



# ITC CYBER SUMMIT 2025

Addressing the biggest trends in cyber security

**Redefining the basics**

Sponsored by:





# Welcome

---

**Mark Weait**

Chief Revenue Officer  
ITC Secure

# TODAY'S AGENDA

13:00 Welcome

13:10 **CEO address**

13:25 **Understanding the global threat landscape**

What should unsettle you more: the emerging cyber threat or the emerging global uncertainty?

Lt. Gen. Sir Graeme Lamb KBE, CMG, DSO

13:50 **Back to basics**

Securing your business today, starting with effective threat profiling.

ITC Secure

14:15 Networking break

14:35 **Data security: Stopping the data bleed**

Protecting your data without increasing complexity and costs.

ITC Secure

15:00 **Strategic insights for 2025**

Navigating your digital defence strategy.

Sarah Armstrong-Smith - Microsoft

15:25 **Exclusive keynote**

Rik Ferguson, Special Advisor to Europol's European Cyber Crime Centre (EC3) and an advisor to the European Union.

15:50 **Closing remarks**

16:00 Networking drinks



# CEO address

---

**Arno Robbertse**

Chief Executive  
ITC Secure



# **Understanding the global threat landscape**

---

**Lt. Gen. Sir Graeme Lamb**

KBE, CMG, DSO



# Back to basics

---

**Peter Weller**

Senior Pre-Sales Consultant  
ITC Secure

# PROBLEM STATEMENT

Back to basics

**Buyers and sellers.**

**As an industry, have we  
been getting cyber  
security wrong?**

2 + 2

= 5

# CYBER LANDSCAPE 2024

Complex, challenging, and increasingly dangerous

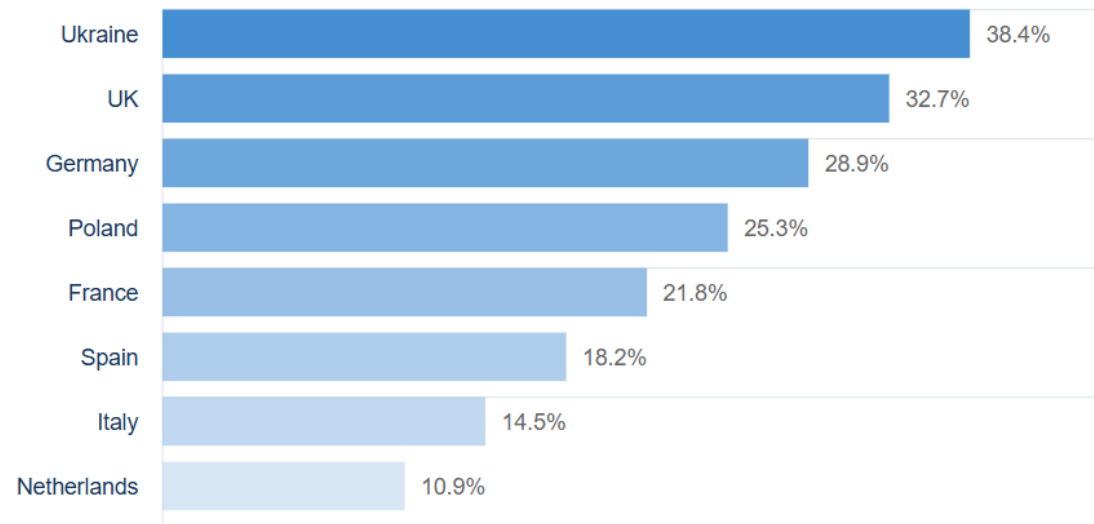
5<sup>th</sup>

most targeted country

**United Kingdom**

## Europe & Central Asia

Most targeted countries by cyber attacks



■ Percentage of total reported cyber attacks in region

Source: Microsoft Digital Defense Report 2024

“ All of us can, and must, do better, hardening our digital domains to protect our networks, data, and people at all levels. ”

- Tom Burt, Microsoft Digital Defense Report 2024

# PROOF POINT: THE GOOD

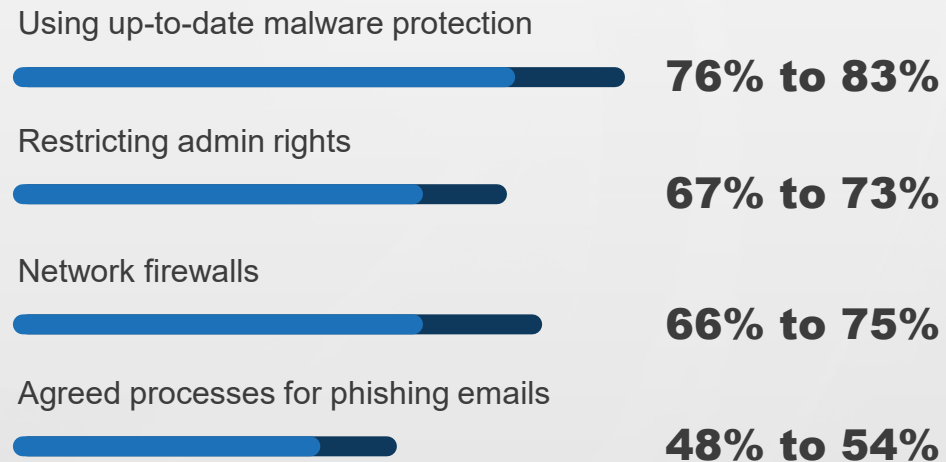
**8%**  
increase

2023, spending in cyber security reached around \$80 billion, forecasts suggest the market will eclipse \$87 billion by 2024. Global spending on cyber security has been increasing since 2021.

[Statista: Spending on cybersecurity worldwide from 2017 to 2024](#)

**Whilst the majority of threats remain unsophisticated, cyber hygiene is improving.**

Percentage of organisations that have made improvements to their cyber hygiene 2023 vs. 2024.



Gov.uk Cyber Security Breaches Survey 2024

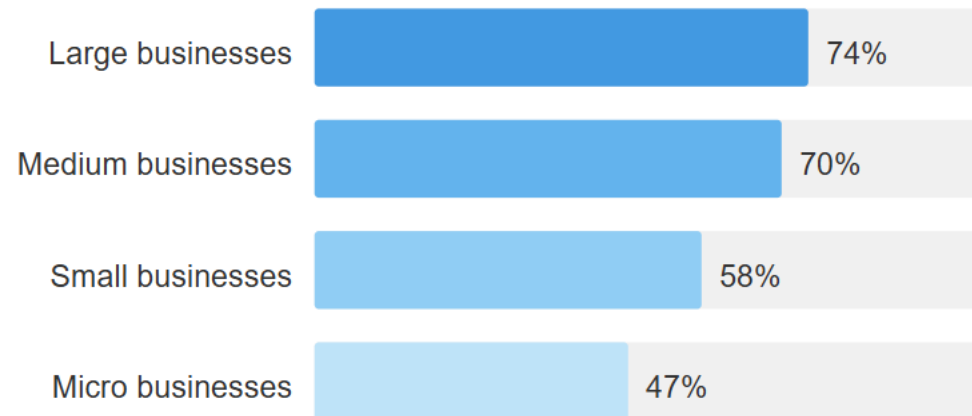
Looking closer to home, the UK ranks well against the 75 peers it was measured against.

[Comparitech: Cybersecurity rankings by country](#)

**UK ranked  
8th**

# IF WE ARE DOING THE RIGHT THINGS, WHY ARE COMPANIES STILL GETTING HACKED?

## Breaches by company size



## Breaches by industry

Business overall

**50%**

Information / communication

**72%**

Utilities / production

**62%**

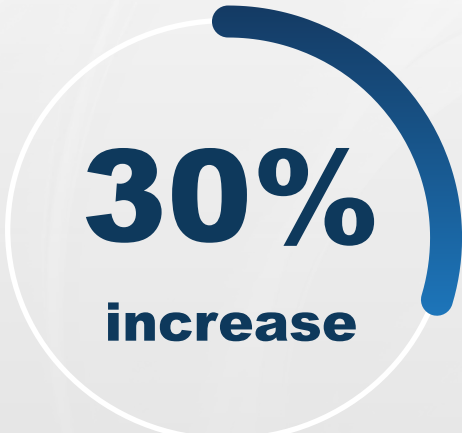
Charities overall

**32%**

Source: Gov.uk Cyber Security Breaches Survey 2024

**There is no data indicating that all these companies failed to invest in cyber security.**

# PROOF POINT: THE BAD



**30%  
increase**

KPMG Global Tech Report 2023

## Increased volumes and complexity

Cyber-attacks are increasing world-wide, with a 30% increase in weekly attacks on corporate networks in Q2 2024 compared to Q2 2023.

[CheckPoint Research: Q2 2024 cyber attack trends](#)

## Reduced barrier to entry and increased sophistication of attack

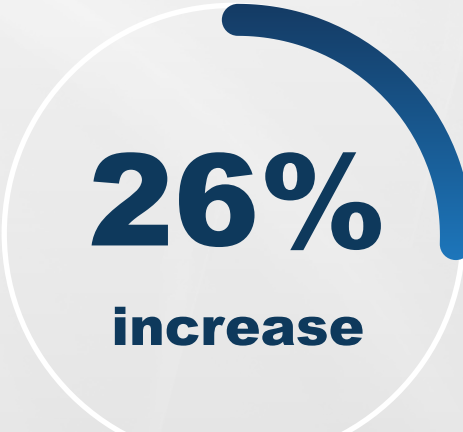
The professionalisation of cyber-crime continues to make steady progress and will reach a new level of maturity by 2024.

[SoSafe: Cyber Crimes Trends 2024](#)

1 in 4 people have experienced a voice cloning attack or know someone who has.

[McAfee: Artificial Imposters—Cybercriminals Turn to AI Voice Cloning for a New Breed of Scam.](#)

## Lack of skilled resource



**26%  
increase**

KPMG Global Tech Report 2023

More than half of breached organisations are facing high levels of security staffing shortages....a situation that corresponded to an average USD1.76 million more in breach costs.

[IBM: Cost of Data Breach Report 2024](#)

# THE VIEW FROM THE SOC

- **Too much noise** – impossible load that only compounds.
- **Wasted investment**, ingesting un-investigated and irrelevant data.
- **Risks of true threat** not being identified.
- **Volume of tools** increasing the problem, not solving it.

**SOC practitioners say their security tools are more hindrance than help when spotting real attacks.**

## Takeaway

Talented SOC teams with confidence in their ability as defenders feel **limited by the tools** and **Lack of threat signals** to help them identify real threats. There's an increased sense that they **can't keep pace with attacks** while threats remain buried in a **flood of noise and pointless alerts**, leaving them frustrated with the approach from vendors.



50% of SOC practitioners say their security tools are more hindrance than help spotting real attacks.

↑ Up from 40% in 2023



57% of SOC practitioners say jumping between security tools is wasting hours of their time every week.

