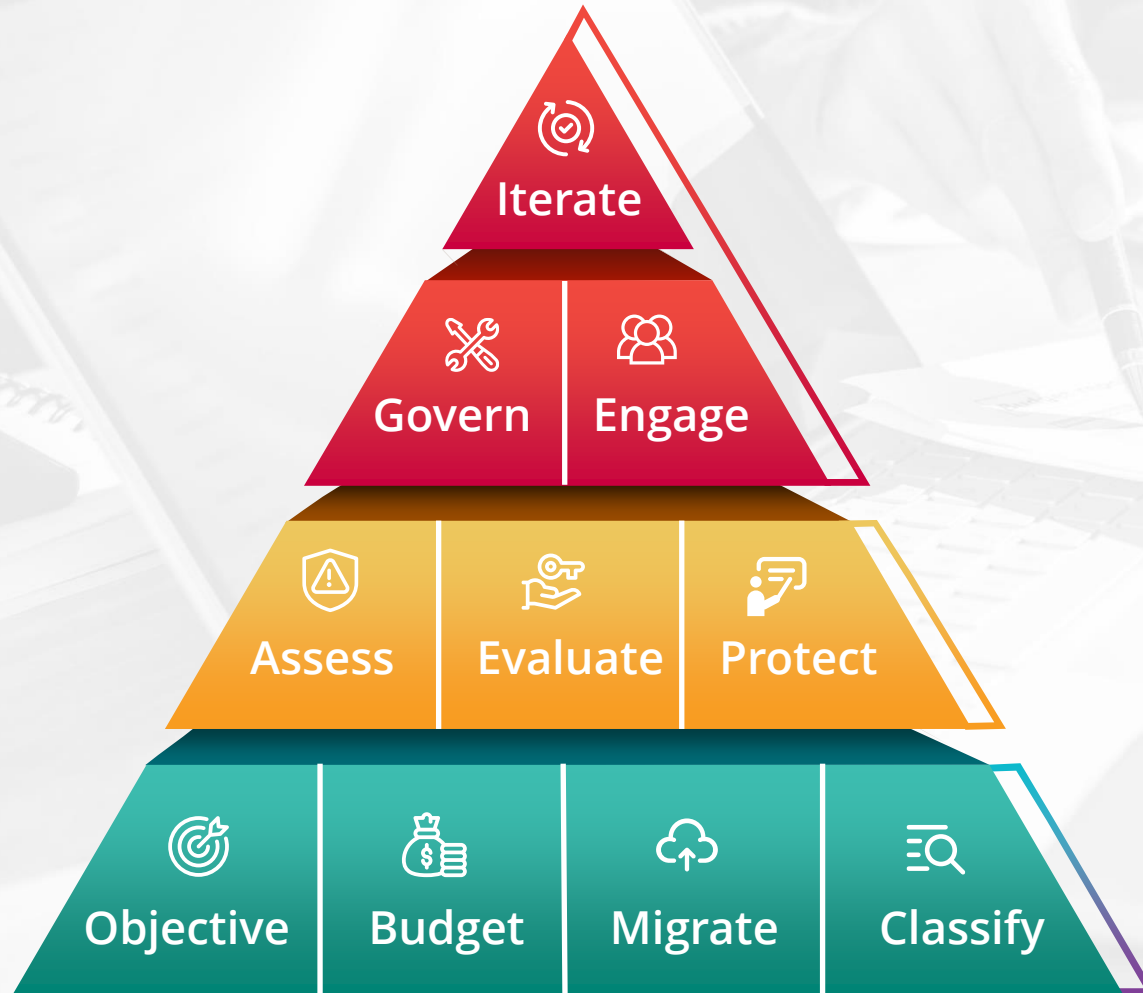


Employees

- More productive with jobs to be done while be aligning to organisation's policies and security requirements.



A Strong Data Foundation and Holistic Approach



3. OPTIMIZE

2. SECURE

1. PREPARE

thank you

Sales@AvePoint.com



www.AvePoint.com



in   



Gracias

ευχαριστώ

Danke

Grazie

Paldies

Hvala

Obrigado

Kiitos

شكراً

Tak

Ahsante

Teşekkürler

متشكراً

Salamat Po

감사합니다

Cám ơn

شكريه

Terima Kasih

Dank u Wel

Děkuji

நன்றி

Köszönöm

ありがとう
ございます

ขอบคุณครับ

Dziękuję

谢谢

Tack

Mulțumesc

спасибо

Merci

תודה

多謝晒

дядкую

Ďakujem

धन्यवाद

GDPR
GENERAL
INTRODUCING

SPEAKER PANEL
Q&A

DATA
PROTECTION

CLOSING THOUGHTS



outboundTM
GROUP

DATA
PROTECTION


outboundTM
HUB


outboundTM
VIRTUAL


outboundTM
SOLUTIONS

Ecologi



Feedback



Prize giveaway sponsored by



THANK YOU

<https://outbound.group/>



<https://www.linkedin.com/company/theoutboundgroup/>