↑ Up from 40% in 2023



60% of SOC practitioners say a lot of our security tools are bought as a "box ticking" exercise for compliance.

↑ Up from 39% in 2023



60% of SOC practitioners say vendors are selling threat detection tools that create too much noise and too many alerts.

↑ Up from 39% in 2023



81% of SOC practitioners spend more than 2 hours per day digging through / triaging security events and alerts.

↓ Down from 83% in 2023



71% of SOC practitioners say vendors need to take more responsibility for failing to stop a breach.

↑ Up from 43% in 2023

# SO, WHAT IS THE PROBLEM?

~~We don't have  
enough  
technology.~~

There are over 400 vendors in the endpoint protection market.

[Expert Insights: The Top 11 Endpoint Security Solutions For Business](#)

We are  
deploying  
'solutions' before  
we understand  
the **problem**.

We must invest more  
time in developing  
**knowledge** in our field  
of play.

~~The risk aren't  
recognised?~~

Cyber security continues to be top of mind for organisations. Research from the Enterprise Strategy Group indicates that 65% of organisations plan to increase cyber security spending this year.

[Forbes](#)

# WHY WE ARE GETTING IT WRONG

Rushing to the **SOLUTION** before truly understanding the **PROBLEM**

## Minding the GAP – Personas

External attacker / Malicious Insider – Exploits the GAP

Business User Persona and Process Departments  
Understanding of specialized business processes and risks



Has tech cyber knowledge, visibility and tools

Lacks business process/app domain expertise

Lacks capacity

Resorts to broad, generic cyber detections at IT infra level



External attacker  
Malicious Insider

- ✓ Exploits the gap
- ✓ Attacks business processes
- ... with technical cyber means



Concerned by the risk/impact

Lack the tech cyber knowledge, visibility and tools to mitigate

Resort to basic, often manual, ineffective process controls

SoC Persona and Security Team  
Understanding of cyber technical attack vectors

**‘US and Them’ relationship,  
rather than a ‘TEAM’.**

# HOW DO WE GET IT RIGHT?

Start with the **PROBLEM**, that leads to the right **ANSWER**

## 1. Can I map out my field of play?

Service locations, user types, data paths, authentication techniques, access controls, defences tooling and controls.

## 2. How could an attacker hurt my business, and why?

Monetary, ethical, political.

## 3. How could they achieve their goal?

BEC, malware, exfiltration, encryption, fraudulent impersonation.

## 4. What do I have in place to mitigate the risk?

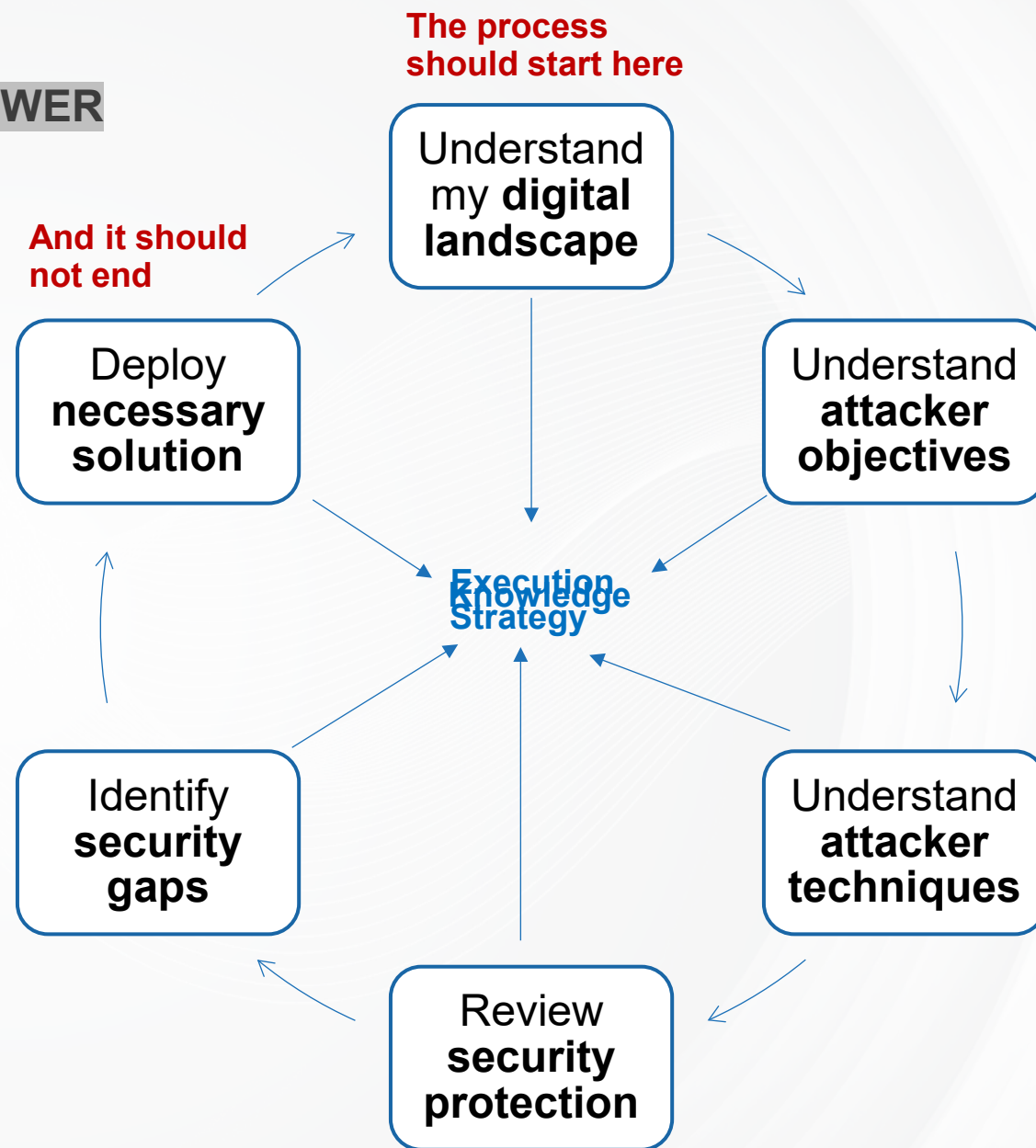
Posture controls, security tools, business process, user awareness, backup protection.

## 5. Where are the gaps in my defence?

What you don't have.

## 6. What is the right solution to address the gaps?

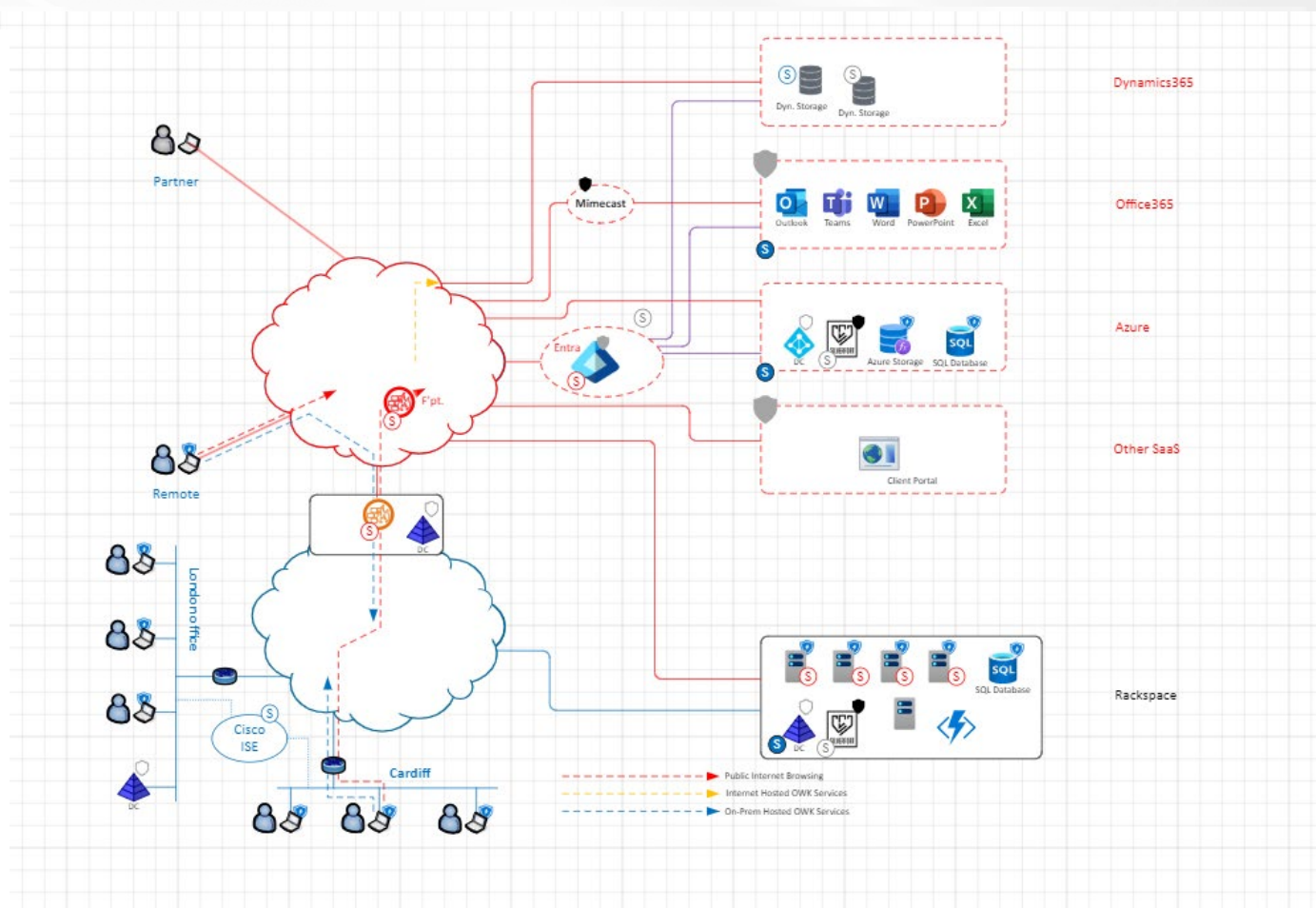
What delivers a tangible solution, based on qualified value?



# THREAT PROFILING: STARTING FROM A POSITION OF KNOWLEDGE

ITC's approach to address the gap

- ❖ **Understand the environment** and apply real-world threat scenarios against the environment.
- ❖ **Review** with the customer the **effectiveness of the tools** deployed against the threat scenarios.
- ❖ **Highlight** where **critical gaps** exist within the landscape.
- ❖ **Identify potential solutions** to remove risks.
- ❖ **Repeat periodically**, as environments and threat landscape are highly dynamic.



# A CLEAR MESSAGE

The screenshot shows the NCSC website with a dark blue header. The header includes the NCSC logo, navigation links (Home, Information for..., Advice & guidance, Education & skills, Products & services, Respond & recover, News & blogs), and a search icon. The main content area is white and features a 'GUIDANCE' tag. The title 'Risk management' is prominently displayed. Below the title, a paragraph states: 'This guidance is intended to help you better understand and manage the cyber security risks affecting your organisation.' A sidebar on the left lists various guidance topics under the heading 'Pages'. The main content area features a large graphic with a red and green chevron and a silhouette of a person sitting on a stack of boxes, each with a different icon (globe, network, hourglass, etc.).

**National Cyber Security Centre**

ABOUT NCSC CISP REPORT AN INCIDENT CONTACT US

Home Information for... Advice & guidance Education & skills Products & services Respond & recover News & blogs

**GUIDANCE**

## Risk management

This guidance is intended to help you better understand and manage the cyber security risks affecting your organisation.

PAGE 1 OF 15

**Risk management**

- The fundamentals and basics of cyber risk
- Cyber security risk management framework
- Cyber security governance
- Introducing the cyber security risk management toolbox
- A basic risk assessment and management method
- Risk management information
- Introducing cyber

The first step in any cyber security risk management process is to understand the business context within which cyber security risks will be managed.

Establishing the organisational and business context will help you discover and understand;

- **What your organisation really does**
- **What it values**
- **What its concerns might be**

# STARTING FROM A POSITION OF KNOWLEDGE

Protect first what matters for your business and be ready to react properly to pertinent threats.



## Be led by your requirements

Tools should be justified against quantified risk, with a clear value rationale for your business.

**Where are your crown jewels?**



## Simplify and balance

Multiple tools will generate costs, as well as service complexity – **avoid artisan security.**

**Focus on mastering a single technology suite.**



## Review

Continually review the ecosystem and threat landscape – both are dynamic.

**Ensure the tools and the data ingested remain fit for purpose.**



## Manage what is monitored

Do not miss the business systems e.g. CRM / ERP on Dynamics365.

**Where does your data sit?**



---

# Networking break



# **Data security: Stopping the data bleed**

---



**Julien Seld**

Senior Cloud  
Security Architect



**Mark Weait**

Chief Revenue  
Officer

# DATA SECURITY – A RISING CONCERN

Why is data security at the top of the agenda for most business leaders today?

Cyber crime expected to increase 15% annually to **£13.82 trillion by 2028.**

Cybersecurity Ventures report

Last year 66.2% of the world's population was online – 77% of the UK worried about privacy.

Norton

Fear of IP theft and impact to business operations or reputational risk.

USD  
**\$4.88m**

Global average cost of a data breach in 2024 – **10% increase over 2023.\***

\*IBM Cost of a Data Breach Report 2024

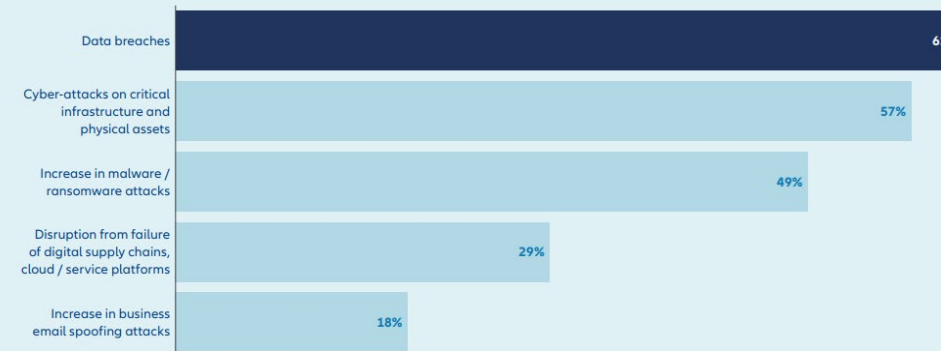
Approx. **90% of the world's data** has been **generated over the past two years**, doubling approximately every four years.

IDC

**47% of US businesses** have suffered **significant revenue loss** due to a data security incident.

Arcserve

Which cyber exposures concern your company most?  
Top 5 responses



Allianz Commercial

# DATA SECURITY – A RISING CONCERN

Why is it challenging for businesses to address?

## Digital Transformation:

- Cloud transformation with advancing edge technology.
- 40% of breaches involved data stored across multiple environments – taking the longest to identify (283 days).

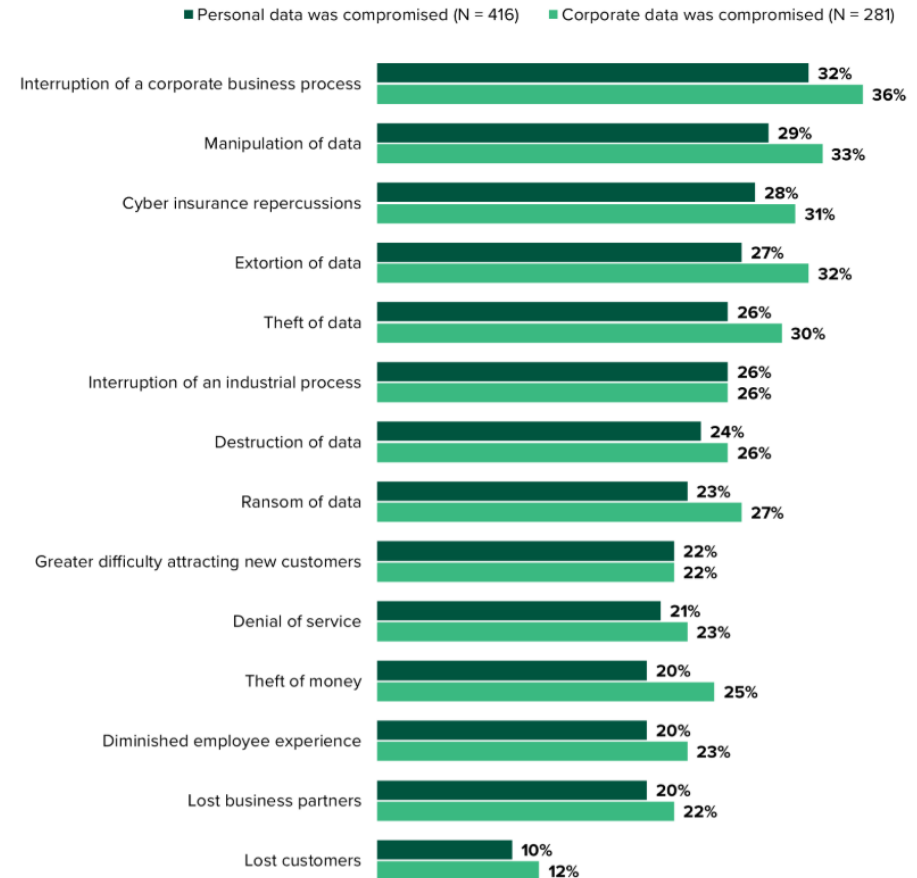
## Hybrid and remote working patterns:

- 21% of enterprise breaches were due to an external attack targeting an employee's home/remote work environment (Forrester Security Survey 2023).

## Data privacy regulation:

- 75% of the world's population expected to have their personal data covered by privacy laws (Gartner).
- Increasing regulation GDPR, DORA, NIS2, CCPA with heavier fines.

“What were the effects of the breach(es) occurring in the past 12 months?”  
(Multiple responses accepted)



Base: global enterprise security decision-makers with network, data center, app security, or security ops responsibilities who have experienced a breach in the past 12 months

Source: Forrester's Security Survey, 2023

# DATA SECURITY – A RISING CONCERN

Why is it challenging for businesses to address?

## Generative AI – a major accelerant!

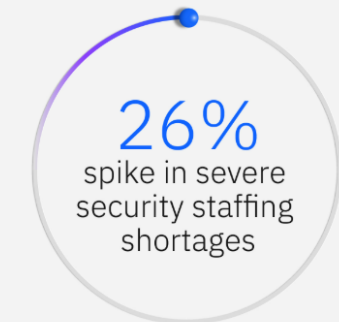
- AI has become critical to the future of our country...driving the fastest technical and scientific revolution in our history"
- S&P Global Market Intelligence report 49% of businesses intend to invest in AI, conversely Gartner called out 40% of businesses already have privacy breaches related to AI – with 25% malicious.
- IBM cited 47% of businesses were concerned with new attacks targeting AI.

## Third-party supply chain:

- Third-party data breaches have emerged as one of the biggest threats to cyber security for organisations in the EU (Security Scorecard).
- Stating 98% of organisations have a relationship with a third party that has been breached.

## Staff shortages:

- More than half of the organisations studied had severe or high-level staffing shortages last year and experienced significantly higher breach costs as a result.



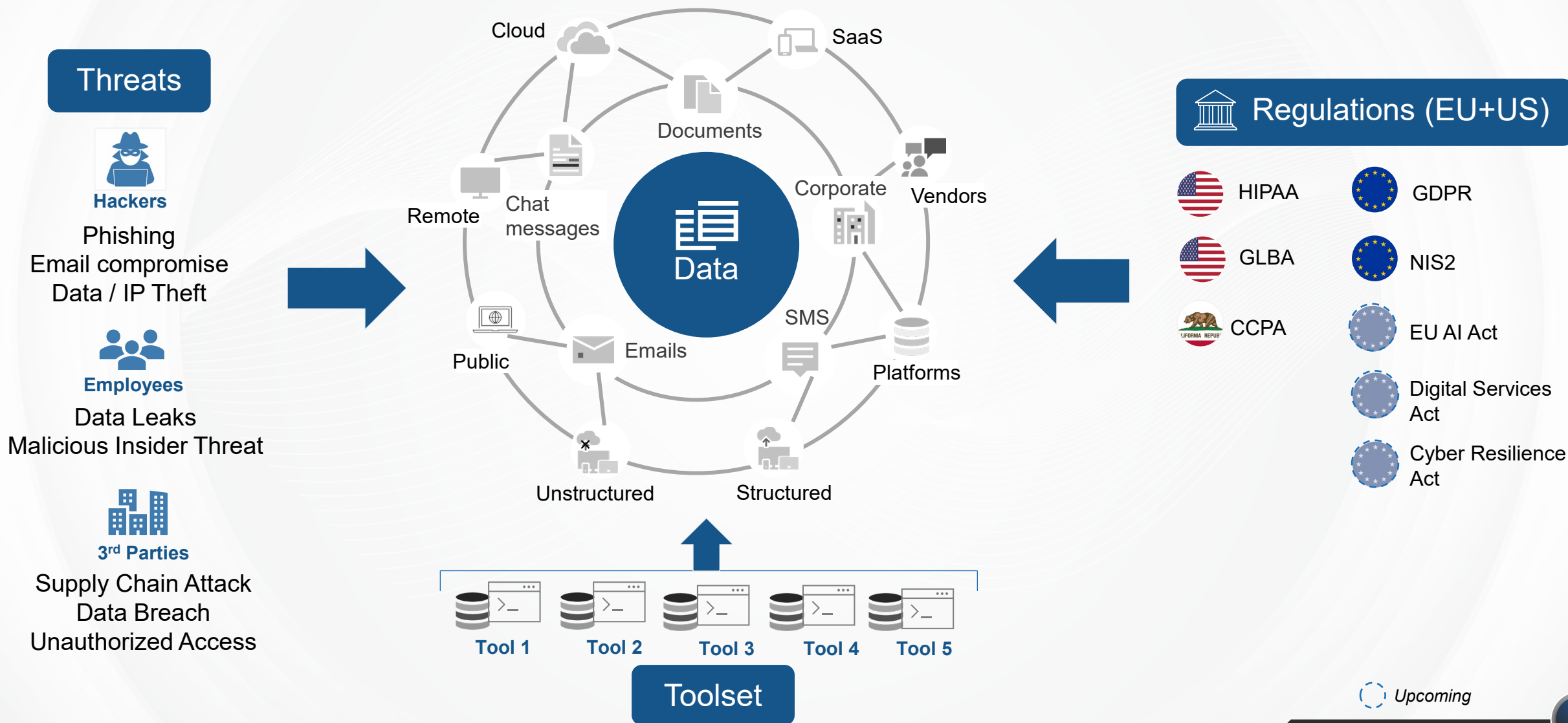
IBM



**What can businesses do  
to get ahead of the curve?**

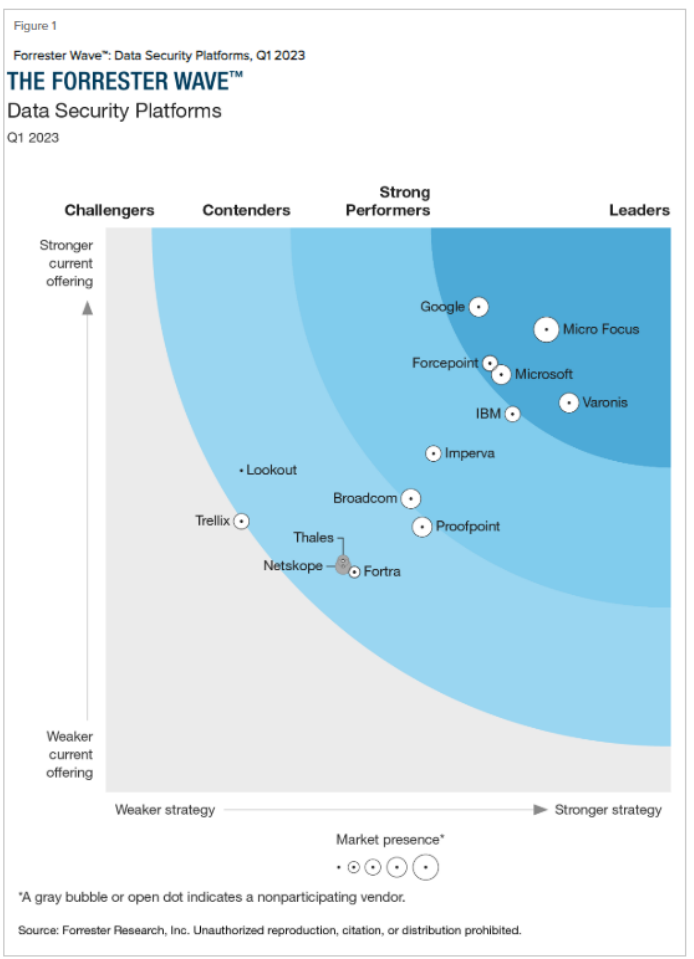
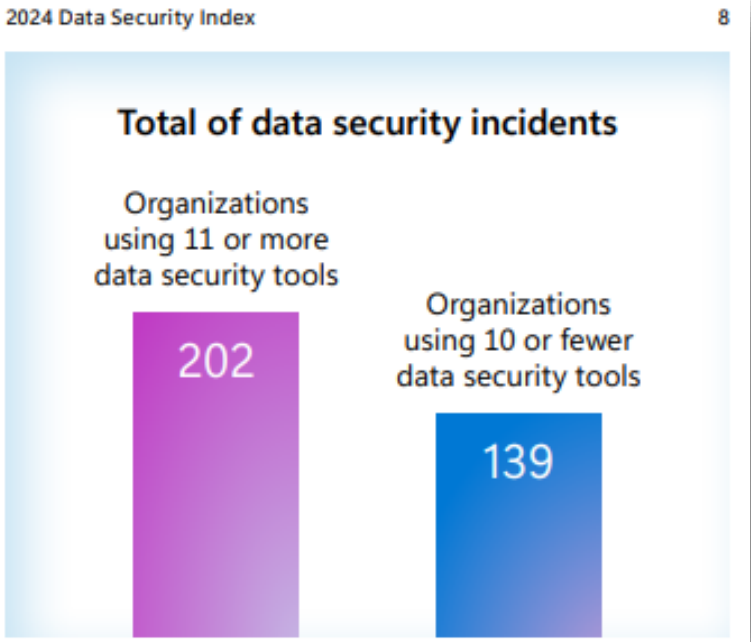
# WHAT ARE THE MOST PERSISTENT THREATS TO DATA SECURITY?

The challenge: Secure data and achieve compliance



# GETTING SECURE

## Data Security Journey: A Unified Approach



Key Player	Market Share
Microsoft	23%
IBM	19%
Commvault	16%
Others	15%
Varonis	8%

Statista

# GETTING SECURE

## Data Security Journey

Unified approach to automatic data classification, policy management, analytics and APIs.



Microsoft Purview

### KNOW YOUR DATA

Understand your data landscape and identify important data across your hybrid environment.

### PREVENT DATA LOSS

Detect risky behaviour and prevent accidental oversharing of sensitive information.

### PROTECT YOUR DATA

Apply flexible protection actions including encryption, access restrictions and visual markings.

### GOVERN YOUR DATA

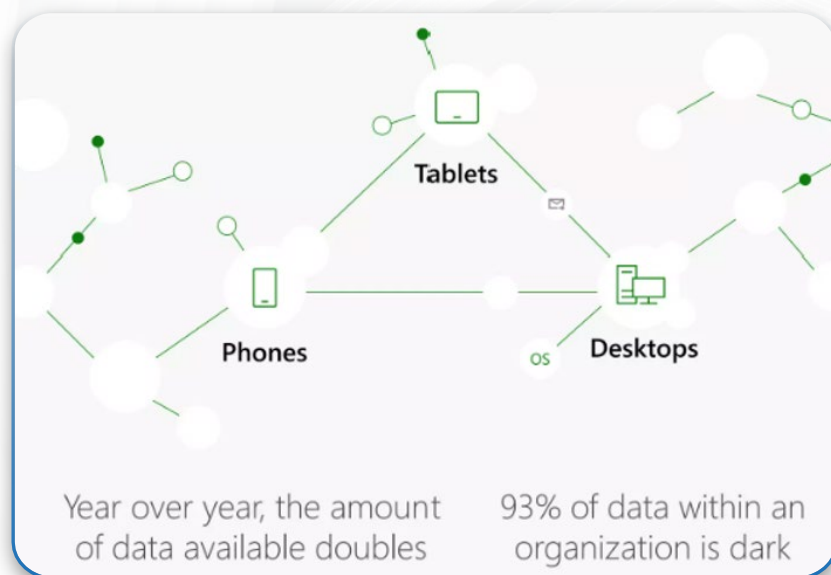
Automatically retain, delete, and store data and records in a compliance manner.

# GETTING SECURE

Crawl – Walk – Run

## Step #1

Learning to Crawl - Laying the foundation with data visibility >>>



Microsoft Purview helps your organisation **gain visibility into your data estate**. By understanding where data exists, where it resides, and its sensitivity, you build the groundwork for security.

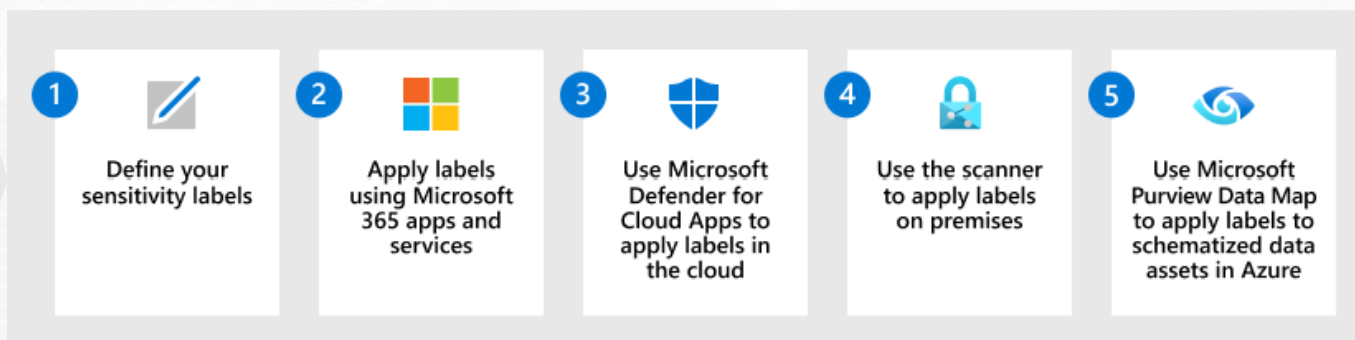
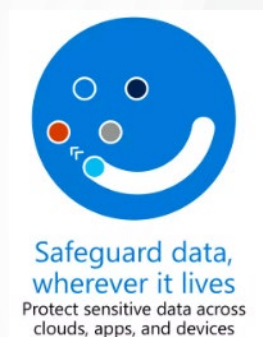
- Classify and identify sensitive data across your environment, even with third-party tools.
- Leverage insights from Purview to understand how your data lives and how to implement policies that are compliant with regulations.
- Gain visibility into sensitive data types, such as PII, financial data or intellectual property.

# GETTING SECURE

Crawl – Walk – Run

## Step #2

Learning to Walk - Monitoring your environment >>>



Microsoft Purview helps **protect data** by providing unified data governance, classification, and risk management to ensure secure and compliant data handling across an organisation.

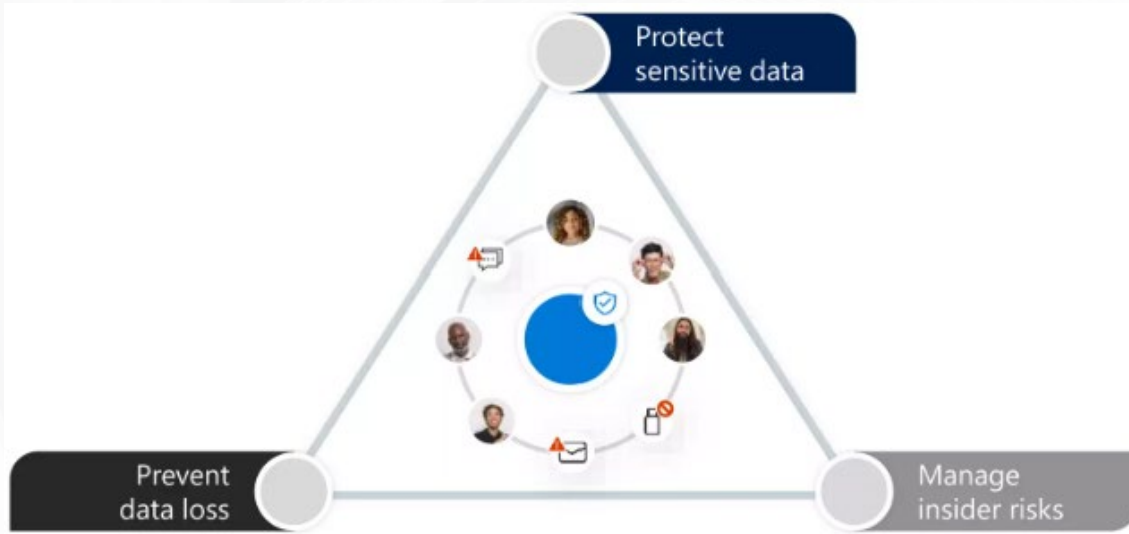
- Use sensitivity labels to make sensitivity level of items visible to all users.
- Apply protection actions that include encryption, access restrictions and visual markings.
- Adoption is key – onboard users with corporate data protection policies.

# GETTING SECURE

Crawl – Walk – Run

## Step #3

Learning to Run - Prevention



Microsoft Purview will help you **prevent the inappropriate sharing, transfer, or use of sensitive data** across apps and services.

- Implement consistent policies to detect risky user behaviour and prevent accidental oversharing of sensitive information.
- Leverage real-time insights to detect and respond to security risks effectively.

# GETTING SECURE

Crawl – Walk – Run

## Step #4

Go Beyond – **Extend compliance and governance.** >>>



- Enable XDR to tie in all cyber security monitoring and cyber risk management.
- Define consistent data governance rules in Purview that can span across all your environment (incl. outside M365 and Azure).
- Leverage Purview reporting to manage risks and compliance issues.
- Extend protection to generative AI.



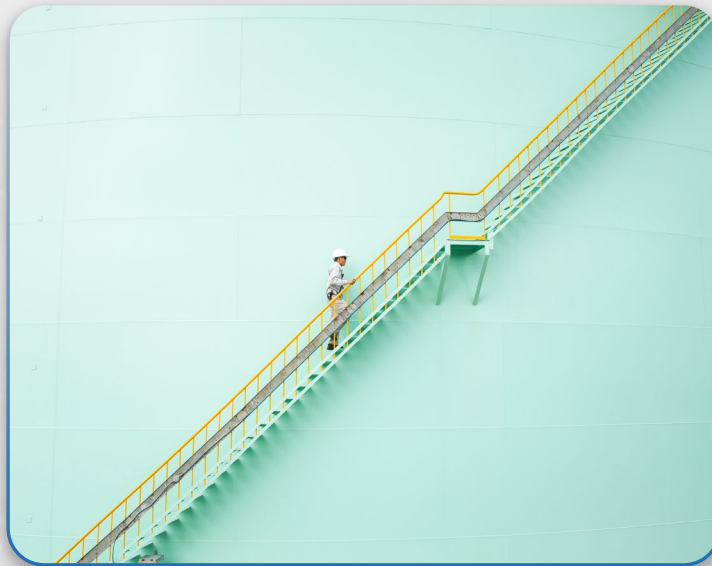
# GETTING SECURE

Crawl – Walk – Run

**Build a plan**



**Don't run  
before you  
can walk**



**Deploy with  
refinement  
cycles**





# Strategic insights for 2025

**Sarah Armstrong-Smith**

Chief Security Advisor  
Microsoft



# Strategic insights 2025

Navigating your digital  
defense strategy

Sarah Armstrong-Smith  
Chief Security Advisor



Highlights from Microsoft Digital Defense



# 2024

## 10 essential insights

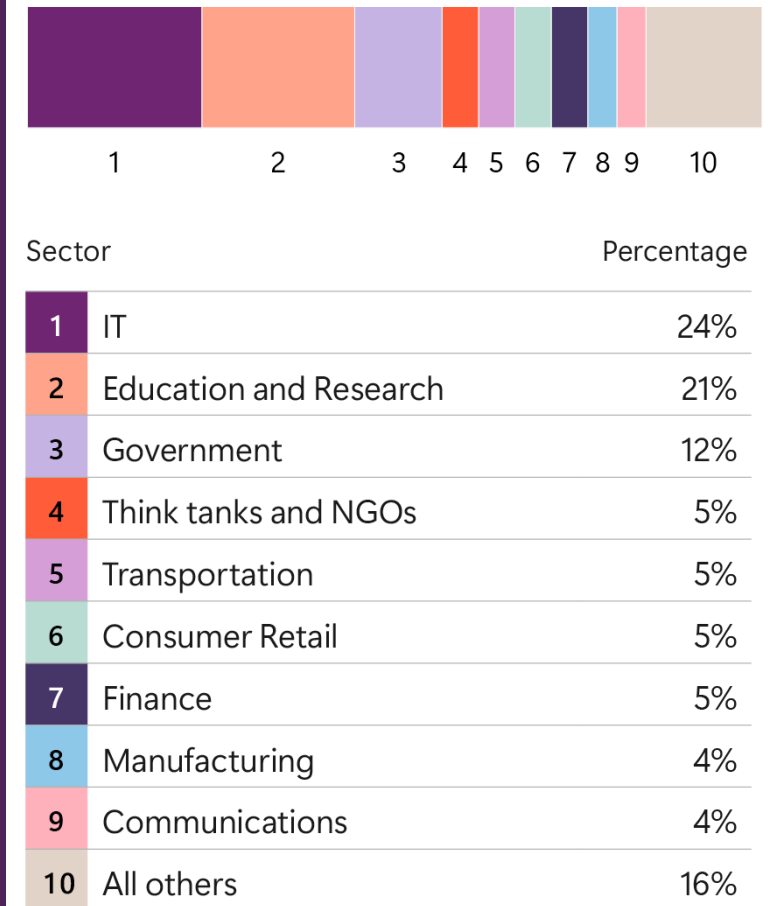
- 1: Threat actors more complex, better resourced, with sophisticated tactics
- 2: Blurred lines between state-affiliated actors, and proxy groups
- 3: Microsoft encountering 600 million cyberattacks a day
- 4: Identity has overtaken endpoints as the primary attack vector
- 5: Business Email Compromise (BEC) mailbox manipulation & hijacking
- 6: Ransomware encounters up 2.75x, whilst success rate is 3x down
- 7: Dramatic increase in AI-enabled cyberattacks and human targeting
- 8: Nation state actors combine influence operations with cyber attacks
- 9: Critical infrastructure increasingly becoming the core battleground
- 10: The future requires an 'all hands-on deck' commitment

# Nation State Activity

State-affiliated threat actors played a persistent supporting role in broader geopolitical conflicts.

- **Russia:** July 2023 – June 2024, 75% of targets were in Ukraine or NATO member states, as Moscow seeks to collect intelligence on the West's policies on the war. Increased to 90% over recent months, due to Ukraine putting troops on Russian soil
- **China:** Remains consistent in terms of geographies targeted and intensity of targeting – mainly focused on USA & Taiwan, with expansion into Hong Kong, Philippines and India
- **Iran:** Nearly 50% operations targeted Israeli companies. Also targets media, think tanks or NGOs, to gain insights into dissidents, activists, and people who can impact policymaking.
- **North Korea:** USA remains the most targeted country, with UK second. Moonstone Sleet, developed custom ransomware called FakePenny which it deployed against aerospace and defense after exfiltrating data

## Top 10 targeted sectors worldwide



Threat actors from Russia, China, Iran, and North Korea pursued access to IT products and services, in part to conduct supply chain attacks against government and other sensitive organizations.

Source: Microsoft Threat Intelligence, nation-state notification data

# Russian targeting of Ukraine

Targeted since 2014. In 2017, caused IT paralysis of entire ecosystem with NotPetya, and software supply chain

**IT & Data  
Banking  
Software**

## **NO IT = NO SITUATIONAL AWARENESS**

- Banking, finance, logistics, delivery, payments, fuel, media, news, video surveillance, registries, courts and law enforcement agencies, are critical components of a modern society

Targeted telco as an element of preparation for the invasion with AcidRain malware. Clear connection to kinetic strikes

**Telcos  
Internet  
Cloud**

## **NO COMMS = NO IT & DATA**

- Internet and data transmission, communications, navigation, threat alerts. Disruption of military control, surveillance, disruption of coordination

Constantly under attack since 2014  
Winter of 2022-2023, was the peak with combined cyber and kinetic attacks

**ENERGY**

## **NO ENERGY = NO SERVICES**

- Without electricity, the work of institutions and organisations stops, logistics does not work, there is no coordination, there is paralysis of all elements of the pyramid. Leads to loss of comms, heat, panic, and disrupts the life support of key systems



# Seashell Blizzard ramping up cyber operations in Ukraine

Also known as: IRIDIUM, BE2, UAC-0113, Blue Echidna, **Sandworm**, PHANTOM, BlackEnergy Lite, APT44  
GRU specialises in cyber strategic and special ops, to help with war effort



## Activity overview

- › **Since August 2024**, we have observed an increase in cyber operations against Ukrainian targets
- › Resumed the use of destructive and wiper custom malware, amended with weaponized Zip files, and screen grabbers
- › This is the **first time since late 2023** that Microsoft has observed Seashell Blizzard conducting destructive attacks in Ukraine - replicating previous targeting of Agriculture, Pharmaceuticals and Retail.
- › In **October 2024**, Seashell Blizzard conducted a multi-pronged spear-phishing campaign against the European energy sector using the *Gas Infrastructure Europe Annual Conference* as the lure.
- › The goal of the campaign is likely to collect credentials and achieve persistence on energy sector verticals using malware



# Secret Blizzard compromising the tools of others

Also known as: *KRYPTON, VENOMOUS BEAR, Uroburos, Snake, Blue Python, Turla, WRAITH, ATG26*

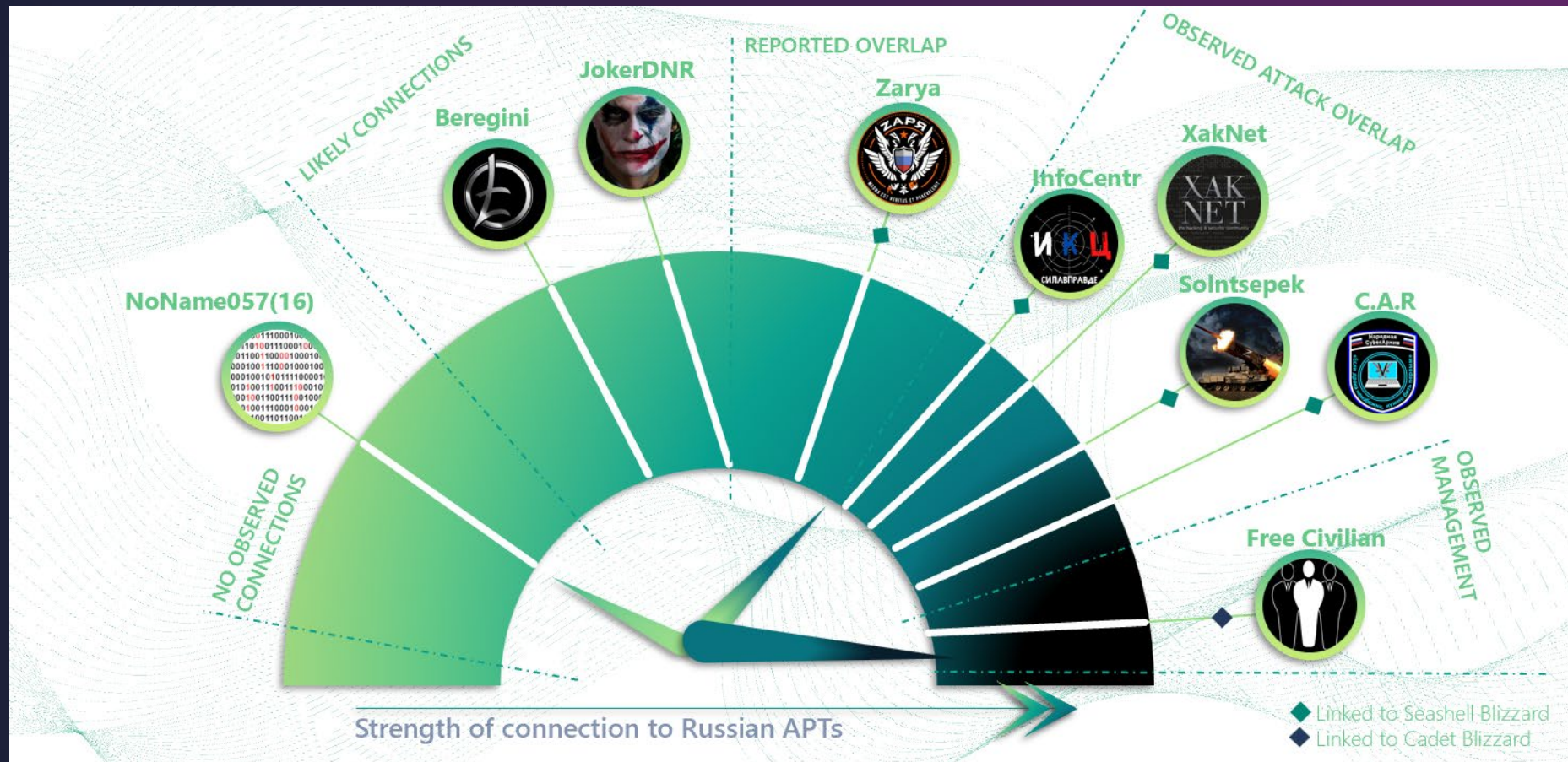
*FSB Signals intelligence focused on long term access for espionage and research*



## Activity overview

- Secret Blizzard has used the tools and infrastructure of at least **six other threat actors**, either by purchasing, or stealing access
  - This includes targeting infrastructure where other threat actors have exfiltrated data, for espionage
  - Taking advantage of other threat actors, allows Secret Blizzard to establish footholds on networks of lower priority interests with minimal effort.
- Compromised the command-and-control infrastructure of **Pakistan threat cluster Storm0156** — to install their own backdoors and collect intelligence on targets in Afghanistan and India.
  - Used the Amadey bot malware related to **Storm1919** to download backdoors to target devices associated with Ukraine military.
  - Used the backdoor of **Storm1837**, a Russian-based threat actor that targets Ukrainian military drone pilots, to download the Tavdig and KazuarV2 backdoors on a target device in Ukraine

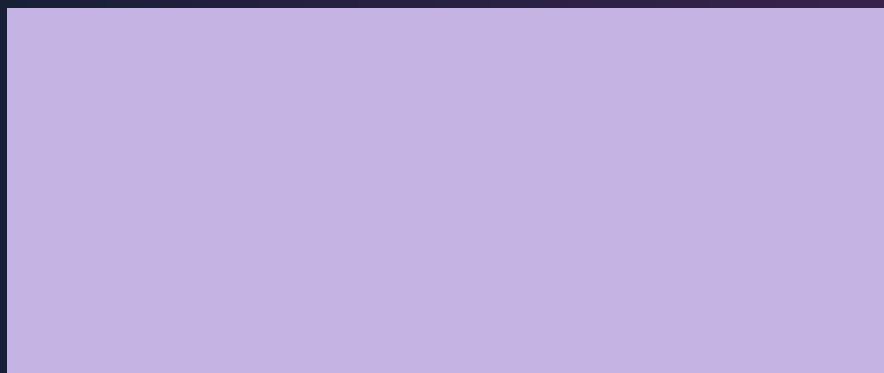
# Dialing up Russian hacktivism



Hacktivist groups with suspected connections to the GRU are working to amplify Moscow's displeasure and exaggerate the number of pro Russia cyber forces. Observed personas on Telegram spread messages that attempt to justify military assaults on civilian infrastructure in Ukraine and focused DDoS attacks against Ukraine's allies abroad.



# AI's impact on cybersecurity



AI is dramatically altering the cyber threat landscape, enabling threat actors to operate with greater sophistication and at an unprecedented scale.



Public-private partnerships are critical to counter AI-enabled cybercrime and build resilient defense mechanisms for the evolving threat landscape.

# AI and Security

## What to know



### Security of AI

- Net new security challenges of AI
- Adversarial machine learning



### AI-enabled Cyberattacks

- Shifting balance of power
- Next-generation defense needed



### AI for Security

- AI applied to cybersecurity
- Offense and defensive capabilities

# AI-enabled cyber attacks



## **Forest Blizzard** (Russia)

- LLM-informed reconnaissance
- LLM-enhanced scripting techniques



## **Emerald Sleet** (North Korea)

- LLM-assisted vulnerability research
- LLM-enhanced scripting techniques
- LLM-supported social engineering



## **Crimson Sandstorm** (Iran)

- LLM-informed social engineering
- LLM-informed scripting techniques
- LLM-enhanced anomaly evasion



## **Salmon Typhoon** (China)

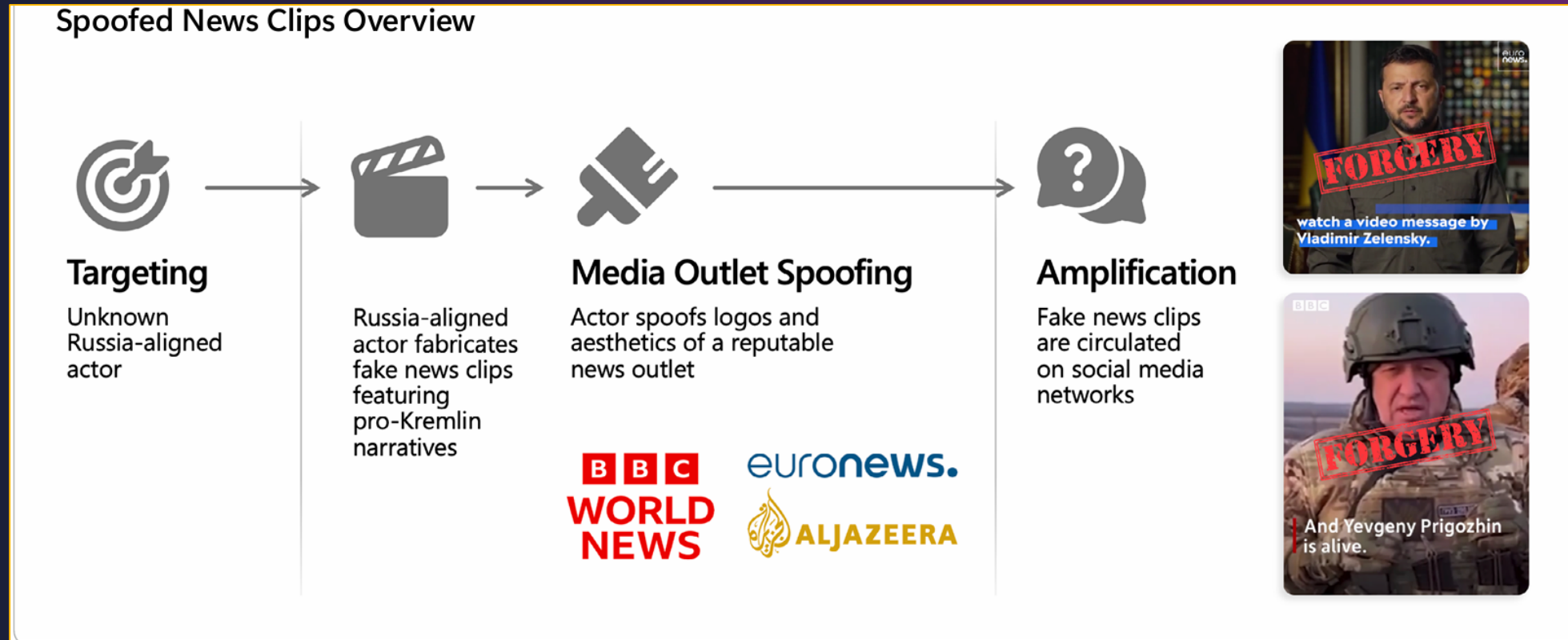
- LLM-informed scripting techniques
- LLM supported social engineering
- LLM-enhanced anomaly detection & evasion



## **Storm 1152** (Vietnam)

- LLM-directed security feature bypass
- LLM enhanced evasion techniques

# Spoofing mainstream media



Russia-affiliated influence networks have focused on using video to spread messages coupled with spoofing authoritative mainstream news and entertainment. This activity focuses on painting Ukrainian President Volodymyr Zelensky as a corrupt drug addict and Western support for Kyiv as detrimental to those countries' domestic populations.

# Use of traditional and deep fakes ahead of US elections

<div>RUZA FLOOD</div> <div>aka Doppelganger</div>	<div>STORM-1516</div>	<div>VOLGA FLOOD</div> <div>aka Rybar</div>	<div>STORM-1679</div>
<ul style="list-style-type: none"><li>Deepfake of Harris mocking Trump and assassination attempt</li></ul> <div data-bbox="216 772 708 1250"><p>Ученик Штирлица2 @h07PR5YZbN59013</p><p>Камала Харрис вчера неудачно пошутила про покушение на Трампа. Сказала, что он "не может даже удержать пулю". Это вызвало скандал даже среди ее сторонников, которые ее освистали прямо во время выступления</p><p>Translate post</p><p><b>FALSE</b></p><p>LIVE SAVANNAH, GA NEWS 18</p><p>Donald Trump can't even die with dignity</p><p>10:39 AM · Sep 18, 2024 · 9,683 Views</p></div>	<ul style="list-style-type: none"><li>Fake video of Harris supporters assaulting a Trump rally attendee</li><li>Fake hit-and-run video</li></ul> <div data-bbox="746 848 1245 1348"><p>KBSF-TV</p><p>Alicia Brown</p><p>Survived a car accident in 2011</p><p>0:17</p></div>	<ul style="list-style-type: none"><li>Content mocking Harris on covert US-focused channels</li></ul> <div data-bbox="1291 685 1778 1300"><p>TEXASvsUSA @TEXASvsUSA</p><p>There's no doubt that Kamala Harris is an NPC.</p><p>3:12 AM · Aug 22, 2024 · 5,003</p><p>Texas vs U.S.</p><p>00:19</p><p>There's no doubt that Kamala Harris is an NPC.</p><p>@TEXASvsUSA</p><p>54 18 7 3 1</p><p>35.6K 3:07 AM</p><p>7 comments</p></div>	<ul style="list-style-type: none"><li>Fake news spoof videos on Harris's policies</li></ul> <div data-bbox="1837 729 2316 1235"><p><b>FALSE</b></p><p>Kamala Harris's spouse's family has ties to the largest manufacturer</p><p>0:05 / 1:12</p><p>2:58 AM · Sep 9, 2024 · 86.3K Views</p></div>

# Lessons learned from AI-enabled attacks

- **AI-enabled human targeting.** These threats will be more difficult to detect and defend against, so tech needs to act as safety net
- **AI for evasion and challenge-solving poses significant challenges for traditional security measures.** Organizations must adapt by incorporating advanced AI-driven detection and mitigation techniques to stay ahead
- **Highlights the critical need for ongoing innovation to counteract the tactics employed by attackers.** As groups continue to evolve, so too must the defenses designed to protect against them





# AI for Security

## Key Use Cases

Triaging alerts on potential attacks

Identifying multiple attempts at compromise that are part of a larger attack campaign

Detecting the 'fingerprints' of malware within a computer or on a network

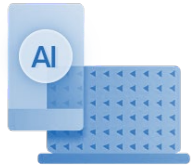
Integrated behavioral and linguistic detections, to identify advanced social engineering

Build of complex workflows, for attack surface disruption

# Layered defense-in-depth approach

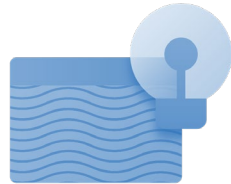
Actionable steps to protect from AI-generated malicious content

## Labeling of AI Content



Increase transparency by labeling content that has been created by generative AI.

## Content Credentials



Enables organizations to assert what content comes from them, using robust metadata.

## Watermarking



Invisibly embedding identifiers into media that is robust to minor modifications like cropping and screenshots.

## Detection



Detection isn't an end-state solution, as the technology on both sides will continue to evolve, but it is a useful tool in many cases.

## Literacy



Education of consumers is an essential component to defeat AI manipulated media.



# Centering our organizations on security

What is the path forward to improve resilience?

---

Hierarchy of security needs

---

Secure Future Initiative

---

# Hierarchy of cybersecurity needs

Drawing inspiration from Maslow's hierarchy of needs, this graphic illustrates a prioritization of cybersecurity, starting with the most basic need: protecting identities. AI has a role at each tier, underscoring its potential to enhance security measures.

Cultivating a robust security culture within the organization, helps ensure the technological defenses and human practices evolve in concert to mitigate threats effectively.



*...prioritizing **security above all else** is critical to our company's future"*



Satya Nadella  
Chairman and CEO



## A more resilient & transparent Microsoft

**Security is Job #1**

### **3 Principles of Microsoft's Secure Future Initiative**

#### **Secure by Design**

Security comes first when designing any product or service

#### **Secure by Default**

Security protections are enabled and enforced by default, require no extra effort, and are not optional

#### **Secure Operations**

Security controls and monitoring will continuously be improved to meet current and future threats

# What can we expect 2025?

- From disruption to destruction, as global threats ripple through supply chains
- Attackers commoditise the power of AI, to amplify attacks at scale
- As technology evolves, attackers will utilise advanced social engineering
- Cyber influence operations converge as a core tactic



# What does this mean for Defenders?

- Scale and deploy '*code & configs*' faster, by design & default
- Protecting identity – *whether people or machines* - is the core objective
- Building transparency through stronger collaboration, and harnessing intelligence '*at the speed of relevance*'.
- Protecting and governing data and intellectual property, no matter where it resides remains consistent





**Thank you**





# **Exclusive keynote**

---

**Rik Ferguson**

# SIGNIFICANT EVENTS IN 2024

Attacks, Accidents, and Nasty Surprises™



kaspersky



## SUPPLY CHAIN RISK

**CHANGE**  
HEALTHCARE

**synnovis**  
A SYNLAB pathology partnership

 **sisense**

 **snowflake**

**FEB '17**

ALP  
compro  
Cha  
Healt



**FEB 2-10**

RansomHub is  
announced on RAMP  
and claims first  
victim



**FEB**

Ranso  
27 m  
thro

s Change  
victim  
ins samples  
cident



**APR 8-30**

RansomHub  
claims more  
victims

# MOST NOTABLE RANSOMWARE GROUPS OF 2024

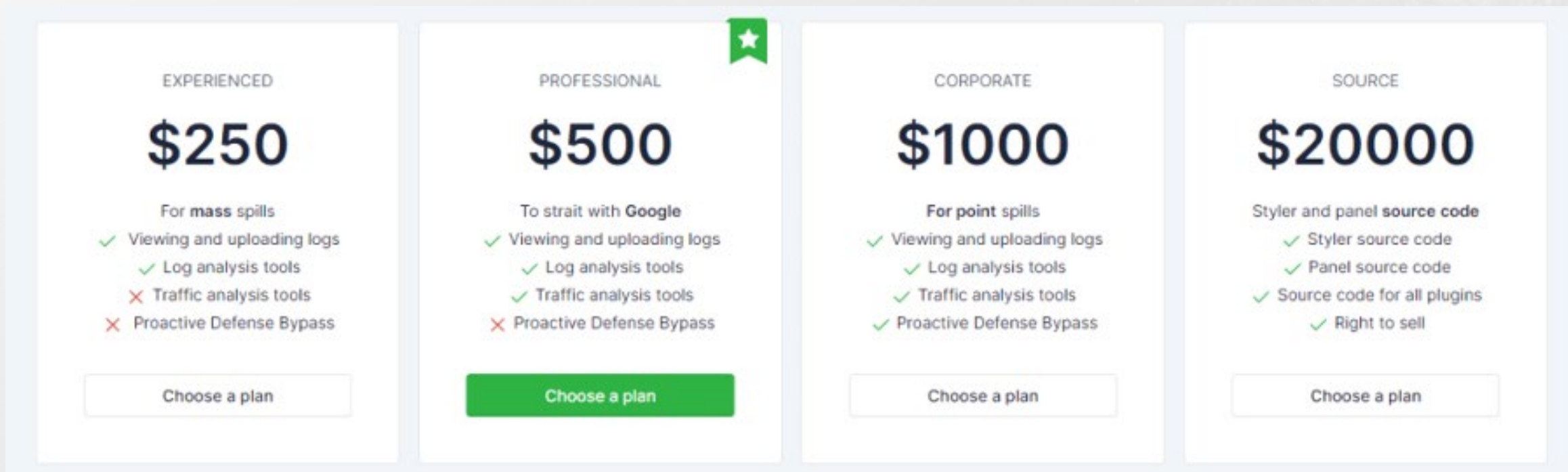
RansomHub	<b>593</b> claimed victims in 2024	First detected 2024
Play	<b>362</b> claimed victims in 2024	First detected 2022
Akira	<b>291</b> claimed victims in 2024	First detected 2023
Hunters Int.	<b>227</b> claimed victims in 2024	First detected 2023
Medusa	<b>212</b> claimed victims in 2024	First detected 2022
Qilin	<b>179</b> claimed victims in 2024	First detected 2022
BlackBasta	<b>176</b> claimed victims in 2024	First detected 2022
BianLian	<b>166</b> claimed victims in 2024	First detected 2021
INC Ransom	<b>162</b> claimed victims in 2024	First detected 2023
BlackSuit	<b>156</b> claimed victims in 2024	First detected 2023

## A BIG NUMBER

1 374 671 706

# RETURN OF THE INFOSTEALER

...now available as a service!



A pricing table for an infostealer service with four plans: Experienced (\$250), Professional (\$500), Corporate (\$1000), and Source (\$20000). The Professional plan is highlighted with a green star icon and a green 'Choose a plan' button. Each plan lists features with green checkmarks for included items and red X marks for excluded items.

EXPERIENCED	PROFESSIONAL	CORPORATE	SOURCE
<b>\$250</b>	<b>\$500</b>	<b>\$1000</b>	<b>\$20000</b>
For mass spills	To strait with Google	For point spills	Styler and panel source code
✓ Viewing and uploading logs	✓ Viewing and uploading logs	✓ Viewing and uploading logs	✓ Styler source code
✓ Log analysis tools	✓ Log analysis tools	✓ Log analysis tools	✓ Panel source code
✗ Traffic analysis tools	✓ Traffic analysis tools	✓ Traffic analysis tools	✓ Source code for all plugins
✗ Proactive Defense Bypass	✗ Proactive Defense Bypass	✓ Proactive Defense Bypass	✓ Right to sell
Choose a plan	Choose a plan	Choose a plan	Choose a plan

Most prevalent include Lumma, Formbook/XLoader and Vidar

# ZERO-DAY VULNERABILITIES IN 2024



# EDGE DEVICE ATTACKS RUN RAMPANT

Access, Exfiltration and Abuse

**FORTINET**®

 **paloalto**®  
NETWORKS

**ivanti**

  
**CISCO**

 **tp-link**

**ASUS**®

**ZYXEL**  
COMMUNICATIONS

  
**RUCKUS**™  
WIRELESS

QUAD7  
botnet

 **tp-link**

# TYPHOON SEASON

## Typhoon Classification\_



**Volt Typhoon**



**Salt Typhoon**




**Flax Typhoon**

# CONSEQUENCES OF WAR



# CONSEQUENCES OF WAR



**Hacked! Зламано!**

Er ENSTO  
Ensto E-RTU 2020  
New control cabinet

Industrial Electrical controller attacked and demolished in SPB, Russia!


Напад на промисловий електроконтролер та його знищення в СПб, Росія!

voltageonefist Nov 17 · 1 min

## Operation Neutrino

Operation Neutrino is an on-going mission where we attacked a high-voltage power-grid controller in SPB Russia. The public release is...

74 views 0 comments 6



**Hacked! Зламано!**

TM258LD42DT

Eight Industrial voltage controllers attacked in Yekaterinburg Russia!

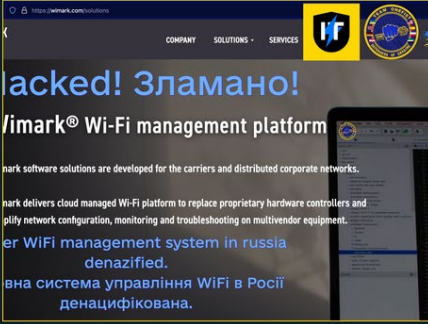
Вісім промислових контролерів напруги зазнали нападу в Єкатеринбурзі, Росія!

voltageonefist Nov 17 · 2 min

## Operation Positron

Fire in the hole! This week, we celebrate the great liberation of Kherson together, with a gift of fire from us: Operation Positron....

29 views 0 comments 2



**Hacked! Зламано!**

Wimark® Wi-Fi management platform

Wimark software solutions are developed for the carriers and distributed corporate networks.

Wimark delivers cloud managed Wi-Fi platform to replace proprietary hardware controllers and simplify network configuration, monitoring and troubleshooting on multivendor equipment.

Відома система управління WiFi в Росії денацифікована.

voltageonefist Nov 8 · 1 min

## Operation Wimark

Оголошено операцію "Вімарк" (відбулася 2 листопада)! Ми атакували і знищили велику систему управління WiFi роутерами в Росії. Зникло...

89 views 2

Save https://orbiilet.ru/city17/any 67%

orbiilet.ru 8-800-698-47-44 support@orbiilet.ru CITY: VVKSA

TICKETS FROM THE ORGANIZER | GUARANTEED MONEY BACK

TICKET SYSTEM КОТАКТИ HELP ENTRANCE

search on the poster All Movie Concert

Dear friends!

Please note that requests for purchases, including ticket refunds, are accepted by email support@orbiilet.ru. In the email, you must specify the name of the event, the venue, and the eight-digit purchase code. In the refund request, you must also indicate the reason for the refund.

Please note that due to the large number of requests, the deadline for reviewing applications may take up to 2 days.

Thank you for your understanding!

< November 2022 >

Mon	Tue	Wed	Thu	Fri	Sat	Sun
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

Lepse Palace of Culture

Россия террористическое государство!

RUSSIA IS A TERRORIST STATE which violates international law

Гордимся представить Путина убийцей! Остановить войну!

KINGDOM VS ROBBERS  
Monday 28 November, 10: 30  
Lepse Palace of Culture  
other sessions (3)

Tickets 160 rub

Россия террористическое государство!

RUSSIA IS A TERRORIST STATE which violates international law

Гордимся представить Путина убийцей! Остановить войну!

HONEST DIVORCE 2  
Monday 28 November, 12: 00  
Lepse Palace of Culture  
other sessions (3)

Tickets 190 rub

Россия террористическое государство!

RUSSIA IS A TERRORIST STATE which violates international law

Гордимся представить Путина убийцей! Остановить войну!

CHINK: THE TAILED DETECTIVE  
Monday 28 November, 13: 50  
Lepse Palace of Culture  
other sessions (1)

Tickets 190 rub

Россия террористическое государство!

RUSSIA IS A TERRORIST STATE which violates international law

Гордимся представить Путина убийцей! Остановить войну!

JEANNE  
Monday 28 November, 18: 50  
Lepse Palace of Culture  
other sessions (2)

Tickets 230 rub

Россия террористическое государство!

RUSSIA IS A TERRORIST STATE which violates international law

Гордимся представить Путина убийцей! Остановить войну!

"Unforgettable"  
Tuesday 29 November, 19: 00  
Lepse Palace of Culture

Tickets 1200-2300 rub

Россия террористическое государство!

RUSSIA IS A TERRORIST STATE which violates international law

Гордимся представить Путина убийцей! Остановить войну!

An ordinary miracle  
Wednesday, November 30, 18: 30  
Lepse Palace of Culture

Tickets 500 rub

Россия террористическое государство!

RUSSIA IS A TERRORIST STATE which violates international law

Гордимся представить Путина убийцей! Остановить войну!

POKERFACE  
Monday 28 November, 17: 00  
Lepse Palace of Culture  
other sessions (1)

Tickets 200 rub

Россия террористическое государство!

RUSSIA IS A TERRORIST STATE which violates international law

Гордимся представить Путина убийцей! Остановить войну!

# CONSEQUENCES OF WAR

**GhostSec**  
@ghost\_s3curity

We, #GhostSec declare that we were infact responsible for the "mysterious" emergency shutdown.

We now state that the ICS attack was successfully executed with 0 casualties in the actual explosion due to our proper timing while preforming our attacks.

[mirror.co.uk/news/world-new...](https://mirror.co.uk/news/world-new...)

East2West THE Sun

0:01 19.4K views

1:14 AM · Jul 20, 2022 · Twitter for Android

**Thraxman** 🌻🌐 @ThraxmanOneFist Nov 13

We attacked their #SCADA/#ICS, demolishing 8 expensive Schneider M258s #PLC, w/2400 channels & 16 DOF each for complex machines. This led to a fire that erased an entire workshop building, and took 13 trucks to extinguish! According to locals the first 3 arrived without water 😂 2/

E10RU PRINZIP

"It reeks of burnt plastic." A large fire broke out at the Sorting station

The source is located at an automobile repair plant

November 16, 2022, 14:28 13 PHO

Expensive only for those who did not live there." It is easy to move to Turkey and the UAE, today realtors answer

Schoolchildren risk their lives on the Tyumen highway to get to classes. Video

In Nizhny Tagil exposed the police officer who received a bribe from the drug dealer

Doctors told why to visit the cardiologist if there are no complaints, and what factors should be abandoned to strengthen the heart

"It's not just about aesthetics." The plastic surgeon told what parts of a body Swedish residents most often ask to change

"We don't want to be in a magnetic field." Yekaterinburg residents rebelled against a cell tower near a kindergarten

The first conspiracy from the

# CHALLENGES IN SECURING OPERATIONAL TECHNOLOGY

## ICS/OT vulnerabilities

- 2,010 ICS/OT vulnerability advisories in 2023.
- 27% of advisories had no patch, of those 18% had no mitigation either!



## Operational technology

- Rarely managed by integrated security teams.
- Limited to zero visibility of assets.



## Industrial Control Systems

- Not designed for connectivity.
- Insecure by design.
- Supply chain weakness.



# TODAY'S REALITY



# THE SCALE OF THE PROBLEM



# IF DATA IS THE NEW OIL



# CYBER SECURITY, THE DEPARTMENT OF NO?

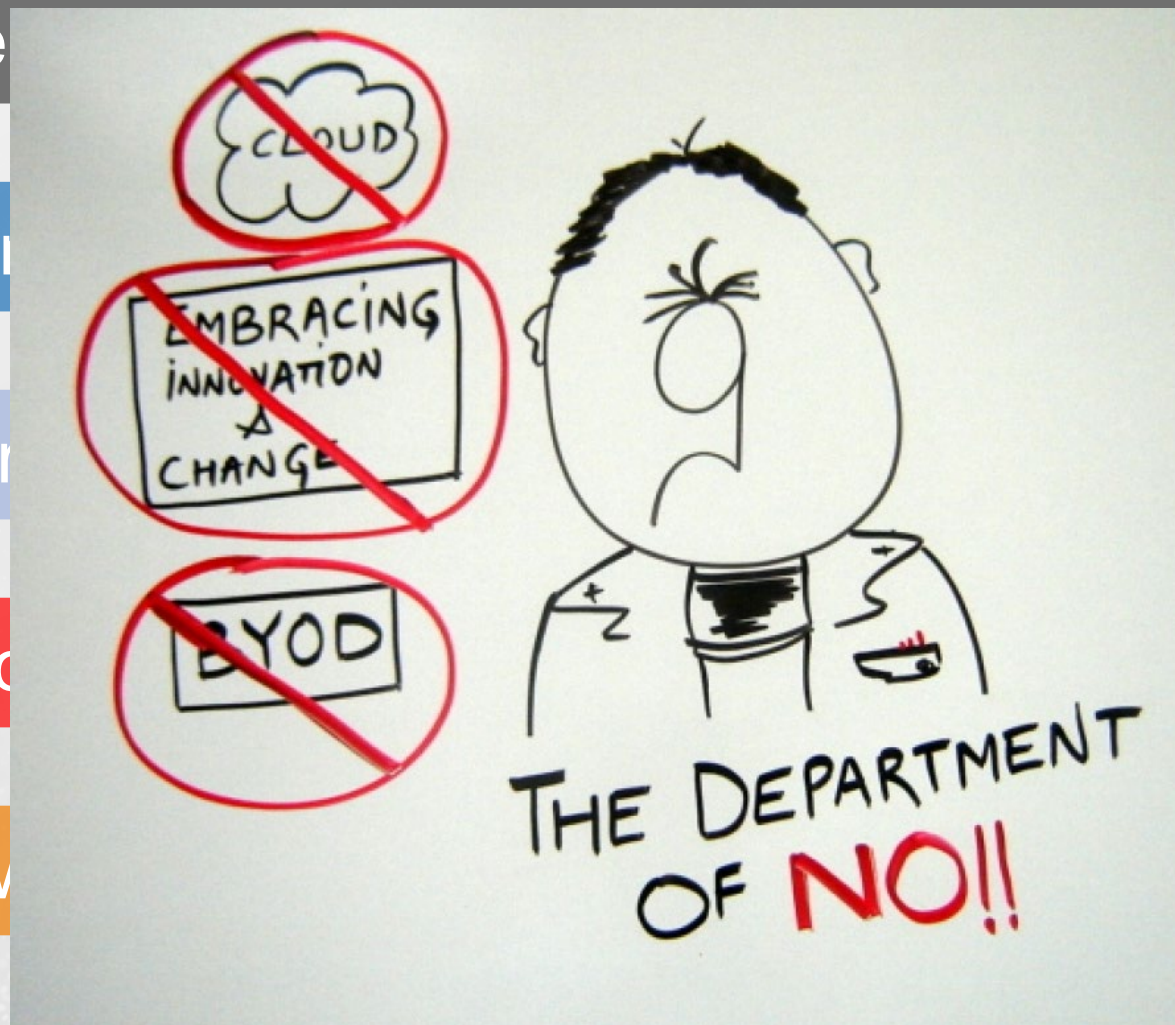
Know your threat

Know your environment

Know your users

Know your data

Know your tools





---

# Closing remarks



---

# Networking drinks



# THANK YOU FOR ATTENDING THE ITC CYBER SUMMIT 2025

Addressing the biggest trends in cyber security

Redefining the basics

Sponsored by:

Sponsored by:

