CONVENZIS

Welcome to the NHS Cyber Security Conference!

25th February 2026
etc.venues, Prospero House, 241
Borough High Street, London, SE1 1GA

CYBERSECURE 2026
CONFIRMED SPONSORS

CONVENZIS TRAINING

Please scan the QR Code on the screen below to register your interest for our accredited training courses.

HESUK Powered by - CONVENZIS

Join the Healthcare Engagement Society (HES)

- **What it is** – A secure, year-round platform bringing NHS professionals together across six specialist communities.
- **Why it matters** – Stay connected beyond today's event, share challenges, and learn from peers facing the same priorities.
- **Your benefits** – Exclusive access to interviews, insights, best practice, and real-time discussion threads with colleagues nationwide.
- **How to join** – Simply scan the QR code, choose your community, and start connecting today.

Slido

Please scan the QR Code on the screen. This will take you through to Slido, where you can interact with us.

SCAN ME

Chair Opening Address

Dr Avi Mehra
Associate Partner & Clinical Safety Officer
IBM

Leadership Lessons from the Front Line

Barry Richardson
Head of Cyber Security and Information Security
NHS Blood and Transplant

PREPARED, PROTECTED, RESILIENT

MANAGING THE RANSOMWARE RISK IN HEALTHCARE AND HOW AI HELPS

FEBRUARY 2026

QUESTION TIME
Q & A SESSION

Q1. I am confident that **my organisation** could detect a ransomware attack before encryption begins (B3/C1/C3)

Q2. Each of **my organisation's** backups are immutable, documented and regularly tested including restoration (D2)

Q3. If called at 3am tomorrow morning I can instantly mobilise my role in **my organisation's** Ransomware Response Plan (D1)

Q4. **My organisation** has tested a ransomware response in the past 12 months at Board level (A1/D1)

Q5. I am confident ransomware risk is understood in **my organisation** and is known to the Board and within the Board's declared risk tolerance level (A2/A1)

Q6. Does anyone know why **my organisation** is in bold in each question?

Q7. I use AI to help shift conversations in **my organisation** from evidence creation and collection to organisational resilience.

OWNERSHIP
RANSOMWARE RISK

Ransomware risk doesn't sit with any one person or team — it sits with **your organisation**.

Across a multidisciplinary industry like ours, people contribute in different ways.

Your role is unlikely to be 'own the risk' (unless you are CEO - who is accountable for Organisational Risk)

Your role is more likely to be one of these:

Identifying cyber risks that are unacceptable/uncontrolled/do not meet the CAF requirement(s)

Proposing how those risks could be reduced/mitigated/~~eradicated~~

Implementing the agreed risk reduction/mitigations

Supporting others as they resolve related issues

INFORMATION
WHAT IS RANSOMWARE?

According to the UK's National Cyber Security Centre (NCSC), ransomware is

'malicious software (malware)
that gains **unauthorised access** to systems, encrypts files, and **blocks access to data and devices**,
with attackers demanding a ransom (usually cryptocurrency) for a decryption key,
often adding threats to **leak stolen data** for further extortion.'

It's a significant cyber threat that locks users out of their own information until they pay up (moot point), causing major disruption and data loss for organisations.

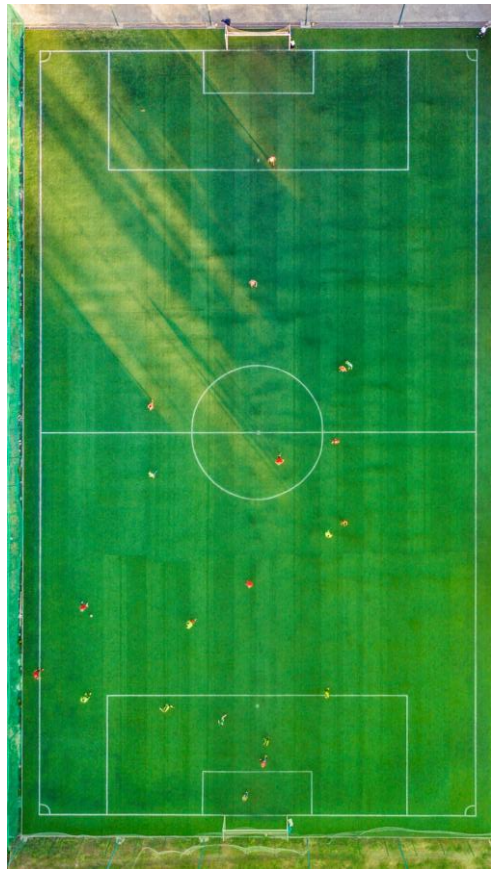
Interesting side points –

Some ransomware gangs build their credibility by always issuing keys post ransom payment – their business model relies upon their integrity (!)

Even if keys are provided, recovery is painful, slow, and not guaranteed

INGRESS
HOW DOES RANSOMWARE GET INTO YOUR NETWORK?

Attack Vector	Technical	Tactical	Behavioural	Notes / Strategic Interpretation
Phishing & Social Engineering	☐	✅	✅	**Human**-centred vector; relies on persuasion, trust, and emotional triggers. Often used for initial access or credential theft.
Exploiting Unpatched Vulnerabilities	✅	☐	☐	Purely **technical** weakness; exposure driven by patch cadence, asset visibility, and configuration hygiene.
Re-using Compromised Credentials & Remote Access	✅	✅	☐	**Identity-driven** attack path; attackers bypass perimeter controls using stolen or weak credentials.
Supply Chain Attack	✅	✅	☐	Compromise arrives through **trusted partners**, software updates, or integrations; high-impact, low-visibility vector.
Drive-by Downloads & Malvertising	✅	☐	✅	Hybrid vector; user **browsing behaviour** intersects with web-based technical exploits.
Physical Media (USB, removable drives)	✅	☐	✅	Still relevant in healthcare and operational environments; relies on curiosity, convenience, or poor device handling.



DETECTION

EARLY RANSOMWARE DETECTION IS THE DIFFERENCE BETWEEN *INCONVENIENCE* AND *CATASTROPHE*

Ransomware is loud at the end, but quiet at the beginning

By the time files start encrypting, the attacker has already:

- Broken in
- Moved laterally
- Escalated privileges
- Stolen data
- Disabled backups
- Mapped the network

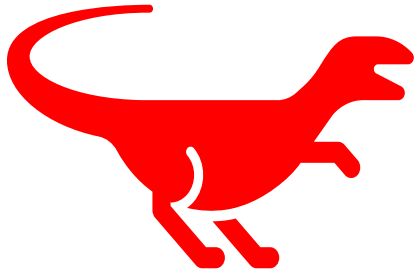
Encryption is the final act — not the beginning. If you detect the attacker *before* this stage, you stop the disaster before it becomes visible.

Early detection stops the attacker before they gain "blast radius"

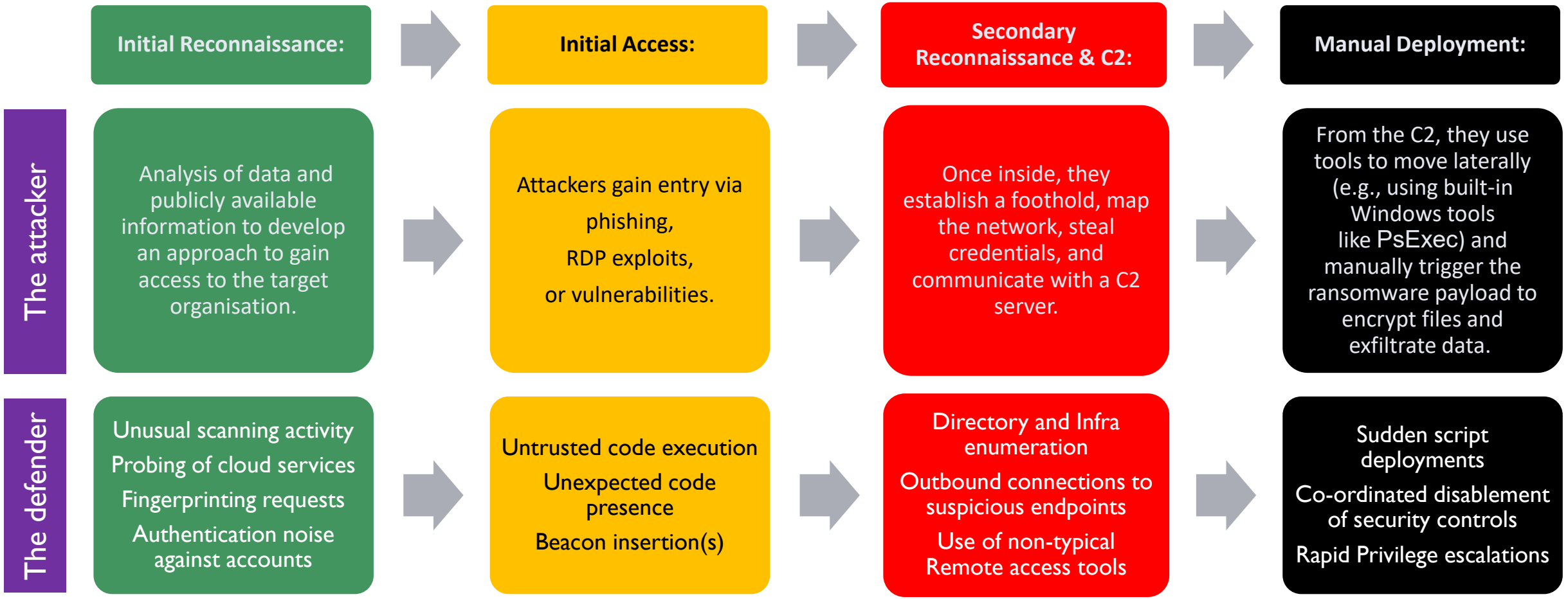
Ransomware becomes catastrophic when attackers reach:

- Domain admin
- Backup systems
- Clinical Systems
- Shared Drives
- Identity providers
- Hypervisors

Ransomware is essentially a near-extinction event

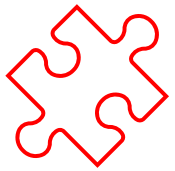


RISK MINIMISATION
RANSOMWARE LIFECYCLE



C2 = Command and Control

HOW IT WORKS
HOW RANSOMWARE SPREADS



Modern ransomware frequently incorporates **worm-like propagation capabilities**, enabling it to automatically identify and compromise other vulnerable systems across the network without requiring manual attacker action on each device.

Ransomware can propagate by exploiting **network shares**, leveraging **software vulnerabilities**, or using **data-transfer** tools such as Rclone to move laterally and spread rapidly across the environment.

The attacker coordinates the overall **campaign** — from the initial breach to target selection and data exfiltration — but the ransomware payload itself is engineered to operate autonomously, propagating rapidly and aggressively once deployed, which makes containment significantly more challenging.

WHY IS HEALTHCARE SO ATTRACTIVE
INHERITED 'UNIQUE' HEALTHCARE RISK

Structural & Technical Factors

Network Architecture - Flat or lightly segmented networks allow threats to move quickly once inside

Legacy - Complex, and highly interconnected estates — includes clinical and portable devices that cannot easily be patched

Supply Chain - A broad, multi-layered supply chain with uneven cyber maturity and shared access routes

Shadow IT - Unmanaged or informal technology adoption (shadow IT), from clinician-led innovation to ad-hoc devices and unsecured peripherals

Operational Realities

Downtime Intolerance - Limited tolerance for downtime, constraining patching, maintenance, and architectural change

Diverse User Base - Clinicians, back-office administrative, contractors, suppliers, and specialists — each with different behaviours, access patterns, and risk profiles

Strategic & Financial Constraints

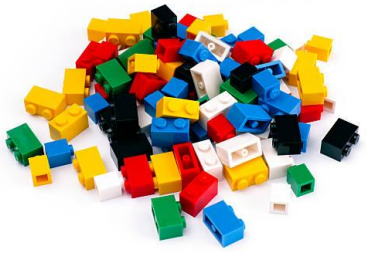
Data Value - High-value data that makes healthcare a prime target for extortion-driven attacks

Investment Constraints - Restricted long-term investment, accumulates technical debt and slows modernisation

Organisational Change - Including mergers increases complexity and reduces control consistency

THE CAF
WHAT THE CAF SAYS (ABOUT RANSOMWARE)

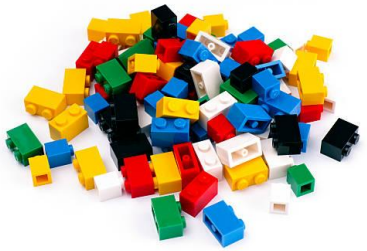
Objective A – Managing Security Risk	Objective B — Protecting Against Cyber Attack	Objective C — Detecting Cyber Security Events	Objective D — Minimising the Impact of Cyber Incidents
A1 – Governance *Ensures ransomware is treated as a strategic risk with accountable owners*	B1 – Identity & Access Control *Prevents credential theft and lateral movement*	C1 – Security Event Detection *Detects suspicious activity (e.g., mass file access, privilege escalation)*	D1 – Response & Recovery Planning *Incident response plans, ransomware playbooks, tested recovery*
A2 – Risk Management *Requires threat-informed risk assessment, including ransomware scenarios*	B2 – Secure Configuration *Hardening, patching, disabling macros, reducing exploitability*	C2 – Situational Awareness *Understanding attacker TTPs, threat intel on ransomware groups*	D2 – Backup & Restore *Backup integrity, offline/immutable backups, restoration capability*
A3 – Asset Management *You cannot protect or recover assets you haven't identified*	B3 – Security Monitoring *Detects early-stage ransomware behaviours (EDR, anomaly detection)*	C3 – Anomaly Detection *Identifies unusual behaviour that precedes encryption*	D3 – Lessons Learned *Post-incident improvements after ransomware attempts or drills*
	B4 – Secure Design & Operation *Segmentation, least privilege, isolation of critical systems*		
	B5 – Supply Chain Security *Prevents ransomware delivered via third-party compromise*		



LIKELY POSTURE
A TYPICAL 'NUTS AND BOLTS' CAPABILITY ASSESSMENT

We likely all have baseline capabilities across most CAF elements, and most likely looks like this:

Objective A – Managing Security Risk	Objective B — Protecting Against Cyber Attack	Objective C — Detecting Cyber Security Events	Objective D — Minimising the Impact of Cyber Incidents
A1 – Governance *You have identified all security accountabilities and documented them.*	B1 – Identity & Access Control *MFA was mandated across Government a couple of years ago*	C1 – Security Event Detection *MS MDE managed via NHSE CSOC – requires proactive log searching and does not cover all ingress points*	D1 – Response & Recovery Planning *Part of DSPT for several years*
A2 – Risk Management *You have adopted Cabinet Office Secure by Design Standard*	B2 – Secure Configuration *Partly addressed by CareCERT alerts*	C2 – Situational Awareness *NHSE webinars recently started to address this through the Cyber Associates programme*	D2 – Backup & Restore *Likely the most immature element – some immutable, some tested, some documented, still work in progress*
A3 – Asset Management *DSPT has been asking for Asset Inventories for several years*	B3 – Security Monitoring *MS MDE managed through NHSE – requires proactive log searching and does not cover all ingress points*	C3 – Anomaly Detection *MS MDE managed through NHSE – requires proactive log searching and does not cover all ingress points*	D3 – Lessons Learned *Being healthcare, we already have matured review processes*
	B4 – Secure Design & Operation *Requested across DSPT for several years – journey started*		
	B5 – Supply Chain Security *Growing understanding over past years – likely LOG4J type incident helped accelerate your capability*		



EASE OF FIX

EASE OF FIX IMPLEMENTATION FOR RANSOMWARE RISK REDUCTION

Low effort	Low-Medium effort	Medium effort	Medium-High effort	High effort
A1 – Governance Roles, accountability, decision authority *Mostly policy, ownership, and clarity — fast to establish.*	**D1 – Response & Recovery Planning** IR plans, ransomware playbooks *Documentation + exercises; fast to stand up, refine over time.*	**A3 – Asset Management** Inventory, classification *Needs tooling + process; harder if estate is messy.*	**B3 – Security Monitoring** EDR/XDR, behavioural detection *Tooling + tuning + SOC maturity; not trivial.*	**B1 – Identity & Access Control** MFA, least privilege, PAM *Identity uplift is complex, touches every user/system.*
A2 – Risk Management Threat-informed risk assessment *Workshops + documentation; no heavy tech uplift.*		**B5 – Supply Chain Security** Supplier assurance, access control *Process + contract uplift; slower but not deeply technical.*		**B2 – Secure Configuration** Patching, hardening, allow-listing *Requires tooling, process change, and estate-wide remediation.*
C2 – Situational Awareness Threat intel, sector alerts *Subscription + process; quick uplift.*		**C1 – Event Detection** Detection rules, log visibility *Needs SIEM/SOC capability but not full redesign.*		**B4 – Secure Design & Operation** Segmentation, secure builds Architectural change; long-tail remediation.
D3 – Lessons Learned Post-incident improvement *Process-driven; easy to implement once IR exists.*		**C3 – Anomaly Detection** Behaviour baselining *Requires monitoring maturity + tuning.*		**D2 – Backup & Restore** Immutable/offline backups

TAKEAWAYS
FOUR ‘FREE GIFTS’

TOOL 1 –
5 minutes Ransomware resilience READINESS Ready-reckoner

- A rapid, high-level indicator of organisational resilience
- A clear baseline to anchor capability discussions
- A quick way to surface priority gaps and opportunities
- A validation tool to test assumptions about current posture
- A prompt for aligned, continuous, and measurable improvement

TOOL 2 –
15 minutes capability review - NCSC top 10 cyber threats readiness tool

- Rapid method to surface risks, gaps
- Validation of your ‘overall posture’
- Gives rapid baseline of capabilities/opportunities
- Broaden thinking across a wider threat surface area
- Allows brainstorming of improvement opportunities particularly against areas which you might consider higher risk

TOOL 3 –
90-day Implementation/Risk Reduction Programme

- A focused, time-bound framework for driving measurable improvement
- A structured way to convert insight into prioritised action
- A mechanism to validate assumptions and confirm organisational risk posture
- A disciplined approach to sequencing effort for maximum impact
- A clear roadmap that aligns stakeholders around what must happen next

TOOL 4 –
Question sets seeding how AI can help your thinking about

- Your CAF Approach
- Testing evidence quality and thoroughness
- Analysing capabilities and gaps
- Stress testing risk thinking
- Strengthening your narrative for wider education and discussion
- Accelerating decision-making

QUESTIONS?

INFORMATIONAL

WHICH CYBER DISCIPLINES **PROTECT DETECT** RESPOND AND RECOVER RE: RANSOMWARE INGRESS?

Protect

Discipline	Role
B4 Security Architecture	Designs layered defences and segmentation to limit spread.
B2 Vulnerability Management	Ensures systems are patched and hardened against exploits.
B1 Identity & Access Management	Prevents lateral movement and privilege escalation.
B4 Network Security	Blocks malicious traffic and isolates critical assets.
B2 Endpoint Security	Detects and blocks ransomware payloads at device level.
A3 Security Awareness & Behavioural Change	Reduces phishing and social engineering success.
B2 Secure Configuration	Minimises attack surface through hardened defaults.
B4* Zero Trust Architecture	Limits trust relationships and enforces continuous verification.
A4 Supply Chain Security	Prevents indirect compromise via third-party software or services.

Detect

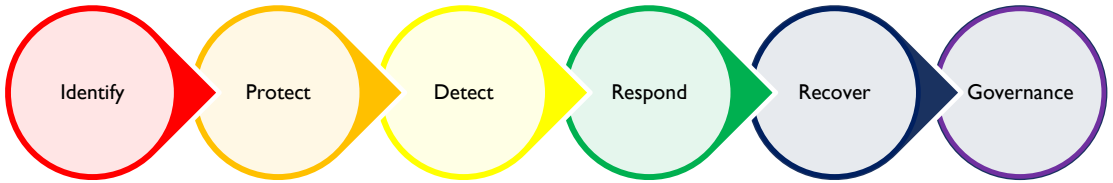
Discipline	Role
D2 Security Operations	Monitors for indicators of compromise and unusual behaviour.
D2 Security Monitoring & SIEM	Aggregates logs and alerts for early detection.
D2 Threat Intelligence	Tracks ransomware groups, TTPs, and emerging threats.
D2 SOC Management	Coordinates detection and triage across the organisation.
D1/D2 Security Automation & Orchestration (SOAR)	Speeds up detection and response workflows.

Respond

Discipline	Role
D1 Incident Response	Coordinates containment, eradication, and communication.
D1 Digital Forensics	Investigates root cause and scope of compromise.
D1 Malware Analysis	Understands payload behaviour and potential impact.
A1 Security Policy & Standards	Guides response actions and escalation protocols.

Recover

Discipline	Role
D1 Business Continuity	Ensures critical services continue during disruption.
D1 Disaster Recovery	Restores systems and data from clean backups.
D1/B4/A2 Resilience Engineering	Designs systems to withstand and recover from ransomware.
A1/A2 Security Programme Management	Oversees long-term improvements post-incident.



* But not uniquely

TOOL 1 –
5 MINUTES RANSOMWARE RESILIENCE READINESS READY-RECKONER

CAF Objective	Core Principle	Readiness Indicator (The "Acid Test")	Status (R/A/G)	Evidence / Required Action
A: Governance	**Asset Mgmt**	Can you identify all internet-facing assets and their current patch status within 1 hour?		
A: Governance	**Supply Chain**	Do you have a manual "paper-based" process to operate if our primary SaaS/Cloud provider is encrypted?		
B: Protection	**Identity (MFA)**	Is MFA mandatory for all users, including service accounts and legacy VPNs?		
B: Protection	**Privilege**	Is there a "Zero Trust" policy preventing users from installing software or executing scripts?		
B: Protection	**Data Security**	Are backups stored on a separate, non-domain-joined, immutable platform (off-site/offline)?	*** MUST BE GREEN ***	
B: Protection	**Segregation**	If a single workstation is hit, is the "Lateral Movement" to your services blocked by VLANs and Firewalls?		
C: Detection	**Monitoring**	Does your SOC/Team receive alerts for "Pre-cursor" tools (e.g., Mimikatz, Advanced IP Scanner, Cobalt Strike)?		
D: Recovery	**Incident Response Planning**	Do you have a physical/printed "Battle Box" containing emergency contacts and recovery runbooks?		
D: Recovery	**Capability**	Have you successfully performed a "Bare Metal Restore" of a core service from backups this year?		

Green: (Highly Resilient) Fully implemented, regularly tested, and documented.
Amber: (partly Resilient) Policy exists, but implementation is patchy or hasn't been tested in >6 months.
Red: (At risk) No formal control in place, or we are relying on "hope" as a strategy.

Pro Tip: In the context of CAF, **Section B3 (Data Security)** is your last line of defence. If you cannot mark B3 as **Green**, your organization's survival during a ransomware event is at extreme risk regardless of other scores.

TOOL 2 – READY RECKONER FOR TOP 10 NCSC THREATS (CONDENSED 'GUT' FEEL)

Threat (NCSC-style)	What it is (very briefly)	Main CAF objectives to lean on	Quick susceptibility checks
Phishing & credential theft	Luring users to give away passwords or MFA codes	**A:** Managing security risk; **B2:** Identity & access; **B3:** Data security; **C1:** Security monitoring	Weak MFA, poor user training, no phishing simulation, limited monitoring of logins, shared accounts
Ransomware	Malware encrypting data and disrupting operations	**A3:** Risk management; **B1:** Protective technology; **B3:** Data security; **D1–D3:** Incident response & recovery	Flat networks, poor patching, weak backups (no offline/immutable), no rehearsed IR playbook, local admin everywhere
Exploitation of known vulnerabilities	Attacks via unpatched software, firmware, or misconfigurations	**A3:** Risk management; **B1:** Protective technology; **B4:** Secure configuration; **C1:** Monitoring	No asset inventory, irregular patching, legacy systems unmanaged, weak vulnerability management, no config baselines
Business email compromise (BEC)	Social engineering to redirect payments or steal data	**A2:** Governance; **B2:** Identity & access; **B3:** Data security; **C1:** Monitoring	No MFA on email, weak finance controls, no out-of-band verification, poor logging of mailbox rules/forwarding
Supply chain compromise	Attack via suppliers, MSPs, software updates	**A1–A4:** Governance & risk; **B1:** Protective tech; **C1:** Monitoring; **D1:** Response planning	No supplier assurance, over-privileged third-party access, no SBOM/patch scrutiny, weak contract security clauses
Insider threat (malicious or negligent)	Harm from staff/contractors, intentional or accidental	**A2:** Governance; **B2:** Identity & access; **B3:** Data security; **C1:** Monitoring	Excessive privileges, no joiner/mover/leaver discipline, weak DLP, no behavioural monitoring, poor culture/reporting
DDoS & service disruption	Overwhelming services to deny access	**B1:** Protective technology; **C1:** Monitoring; **D2–D3:** Continuity & recovery	No DDoS protection, single-homed connectivity, no tested failover, no traffic baselining or runbooks with ISP/CDN
Data exfiltration & privacy breach	Theft or leakage of sensitive data	**A3:** Risk management; **B3:** Data security; **B2:** Access control; **C1:** Monitoring	No data classification, weak encryption, broad access to sensitive stores, no egress controls, minimal logging
Cloud misconfiguration & abuse	Poorly configured SaaS/IaaS/PaaS leading to compromise	**A3:** Risk; **B1:** Protective tech; **B2:** Identity & access; **B4:** Secure configuration	No cloud security baselines, weak IAM (no conditional access), public buckets, unmanaged keys, no CSPM tooling
Website/app compromise (incl. web-facing APIs)	Attacks on public apps (SQLi, XSS, auth flaws)	**B1:** Protective tech; **B4:** Secure configuration; **C1:** Monitoring; **D1:** Response	No secure SDLC, no regular app testing, weak WAF, shared admin accounts, no structured logging of app events

TOOL 3- RANSOMWARE RECOVERY AND PROTECTION 90 DAY PLAN **INTRODUCTION**

Context:

All organisations—especially the NHS—face complexity.

Legacy technology and system interdependencies mean rapid execution is often impractical without significant capital and effort.

Strategic Response:

Where immediate action is constrained, profile and prioritise risks.

Focus on:

- Capturing the consequences of inaction
- Assigning ownership for risk management and containment
- Clarifying technology and capability responsibilities

Execution Timeline:

- Days 01-30 - *Blocking the most common entry points and securing the "Last Line of Defence"*
- Days 31-60 - *Spotting the "Pre-cursors" (the 24-48 hours attackers spend in your network before encrypting)*
- Days 61-90 - *Proving you can actually recover without a decryption key*

SECTION 3 – TURNING TO THE CAF

CAF Principle	Ransomware Relevance
B3.a Data Security	Offline/Immutable Backups (prevents permanent data loss).
B4.c Malicious Code	Endpoint Protection (stops the ransomware .exe from running).
B5.a Network Design	Segmentation (stops the virus from spreading to other computers).
B2.a Identity/Access	MFA & Least Privilege (prevents hackers from using stolen passwords).
C1.a Monitoring	Anomaly Detection (detects mass encryption or data theft).
D1.a Response Plan	Recovery Drills (ensures you can restore the business without paying).

DAYS 1-30 HIGH IMPACT 'KILL CHAIN' BREAKERS

FOCUS: BLOCKING THE MOST COMMON ENTRY POINTS AND SECURING THE ***LAST LINE OF DEFENCE***

Objective A: Managing Security Risk

- **Asset Sweep:** Run a discovery scan to find "Shadow IT" or forgotten servers.
- **Crown Jewels:** Document the top 5 systems required to run the business.
- **Board Brief:** Secure a "Ransomware Decision Maker" (who decides whether to pay/not pay

Objective B: Protecting Against Attack

- **MFA Enforcement:** Enforce MFA on all remote access (VPN, Citrix, RDP).
- **Admin Isolation:** Disable internet access and email on all Domain Admin accounts.
- **Legacy Auth:** Disable "Legacy Authentication" (e.g., POP3, IMAP) in Microsoft 365.
- **RDP Exposure:** Scan for and shut down any RDP ports (3389) open to the internet.
- **Back-up Immutability:** Move one copy of backups to a "Write Once Read Many" (WORM) storage.
- **Back-up Air-Gap:** Physically or logically disconnect the backup server from the main domain.
- **Privileged Access:** Change all local admin passwords using a tool like LAPS (Local Administrator Password Solution)
- **Service Accounts:** Audit service accounts and reset passwords for any with "Domain Admin" rights.
- **Macro Blocking:** Disable Office Macros for all users except those with a documented business need.
- **Powershell:** Enable "Constrained Language Mode" to stop attackers running malicious scripts.
- **Software Restriction:** Block execution of files from AppData/Local and Temp folders.
- **Patching:** Apply "Emergency" patches to all internet-facing firewalls and VPNs within 24 hours.

DAYS 31-60 DETECTION AND CONTAINMENT

FOCUS: SPOTTING THE "PRE-CURSORS" (THE 24-48 HOURS ATTACKERS SPEND IN YOUR NETWORK BEFORE ENCRYPTING).

Objective B: Staff Awareness

- **Phishing Sim:** Run a simulation targeting the Finance and IT teams.
- **"Report" Button:** Ensure every user has a one-click way to report a suspicious email.
- **Admin Training:** Train IT staff on why they should never browse the web using admin creds

Objective C: Detecting Cyber Security Events

- **Canary Files:** Place "honey-files" (e.g., Salary_2025.xlsx) on file shares; alert if they are touched.
- **EDR Deployment:** Ensure your Endpoint Detection (EDR) is in "Block" mode, not just "Alert."
- **Log Centralization:** Direct your VPN and Firewall logs to a central, protected log server.
- **Alerting:** Set alerts for "Mass File Renaming" or "Mass Data Deletion."
- **Admin Activity:** Alert on any new "Domain Admin" account creation.
- **Network Segregation:** Fire-wall off your Backup Server so it only talks to its agents.
- **Lateral Movement:** Block "Workstation-to-Workstation" communication via Windows Firewall.
- **Inbound Mail:** Implement DMARC/SPF/DKIM to reduce phishing success.
- **DNS Filtering:** Use a DNS filter (like Quad9 or Umbrella) to block known ransomware C2 domains.
- **Data Egress:** Set a threshold alert for large volumes of data leaving the network (Exfiltration).

DAYS 61-90 RESPONSE AND RECOVERY READINESS

FOCUS: *PROVING YOU CAN ACTUALLY RECOVER WITHOUT A DECRYPTION KEY.*

Objective A & B: Governance & Supply Chain

- **Mover/Leaver:** Automate the 24-hour disabling of accounts for staff who leave.
- **Supply Chain Audit:** Ask your top 3 software vendors for their own Ransomware Resilience statement.
- **Cloud Config:** Audit AWS/Azure/M365 "Global Admin" accounts—ensure they all use hardware MFA.
- **Vulnerability Scan:** Run a credentialed internal scan to find unpatched software.
- **Device Hardening:** Disable LLMNR and NetBIOS (common protocols used for password theft).
- **Shadow IT:** Block unauthorized Cloud Storage sites (Dropbox/WeTransfer) to prevent exfiltration.
- **Cyber Insurance:** Verify that your policy actually covers "Ransomware Remediation" and "Loss of Business."
- **BYOD Policy:** Ensure personal laptops cannot connect to the core server network.
- **Scripting Audit:** Disable "vbs" and "hta" file associations on workstations.
- **Inventory Update:** Label every server as "Critical," "Important," or "General."
- **Post-Mortem Setup:** Create a template for "Lessons Learned" to use after every minor incident.
- **Final Audit:** Re-run the **CAF Ready Reckoner** to verify the 90-day progress.

Objective D: Minimising Impact

- **Restoration Test:** Perform a "Bare Metal Restore" of your #1 Crown Jewel system.
- **RTO/RPO Validation:** Calculate exactly how long it takes to restore 1TB of data from your current backups.
- **Out-of-Band Comms:** Set up a WhatsApp or Signal group for the IT team to use if email is down.
- **Hard-Copy Playbook:** Print your Incident Response plan (you can't read a PDF on an encrypted drive).
- **Emergency Contacts:** Print a list of all critical vendor support numbers and insurance details.
- **Tabletop Exercise:** Run a 2-hour "What If" session with the leadership team.
- **Wipe Policy:** Define the "Point of No Return" for when you stop cleaning and start wiping/reimaging.
- **Forensic Retainer:** Ensure you have a contract with a 24/7 incident response firm.
- **Public Relations:** Draft a "Holding Statement" for customers/press for a data breach.
- **Legal:** Review your GDPR notification obligations (the 72-hour clock).

TOOL 4 – SEED QUESTIONS TO USE IN YOUR CO-PILOT TENANT (PRIVATE CONTAINER)

Clarifying the DSPT/CSF Approach

- *"Summarise the core logic of this DSPT/CSF approach — what is it trying to achieve?"*
- *"What assumptions underpin this approach, and which of them look weak or untested?"*
- *"Where might this approach be misaligned with the intent of the DSPT or the CSF?"*
- *"What alternative interpretations of the standard could a reviewer reasonably take?"*

Testing Evidence Quality

- *"Assess this evidence against DSPT/CSF expectations — what's strong, what's thin, what's missing?"*
- *"What would an auditor challenge in this evidence set?"*
- *"Which claims are well-supported, and which rely on inference rather than proof?"*
- *"What additional artefacts would strengthen assurance?"*

Analysing Capabilities & Gaps

- *"Based on this description, what capabilities are clearly demonstrated, and which are implied rather than evidenced?"*
- *"What gaps are likely to matter most from a risk perspective?"*
- *"Which gaps are structural (process, governance) versus operational (execution, tooling)?"*
- *"What would a realistic maturity level look like for this organisation?"*

Stress-Testing Risk Thinking

- *"What risks are under-acknowledged in this narrative?"*
- *"Which risks are overstated or not proportionate to the evidence?"*
- *"How would a regulator or external partner interpret this risk position?"*
- *"What scenarios would expose weaknesses in this control set?"*

Strengthening the Narrative

- *"Rewrite this explanation so it is clearer, more neutral, and auditor-friendly."*
- *"Highlight any ambiguous or repetitive statements that could be misinterpreted."*
- *"Suggest ways to present this capability/gap analysis more coherently."*
- *"What's the simplest, most defensible way to express this conclusion?"*

Accelerating Decision-Making

- *"What are the three most important insights from this analysis?"*
- *"If we had to prioritise action, what would be the top two areas to address?"*
- *"What would a proportionate, risk-based improvement plan look like?"*

Slido

Please scan the QR Code on the screen. This will take you through to Slido, where you can interact with us.

SCAN ME

CONVENZIS

Morning Skill Clinic

Barry Richardson
Head of Cyber Security and Information Security
NHS Blood and Transplant

Dr Avi Mehra
Associate Partner & Clinical Safety Officer
IBM

Manash Rich Ray
Head - Customer Success (UKI)
ManageEngine

Slido

Please scan the QR Code on the screen. This will take you through to Slido, where you can interact with us.

SCAN ME

CONVENZIS

Main Sponsor

zscaler™

Main Sponsor

Mike Culshaw
Security Specialist
Zscaler

Zscaler- Zero Trust Everywhere

Mike Culshaw -
Healthcare Solutions
Consultant

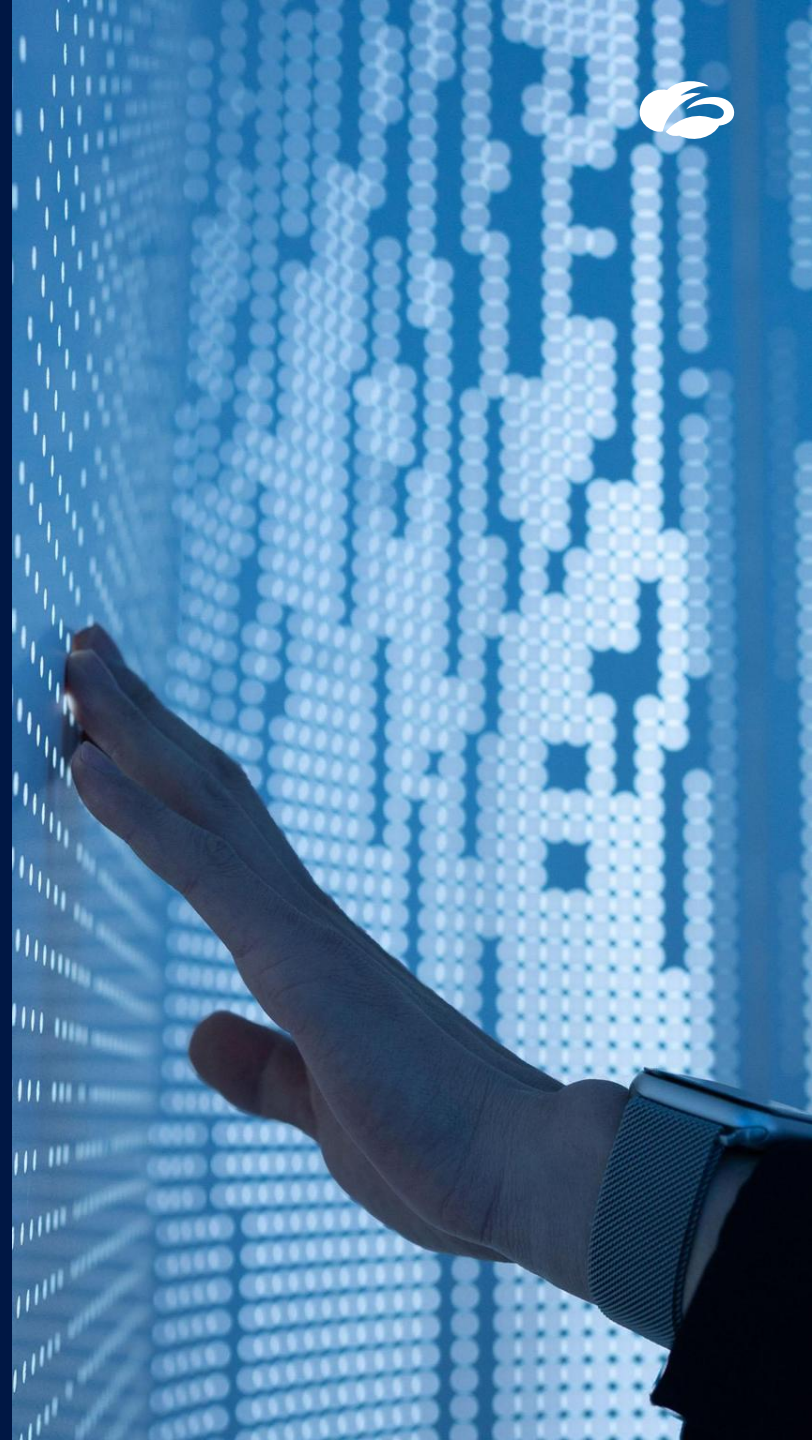
Hugo Costa -
Health Care Solutions
Consultant

2026

zscaler™

Agenda

1. Why Zscaler for a Digital Age
2. The AI Headache
3. How to Beat Hackers with Zscaler Deception
4. Zero Trust Browser - NHS use cases
5. Privileged Remote Access - NHS us
6. Questions



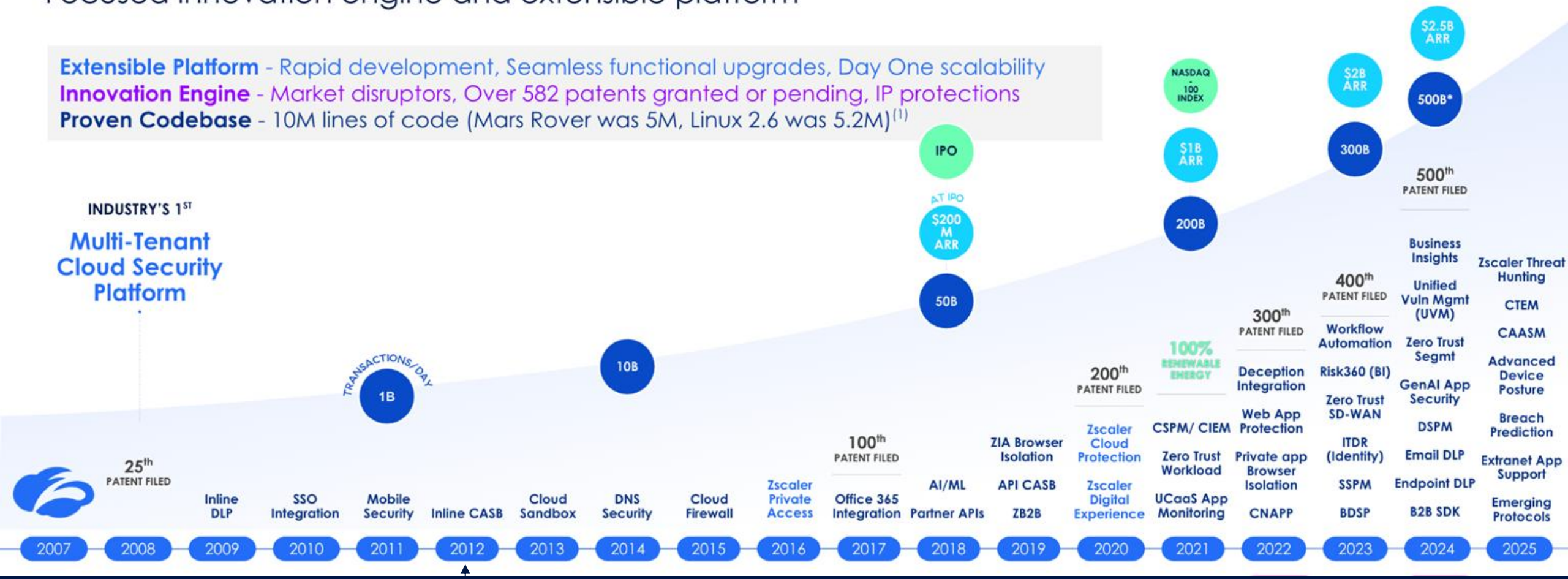
ZSCALER VISION

Any-to-Any Zero Trust Communication using business policies, not networks

Not all Zero Trust solutions are the same! - Zscaler Born in the cloud

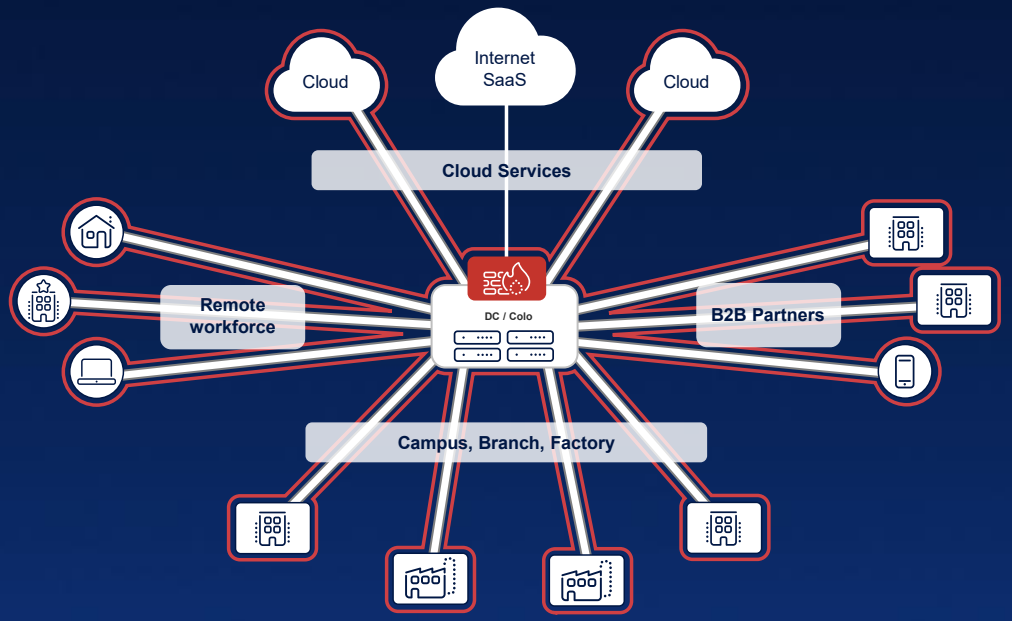
Focused innovation engine and extensible platform

Extensible Platform - Rapid development, Seamless functional upgrades, Day One scalability
Innovation Engine - Market disruptors, Over 582 patents granted or pending, IP protections
Proven Codebase - 10M lines of code (Mars Rover was 5M, Linux 2.6 was 5.2M)[1]



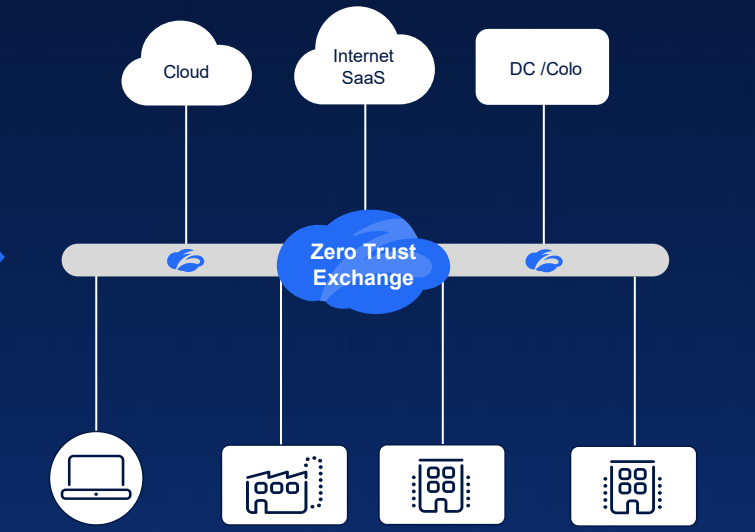
A different approach for a Digital Age

Traditional Network and Firewall Architecture



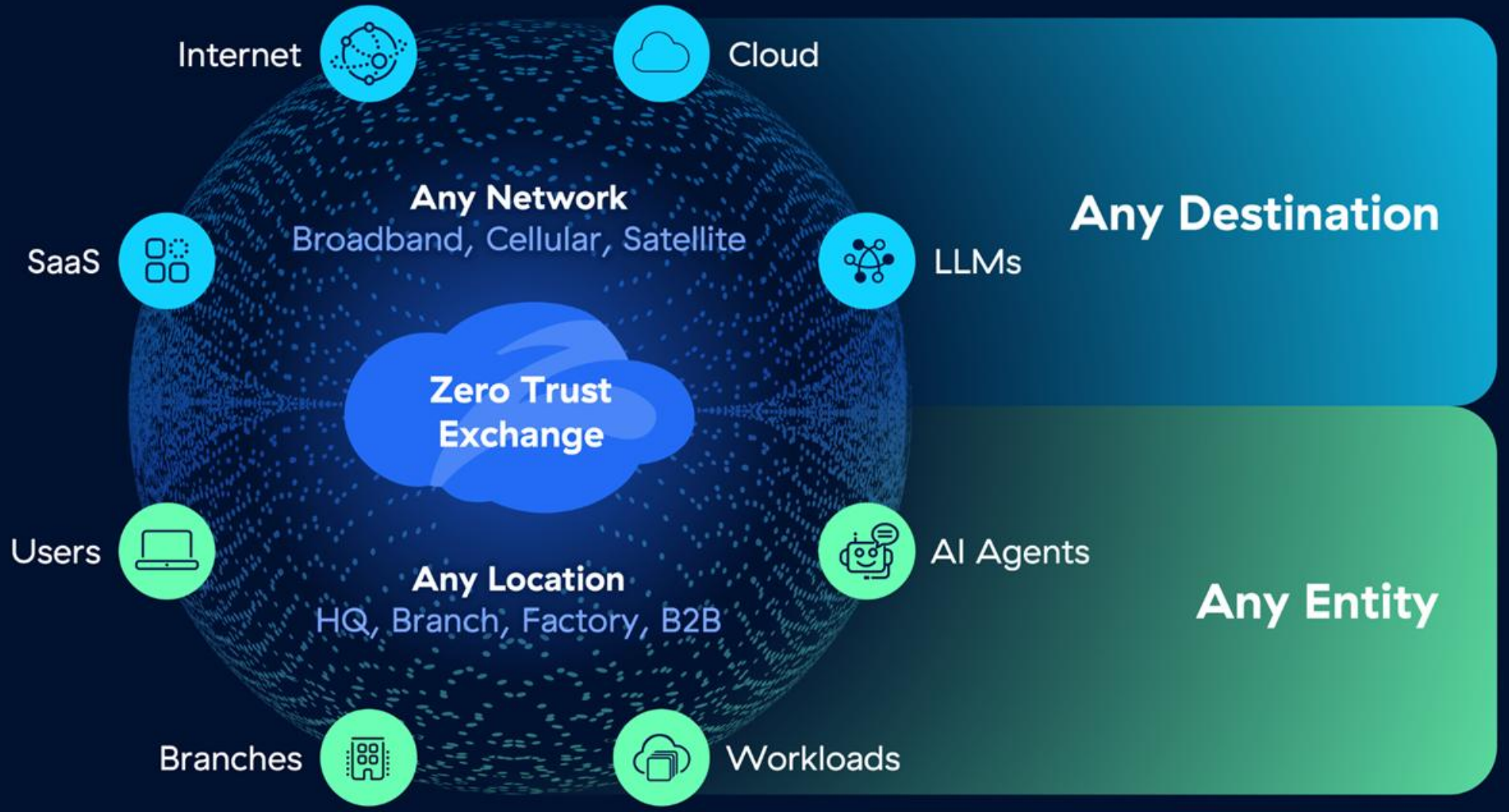
A liability
Rigid, Expensive, Security Risk

Zscaler Zero Trust Architecture



Increased Agility, Superior Security, Significant Cost Savings

Zero Trust Everywhere



AI

Friend, Foe, Disruptor or Liability?

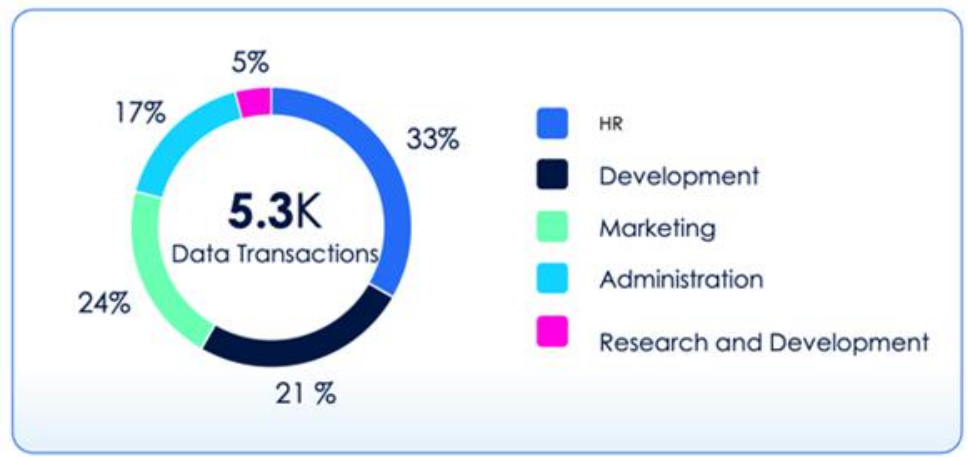
Gain Insights into Use of AI Apps

Endpoint AI Apps
AI Plugins, AI Browsers, AI IDEs

Claude CURSOR windsurf

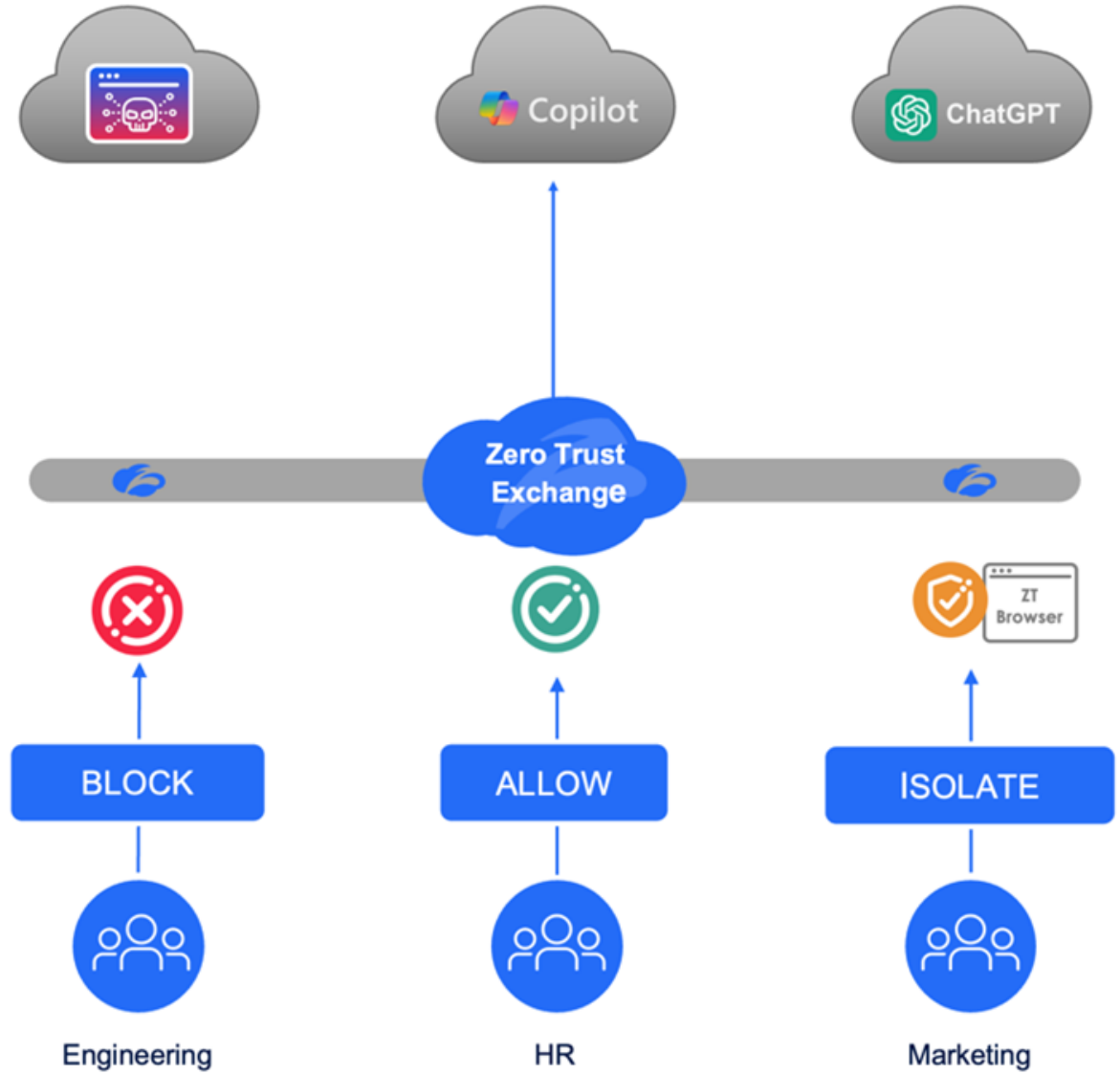
Generative and Embedded AI Apps and Usage

Know Which Departments are Using AI



Control Access to AI applications

- Block, Allow or Isolate Access to AI applications
- Coach users on appropriate use of Gen AI based on business policies
- Monitor activity and adjust policies to optimize safe use of AI

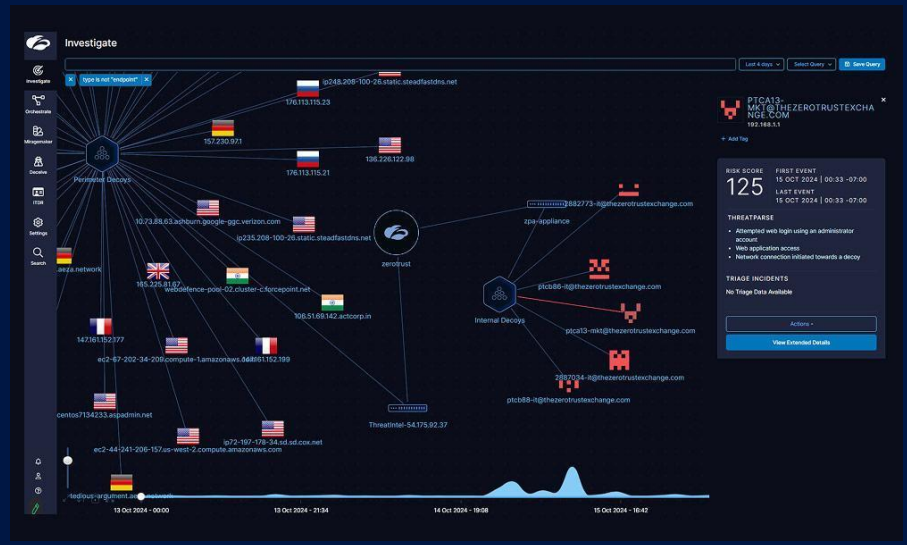


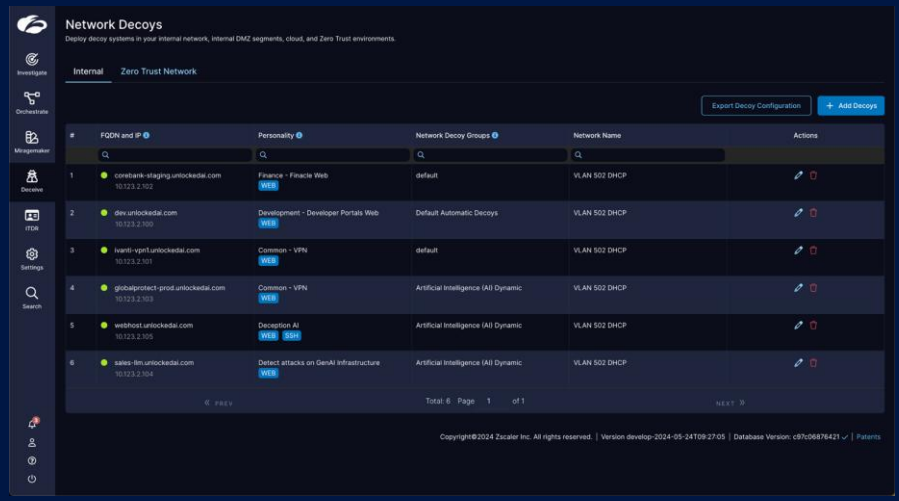
Zscaler Deception

Discover the tools and techniques hackers use

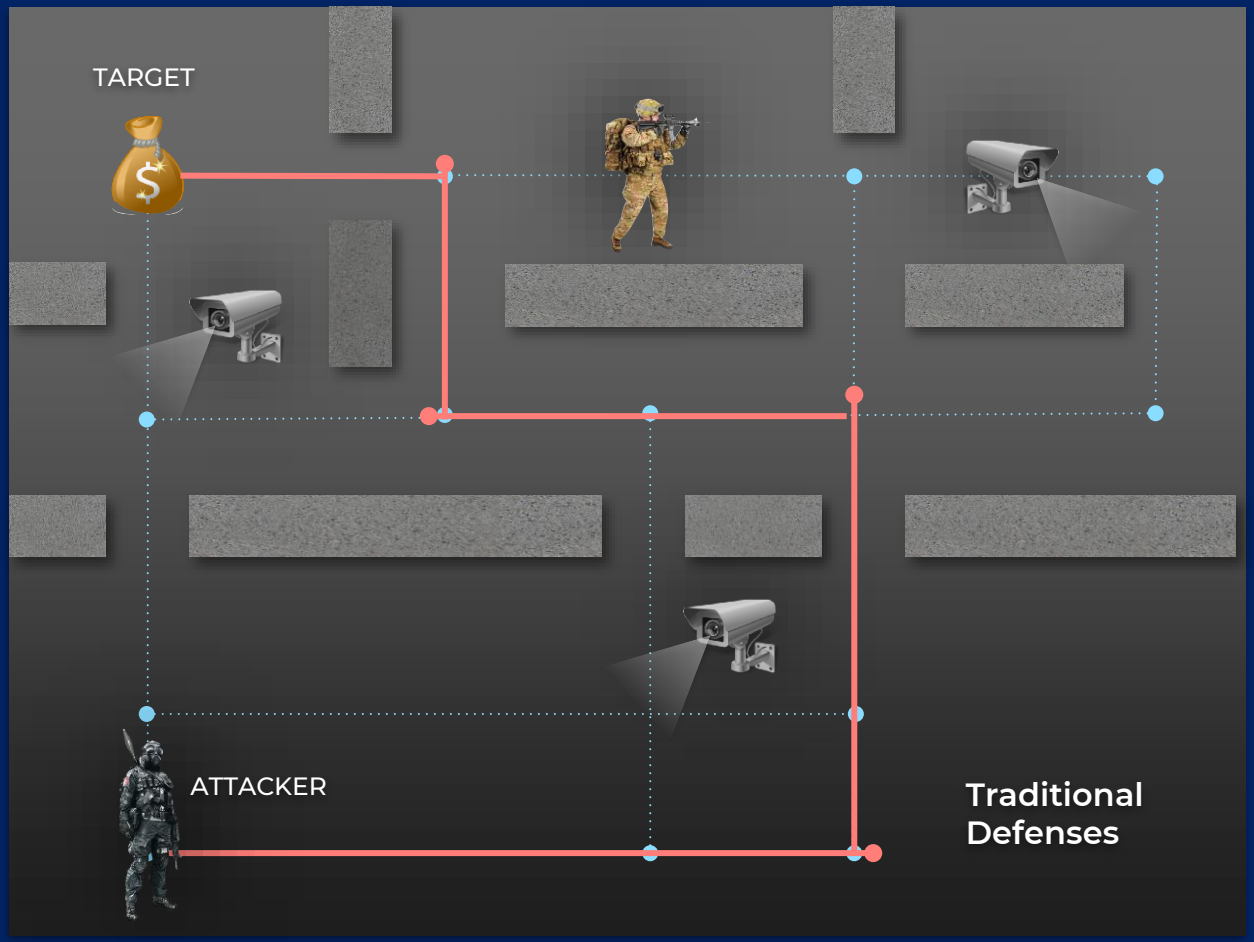
Deception

- Detect threats earlier using decoy apps, servers, users, and resources
- Add convincing fake targets to lure and intercept attackers, so they stay away from real assets
- Get instant alerts for real threats - no false positives, no operational overhead
- Deploy decoy chatbots, LLM APIs, and agents to catch AI-targeted attacks

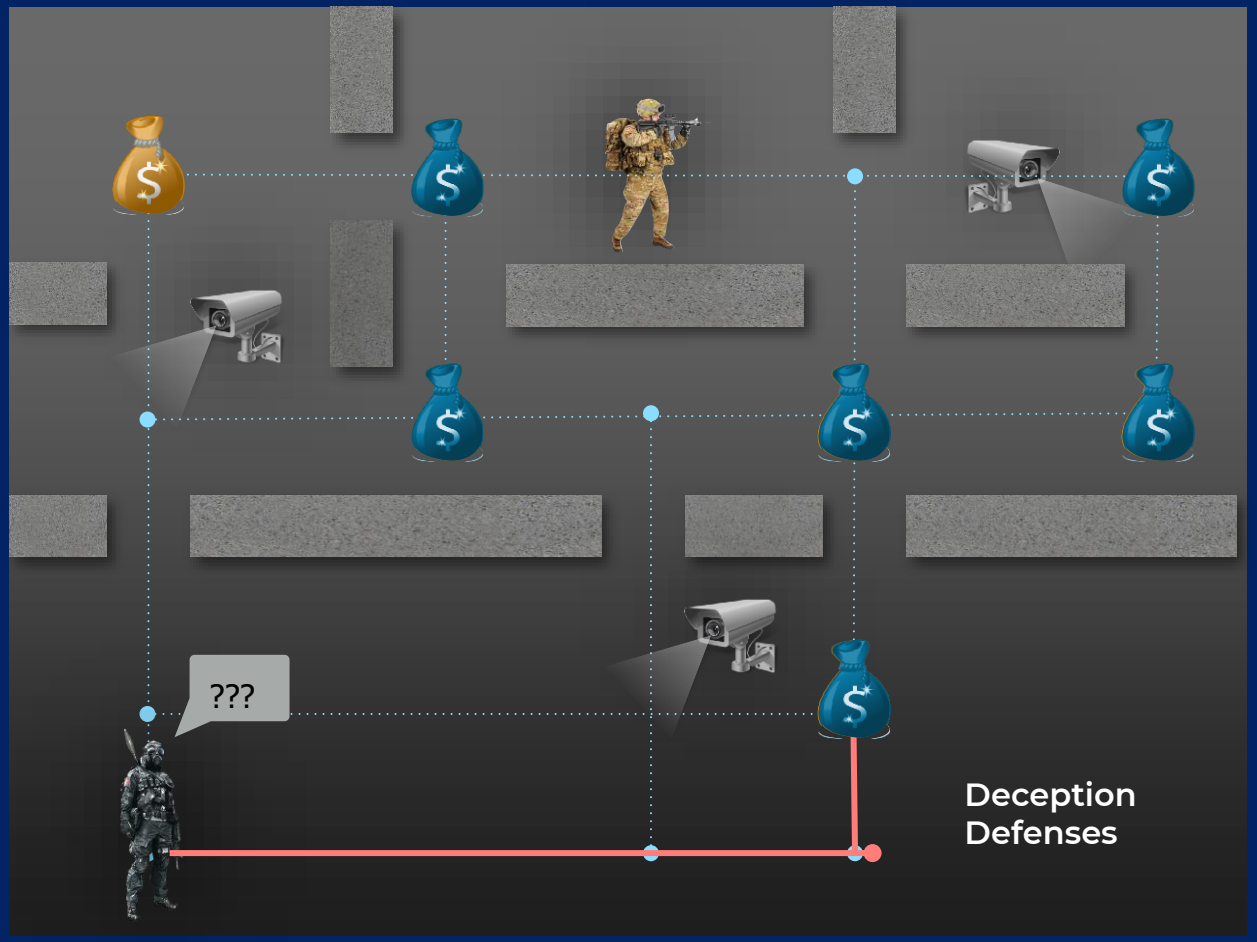




How Deception works



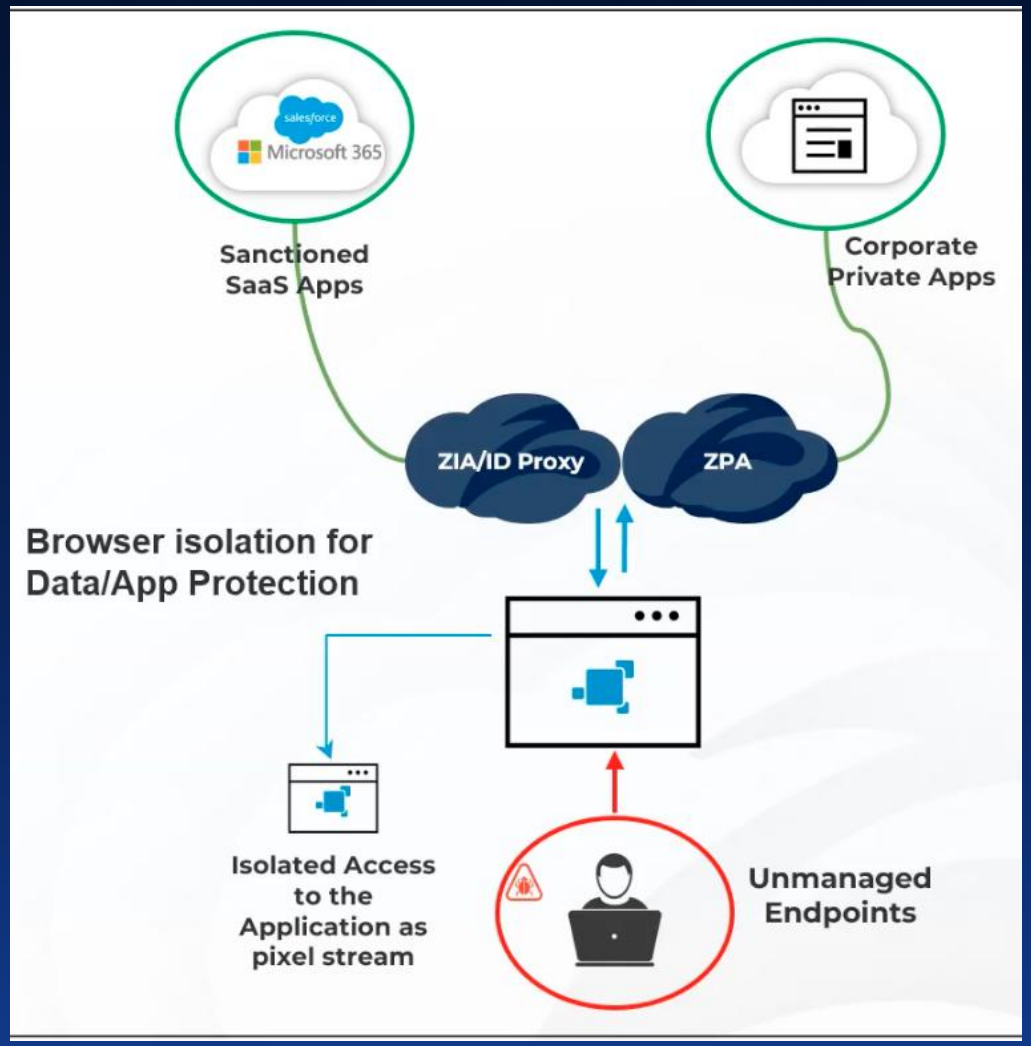
Attackers know your strategy.
Predictable defenses are easily bypassed



Decoys and traps make your environment unpredictable,
disrupt attacker playbooks

Zero Trust Browser

NHS Use Cases



- Access into Shared Care Records from unmanaged Devices

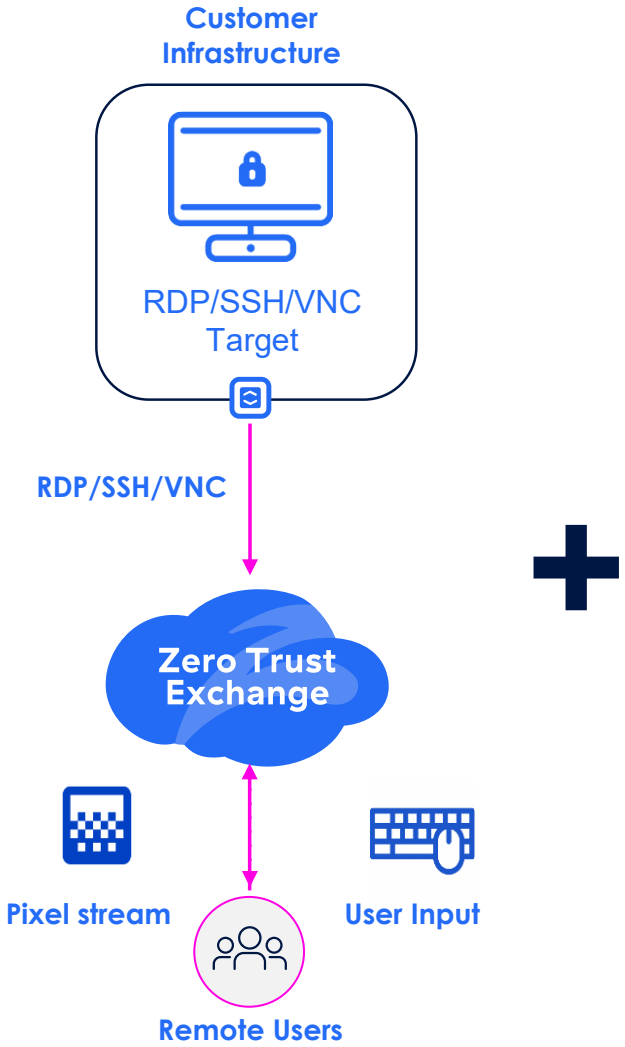
- Access into University Systems for uploading of course work

Privileged Remote Access

NHS Use Cases

Zscaler Privileged Remote Access

Clientless RDP, SSH and VNC Access with Powerful Data, Security and Session Controls



Time-bound access

- Access during an allotted window of time including business working hours constraints.

Sandboxed File Transfer

- Protect against zero-day threats and Advanced Persistent Threats (APTs) through Sandbox analysis.

Credential Vault and Mapping

- Store shared/privileged credentials of target systems in the Cloud Vault. Perform secret-less brokering using credential map policies.

Session proctoring, recording and playback

- Ushered access with control and transfer along with on-screen activity recording.

Thank you

Please visit the zscaler stand upstairs

Or reach out to
mculshaw@zscaler.com
hcosta@zcaler.com

Slido

Please scan the QR Code on the screen. This will take you through to Slido, where you can interact with us.

SCAN ME

Refreshments & Networking

CONVENZIS

Welcome to the NHS Cyber Security Conference!

25th February 2026
etc.venues, Prospero House, 241
Borough High Street, London, SE1 1GA

CONVENZIS TRAINING

Please scan the QR Code on the screen below to register your interest for our accredited training courses.

HESUK Powered by - CONVENZIS

Join the Healthcare Engagement Society (HES)

- **What it is** – A secure, year-round platform bringing NHS professionals together across six specialist communities.
- **Why it matters** – Stay connected beyond today's event, share challenges, and learn from peers facing the same priorities.
- **Your benefits** – Exclusive access to interviews, insights, best practice, and real-time discussion threads with colleagues nationwide.
- **How to join** – Simply scan the QR code, choose your community, and start connecting today.

Chair Morning Reflection

Dr Avi Mehra
Associate Partner & Clinical Safety Officer
IBM

CONVENZIS

Case Study

RAPID7

Case Study

Alex Noble
Head of Public Sector
Rapid7

25 Feb 2025

MODERNISING THE SOC: ENHANCING NHS SECURITY AND AUGMENTING CSOC CAPABILITIES BY UNLEASHING THE POWER OF EXISTING INVESTMENTS

Alex Noble

Head of UK&I Public Sector
Rapid7

Slido

Please scan the QR Code on the screen. This will take you through to Slido, where you can interact with us.

SCAN ME

CONVENZIS

Case Study

INTA FORENSICS

Case Study

Lisa Washer
Head of Cyber
IntaForensics Ltd

Case Study: Cyber Risk Lives in the Gaps

Organisational Fragmentation and Information Security in the NHS

‘Digital integration is accelerating, Governance integration often isn’t’

A Familiar Scenario

INTA FORENSICS

A shared digital platform:

- Used across multiple providers
- Hosted by a supplier
- Operationally managed by one organisation
- Accessed by many

First Questions

- Who is accountable?
- Who can suspend access?
- Who informs regulators?
- Who speaks publicly?

Cyber Risk Lives in the Gaps

INTA FORENSICS

Accountability	Governance	Capability
• Shared systems. • Distributed funding. • Split operational control. • Diffused risk ownership. • Responsibility does not match authority. • Accountability remains siloed.	• There is no unified system-level escalation pathway. • No shared real-time risk view. • No agreed joint incident command structure. • The clinical model is integrated. • The governance model is not.	• Different cyber maturity levels. • Legacy infrastructure still connected. • Patch cycles misaligned. • Variable supplier assurance. • The system is only as strong as its weakest boundary.

When systems integrate faster than governance, risk accumulates between organisations

The Board Realisation

- Each organisation compliant
- Frameworks submitted
- Risks reported locally

But:

- No system-wide risk visibility
- No cross-boundary accountability
- Compliance ≠ resilience

The Solution

INTA FORENSICS

The Problem

1. Shared systems, unshared accountability.
2. Governance built for organisations, not ecosystems.
3. Technology cannot fix structural gaps.
4. Cyber is still treated as IT risk.

The Changes Required

1. Named system-level accountable executive.
2. Unified cyber governance framework.
3. Agreed cross-organisational incident command.
4. Authority aligned with responsibility.

The Outcome

1. Faster coordinated response.
2. Clearer supplier accountability.
3. Reduced duplication.
4. Stronger Board assurance.
5. Greater transparency of interdependencies.
6. Cyber risk became visible between organisation.

Closing Reflection

In a connected NHS:

- Resilience is not determined by your strongest organisation.
- It is determined by the space between them.

And that is where cyber risk lives.

Get in Touch

Your trusted partner for Cyber Security,
Digital Forensics and Investigation services.

Web: www.intaforensics.com

Phone: 0247 77 17780

Slido

Please scan the QR Code on the screen. This will take you through to Slido, where you can interact with us.

SCAN ME

Presentation

Dr Saritha Arunkumar
Chief Technology Officer Healthcare
IBM Technology

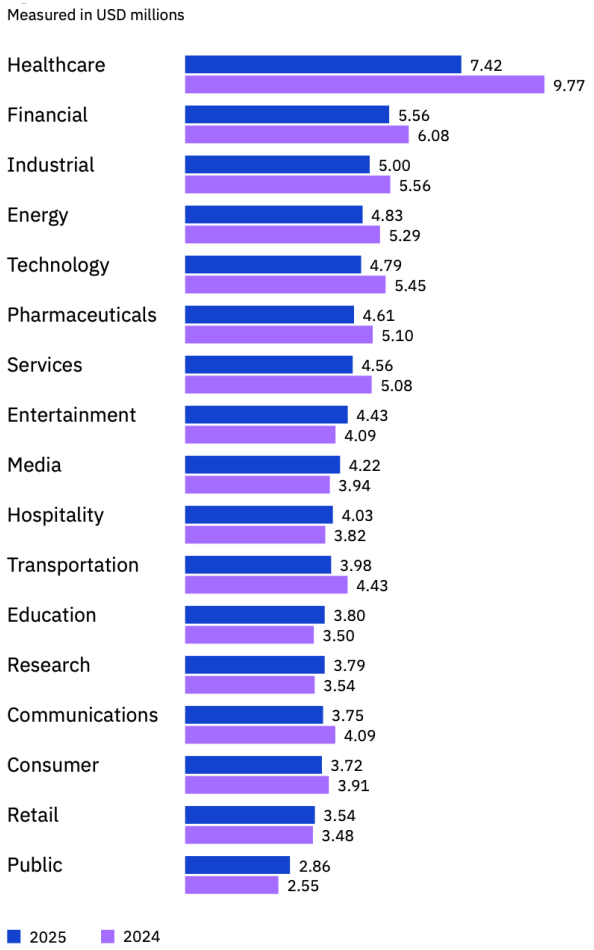
The critical need for Cybersecurity in healthcare

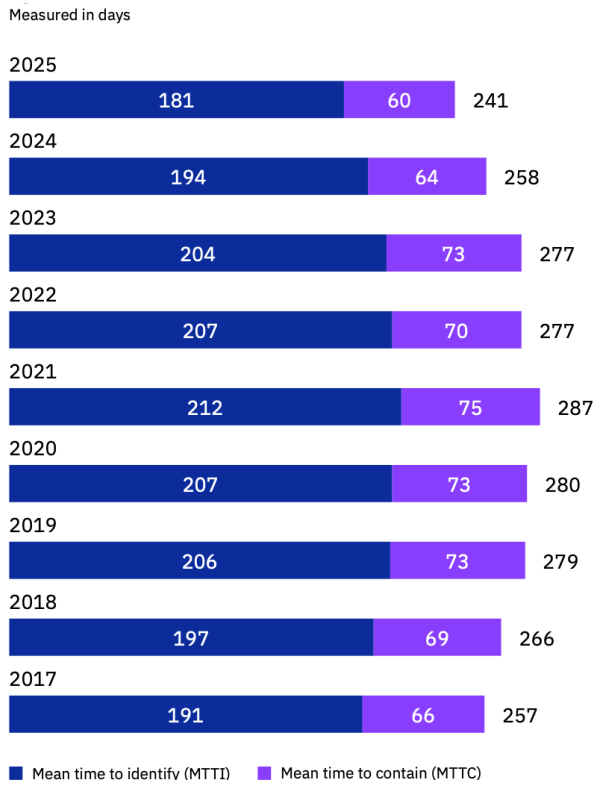
Dr Saritha Arunkumar
CTO for Healthcare– IBM Technology
Master Inventor

Cost of a Data Breach Report 2025

Healthcare remained the most expensive industry for breaches

At USD 7.42 million, healthcare recorded the highest average breach cost among industries for the 12th consecutive year—even as it saw a sharp reduction from last year (USD 9.77 million). Attackers continue to value and target the industry's patient personal identification information (PII), which can be used for identity theft, insurance fraud and other financial crimes. Healthcare breaches took the longest to identify and contain at 279 days. That's more than five weeks longer than the global average.





4.4M

The global average cost of a data breach, in USD, a 9% decrease over last year—driven by faster identification and containment.

97%

Share of organizations that reported an AI-related security incident and lacked proper AI access controls.

63%

Share of organizations that lacked AI governance policies to manage AI or prevent the proliferation of shadow AI.

1.9M

Cost savings, in USD, from extensive use of AI in security, compared to organizations that didn't use these solutions.

[Cost of a Data Breach 2025 full report]

X-Force Threat Intelligence Index 2026 - Released 25th Feb 2026

Top trends in this year's report

44%

Increase in the exploitation of public-facing applications

X-Force observed a rise in the exploitation of public-facing applications due to weaknesses in software pipelines and third-party components. Of the nearly 40,000 vulnerabilities that were tracked, over half required no authentication to exploit, making vulnerability exploitation the top driver of incidents.

56%

Percentage of vulnerabilities that didn't require authentication to exploit

The number of vulnerabilities tracked by X-Force approached 40,000 and over half didn't require authentication. This signals a weakness in software secure-by-design implementation. Attackers are finding success without using credentials, multi-factor authentication (MFA) bypass or even end user interaction.

>300K

Number of ChatGPT credentials observed for sale on the dark web

Infostealer malware enabled the exposure of ChatGPT credentials, demonstrating that AI platforms have reached the same credential risk as other core enterprise SaaS solutions. The trend indicates organizations are accumulating sensitive authentication data on inadequately secured systems.

~4X

Increase in major supply chain or third-party breaches over 5 years

Attackers exploit software supply chains' fragility. Major incidents increased nearly 4X in 2025
as attackers target developer trust, automation workflows and cloud interfaces. Sprawling third-party dependencies create hard-to-secure attack surfaces, where one weak link can expose many targets. AI-driven tools may further pressure supply chains in 2026.

49%

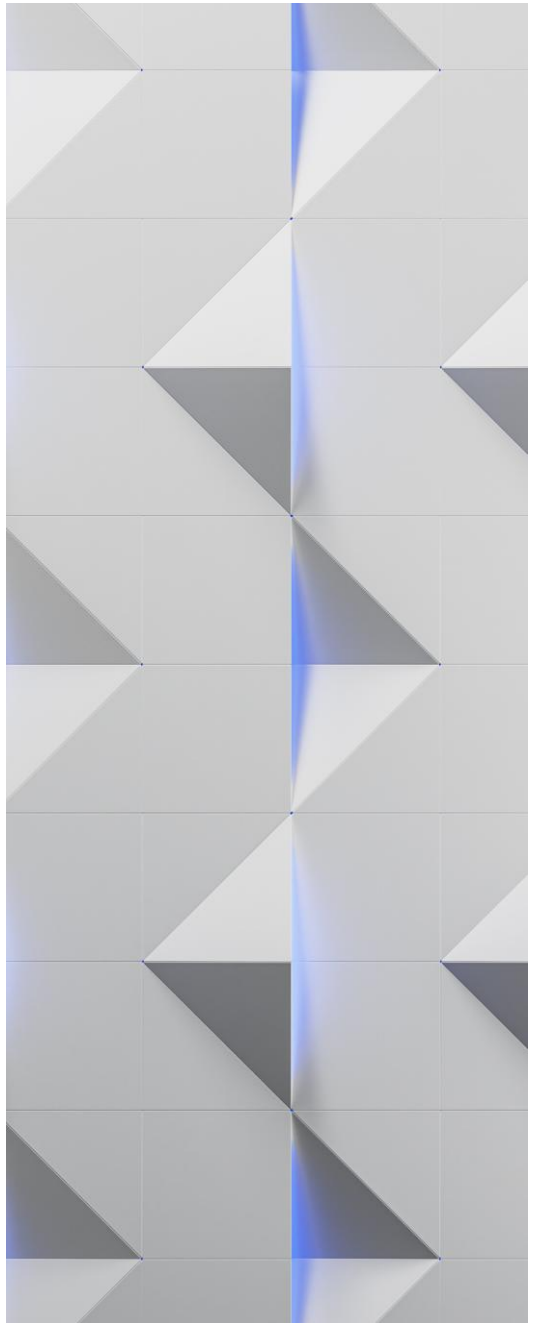
Increase in active ransomware groups compared to 2024

Fragmentation continues, with 109 ransomware extortion groups identified by X-Force in 2025, up from 73 in 2024. This increase reflects a lower barrier to entry as threat actors reuse leaked tools, follow playbooks, or shift identities, enabling small operators to conduct opportunistic, low-volume attacks.

#1

Manufacturing was the top-targeted industry

The manufacturing sector accounted for 27.7% of incidents, up only slightly from 26% last year. This figure is only a few tenths of a percent higher than the finance and insurance sectors, which accounted for 27% in 2025 and 23% in 2024.



71%

of organizations say decisions must be made faster and more frequently.[1]

Gartner

80%

of organizations rely on stale data for decision-making[2]

businesswire
A BERKSHIRE HATHAWAY COMPANY

85%

of data leaders cost their company money with stale data[3]

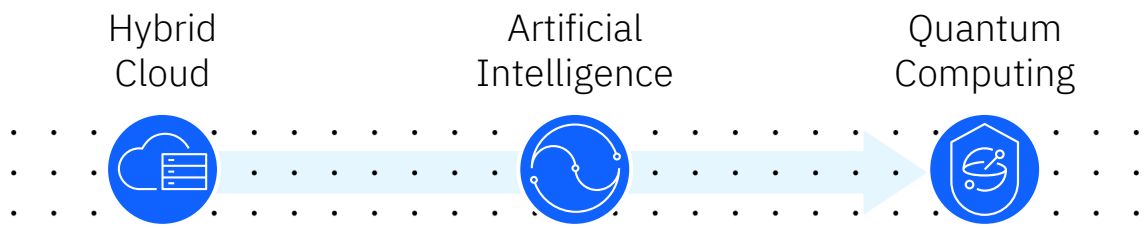
Agility PR Solutions

Data Security Challenges

Rapid business and technology innovation leaves critical data unprotected

Traditional methods of data protection must evolve to protect data in the cloud, in AI, and in the Quantum era

Technology innovations drive an expanded threat surface



To simplify data protection in the future, a shift from point products to a data security platform is happening

Compliance challenges

1000's of hours preparing for audits with existing regulation complexity

New regulations are expected to address AI usage and eventually cryptographic risks posed by Quantum

Data Exposure

Cloud and Generative AI adoption has created a loss in visibility of where data is stored, who has access, and how it is protected

Traditional encryption will be exposed enabling "Harvest now, decrypt later" strategy

AI Risks

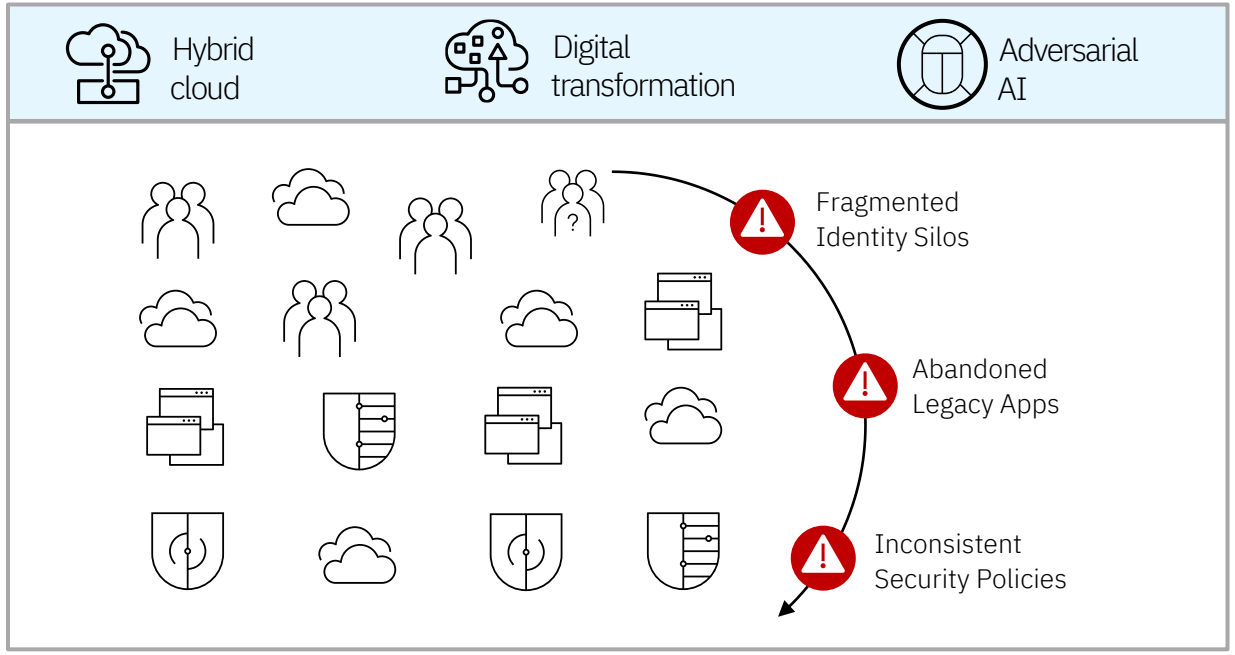
Generative AI creates a new threat surface — training and fine-tuning data, models and applications — that must have a security and governance lifecycle to protect against risks (e.g., shadow AI, data poisoning, model evasions etc.)

Security posture

Organizations are struggling with visibility, a way to prioritize risks, and how to address security gaps across a spectrum of use cases — from shadow data, shadow AI to cryptographic posture — where data can be exposed; Siloed tools exacerbate this problem

IBM

IT modernization leaves organizations managing fragmented cloud and legacy solutions



Inconsistent User Experience

Different IAM solutions have different capabilities, making consistent policy and authentication impossible

Elevated Identity Risk and Drift

Disconnected identities lead to a fragmented view of user behavior across the enterprise and unintentional access exposure

Expensive Management

Teams lack the ability and budget to manage policy and compliance across IAM stacks, abandoning protection for legacy apps

Compliance challenges

Too much time and resources spent preparing for security audits, and to aligned with compliance frameworks such as SOX, GDPR, HIPPA, NIST, FISMA, NERC. Innumerable hours spent on certifying user access, and enforcing the Principle of Least Privilege and Separation of Duty

Rapid innovation is leaving critical enterprise data exposed

Hybrid Cloud

Data is sprawling across hybrid cloud platforms

What to focus on

- Build an accurate inventory of sensitive data, whether structured or unstructured, across on-premise and cloud
- Scan data environments for vulnerabilities and prioritize remediation efforts
- Automate compliance tasks to reduce manual effort and support audit-readiness
- Monitor how users access data and flag risky behavior

Rapid innovation is leaving critical enterprise data exposed

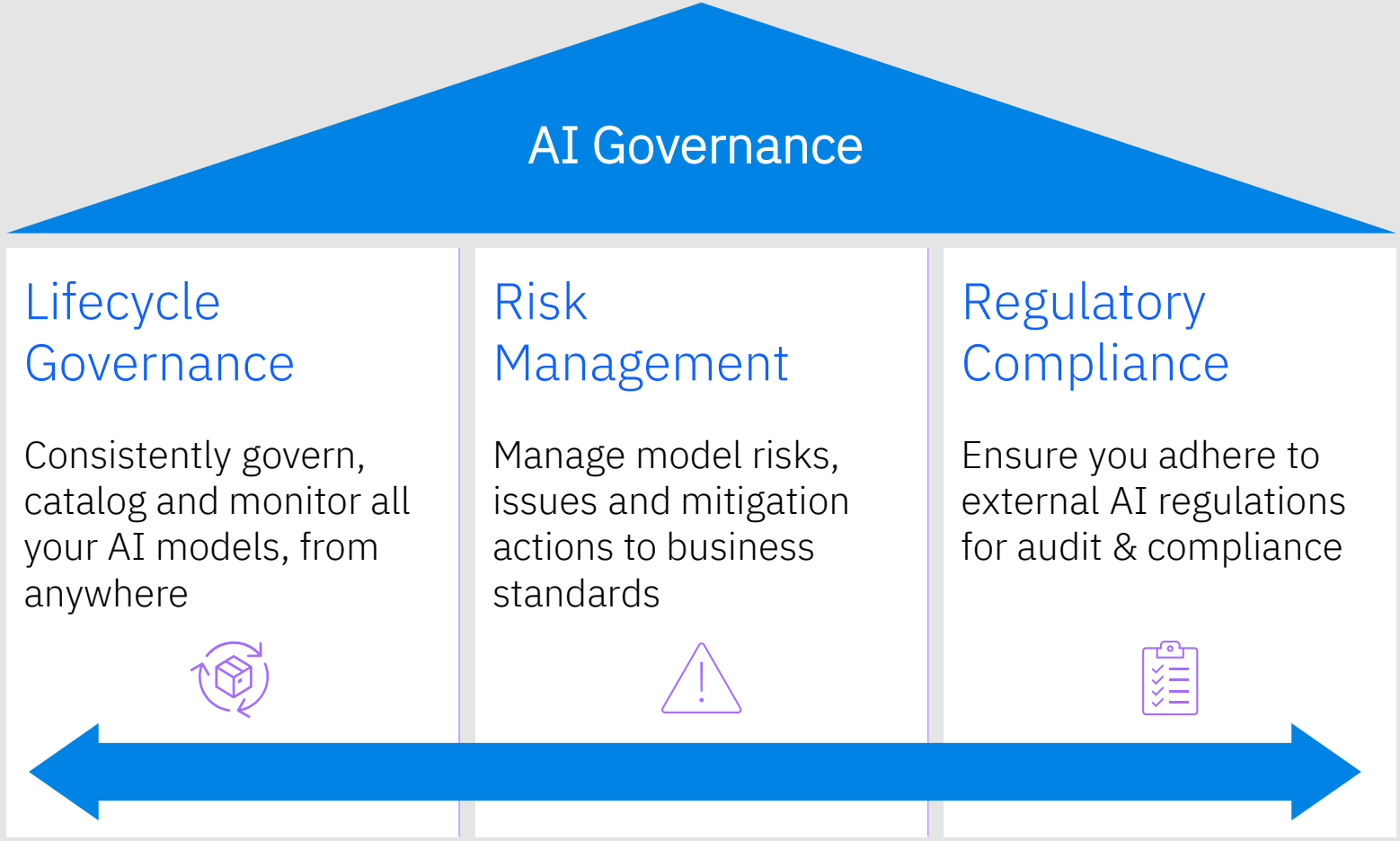
AI

AI is the new, often unprotected, attack surface

What to focus on

- Identify all AI models in use, including what data they rely on and where they run
- Prevent sensitive data exposure and runtime attacks using policies and guardrails
- Apply consistent security policies across AI projects
- Integrate governance tools and processes to manage risk and comply with emerging regulations

Three pillars of AI governance



Rapid innovation is leaving critical enterprise data exposed

Quantum

Quantum computing will break current encryption

What to focus on

- Take inventory of all cryptographic assets and assess your risk posture
- Prioritize and upgrade weak or outdated encryption – especially those vulnerable to quantum threats
- Centralize and automate key and certificate lifecycle management
- Adopt a crypto-agile strategy that supports fast adoption of new encryption standards

You can’t secure what you don’t know exists

Discover your sensitive data

- Database: MongoDB, ORACLE, MySQL, IBM Db2, elasticsearch
- Cloud: aws, Azure
- SaaS: salesforce, slack, Jira, workday, Office 365
- DBaaS: snowflake, databricks

Understand your data

Build an asset inventory

- Discover structured & unstructured data
- Classify how sensitive it is
- Map to regulations and policies
- Compile this to a central inventory

Explain data for compliance

- Who and what is accessing your data?
- What have they done, and what *can* they do?
- Who has privileged entitlements to sensitive data?
- What controls are in place on this data store?
- When did this change take place and who performed it?

Security Culture

Leadership

Leader's Intent

Fusion Team

Incident Command

Accountability

Cyber Safety Training
- At Work
- At Home

What Why How

Communication

PACE Model
- Primary
- Alternate
- Contingency
- Emergency

Break the Glass
- Runbooks with Dual Verification

Orchestration & Automation

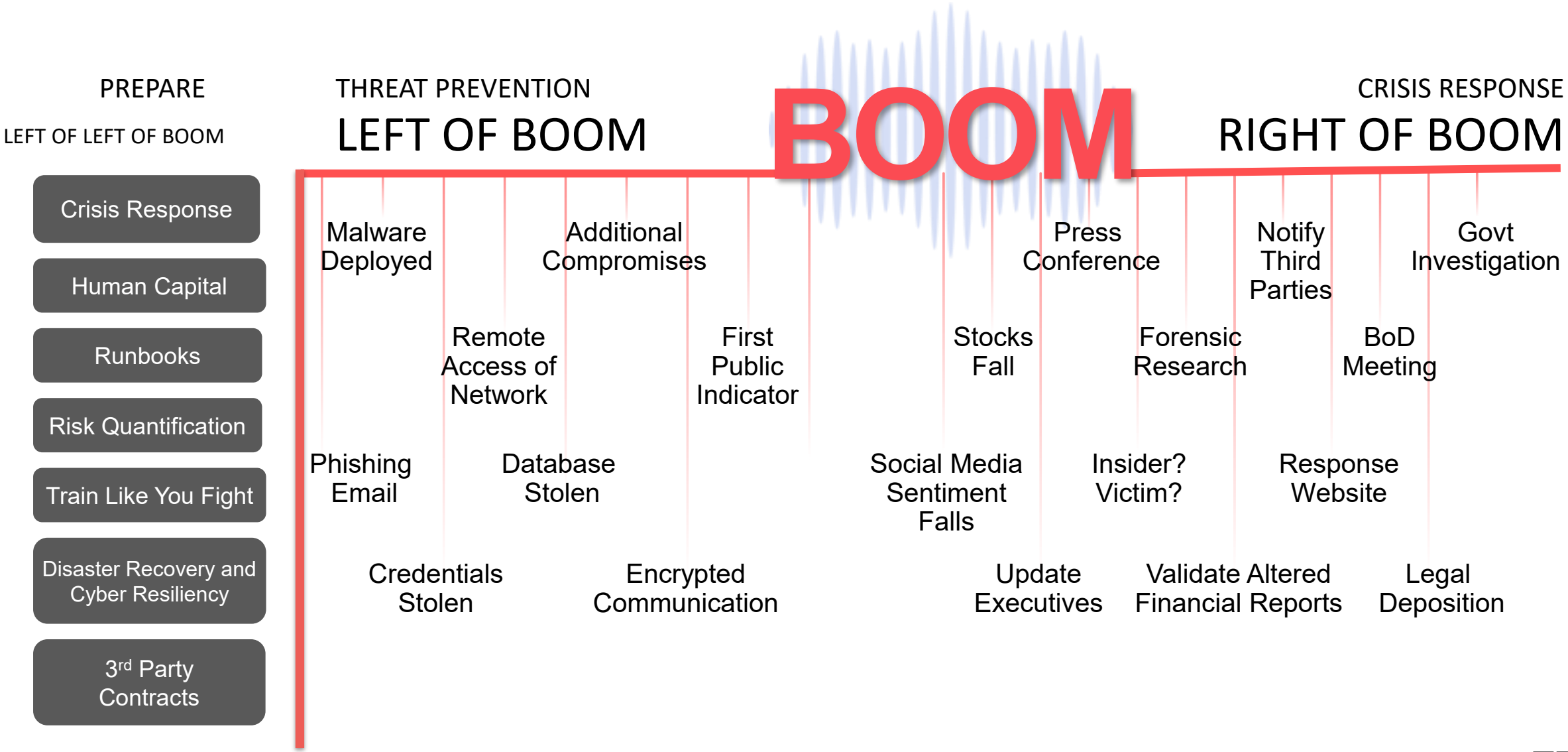
Policies

EISP – Enterprise Information Security

SysSP – System Specific Policies

ISSP – Issue Specific Security Policies

How to be better prepared for Cyber attacks



Recommendations

Here are the actions your clients can take right now to defend against the threats highlighted in this report

Prepare for AI-Enabled Threats

Refresh threat models, to accommodate for the new wave of AI enabled threats. This often relates to the need to adapt to a higher volume of autonomous attacks such as spear phishing. To address this, consider the use of Agentic AI-powered digital workers to prepare, prevent and respond to stay ahead of fast, AI-powered attacks.

Shift left with strong risk based exposure management, secure-by-design practices and identity-aware development to limit attacker opportunities.

Monitor identities with AI

Treat identity as a perimeter asset, as attackers are increasingly exploiting human identities through deepfakes, system identities through stolen credentials, and agent identities through compromised tokens.

Use AI-powered identity threat detection and response (ITDR) and posture tools to help spot risks and prevent attacks.

Elevate identity systems to the same level of resilience, governance and monitoring as core infrastructure components.

Accelerate data security

Reinforce proper data protection controls by discovering and classifying sensitive data, enforcing safeguards, and meeting regulatory requirements to secure information used in AI workflows and digital operations.

Prepare for the post-Quantum Era to maintain data security and integrity for critical networks and applications.

Shift to Continuous Security

Adopt a Secure-by-Design culture with a continuous, proactive approach to identifying weaknesses across environments.

Conduct regular penetration testing across the full technology stack.

Continuously assess exposures and automatically remediate and scan code, credentials, and configs on hybrid cloud environments.

Prioritize AI Platform security

Enforce strong access controls, protect credentials, and monitor for misuse of AI applications.

Use traditional and modern technologies to protect against sensitive data leakage and protect intellectual property.

Employ AI security and Governance to test, secure, and ensure the trustworthy use of AI across build and consumption.

Track your Exposure footprint

Continuously identify exposed assets across the enterprise hybrid cloud environment by using solutions that monitor your attack surface, deep, and dark web along with other external sources.

Leverage data from attack surface management tools, to proactively reduce your footprint.

Embed AI security Governance

Strengthen the security governance model to align with the AI security strategy and the enterprise-wide AI-driven transformation.

Adopt adaptive security governance capabilities that use Agentic AI-powered digital workers to continuously discover and address requirements, manage control-environment changes, and reduce security-risk exposure across the digital ecosystem landscape.

Apply enforcement controls to meet regulatory obligations and broader requirements to support security-risk remediation and oversight.

Key Takeaways

- Have a Cyber Crisis Management Plan with:
  - Team Roles & Responsibilities, RACI charts
  - Leader's Intent
  - Crisis Qualification Criteria
  - Incident Escalation & Activation process
  - Deactivation Criteria
- Have executive-level Playbooks based on specific roles or scenarios such as:
  - HR / Legal /Comms
  - "Executive Ransomware Response" or "Sensitive Data Breach"

- Ensure DRP prioritizes critical business processes
- Ensure BCP considers IT continuity
- Drive "top down" culture of cyber awareness
- Establish Zero-Trust architecture
- Implement MFA
- Effective Asset Inventory
- Security Awareness Training with:
  - Public Media Policies/Training
  - Conduct Phishing tests and have a reporting process

IBM

Thank you

Dr Saritha Arunkumar

Slido

Please scan the QR Code on the screen. This will take you through to Slido, where you can interact with us.

SCAN ME

CONVENZIS

Case Study

CROWDSTRIKE

CONVENZIS

Case Study

James Burchell
Sales Engineer Manager
CrowdStrike

Beyond the AI Buzz: *What Adversaries Are Really Doing to Healthcare Organisations*

James Burchell

Sales Engineering Manager

Slido

Please scan the QR Code on the screen. This will take you through to Slido, where you can interact with us.

SCAN ME

Lunch & Networking

Chair Afternoon Address

Dr Avi Mehra
Associate Partner & Clinical Safety Officer
IBM

CONVENZIS

Case Study

BlueFort Security

Case Study

Josh Neame
Chief Technology Officer
BlueFort Security Ltd

Peter Batchelor
Regional Sales Director
Silverfort

BlueFort Security

Silverfort

Securing Human and Non-Human Identities to comply with NCSC CAF Requirements

NHS

Who Are We?

Peter Batchelor

Regional Sales Director

Peter brings extensive experience in enterprise security solutions and client relationship management. He specialises in helping NHS organisations navigate complex cybersecurity challenges and align security initiatives with strategic business objectives.

Josh Neame

Chief Technology Officer

Josh leads technical strategy and innovation efforts, ensuring BlueFort delivers cutting edge security solutions. His expertise spans identity management, cloud security, and infrastructure protection across diverse environments.

Thank you

BlueFort
Security

Slido

Please scan the QR Code on the screen. This will take you through to Slido, where you can interact with us.

SCAN ME

Interactive Workshop

Nasser Arif
Award Winning Cyber Security Manager
London Northwest Healthcare NHS Trust and The Hillingdon Hospitals NHS Foundation Trust

What Would a ‘Hacker’ Do?

Practical Cyber Habits for Everyday NHS Life

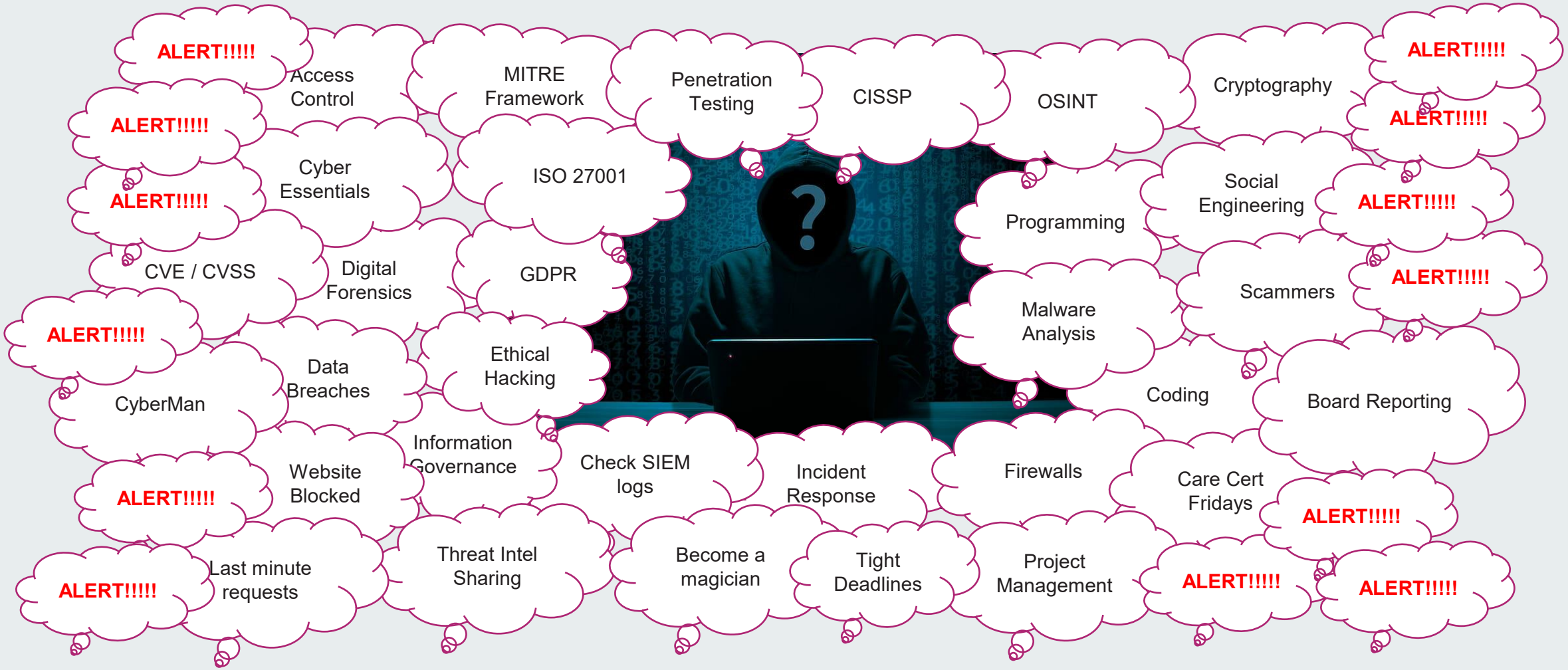
Nasser Arif

MEng (Hons), CISSP

Cyber Security Manager, NHS

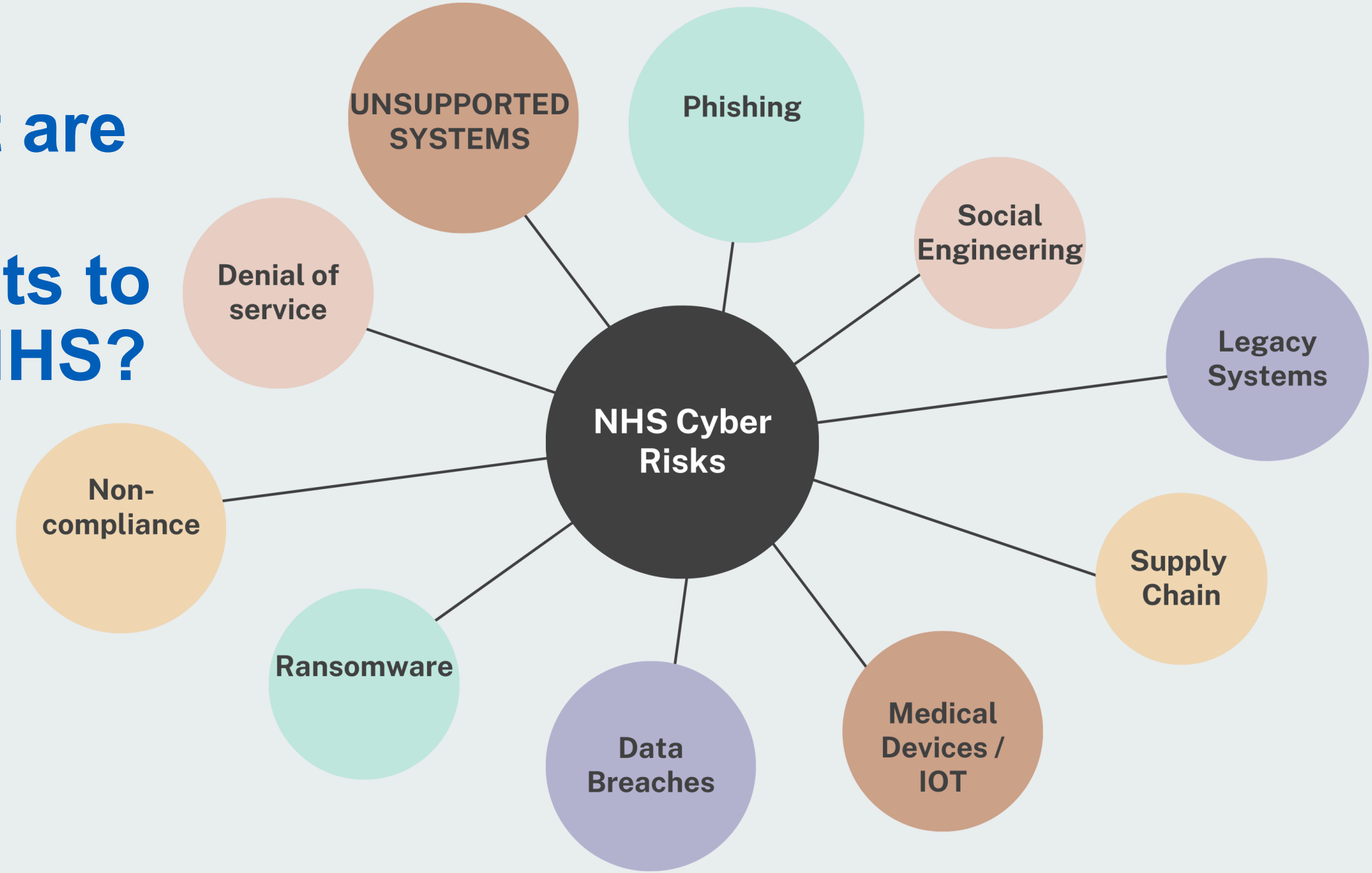
National Cyber Award Winner

(Views / opinions are my own)



What do we do in NHS Cyber Security?

What are the threats to the NHS?



NHS Data Security and Protection Toolkit

#Compliant

NHS suppliers urged to sign cyber security best practice charter

CYBER SECURITY, NEWS

16 May 2025

Credit: Shutterstock.com

Source: Digital Health

CYBER ESSENTIALS

Cyber Security and Resilience (Network and Information Systems) Bill

Government Bill

Originated in the House of Commons, Session 2024-26

Source: Gov UK, NCSC

ARE YOU COMPLIANT?

Not achieved	Partially achieved	Achieved
At least one of the following statements is true.	All the following statements are true.	All the following statements are true.

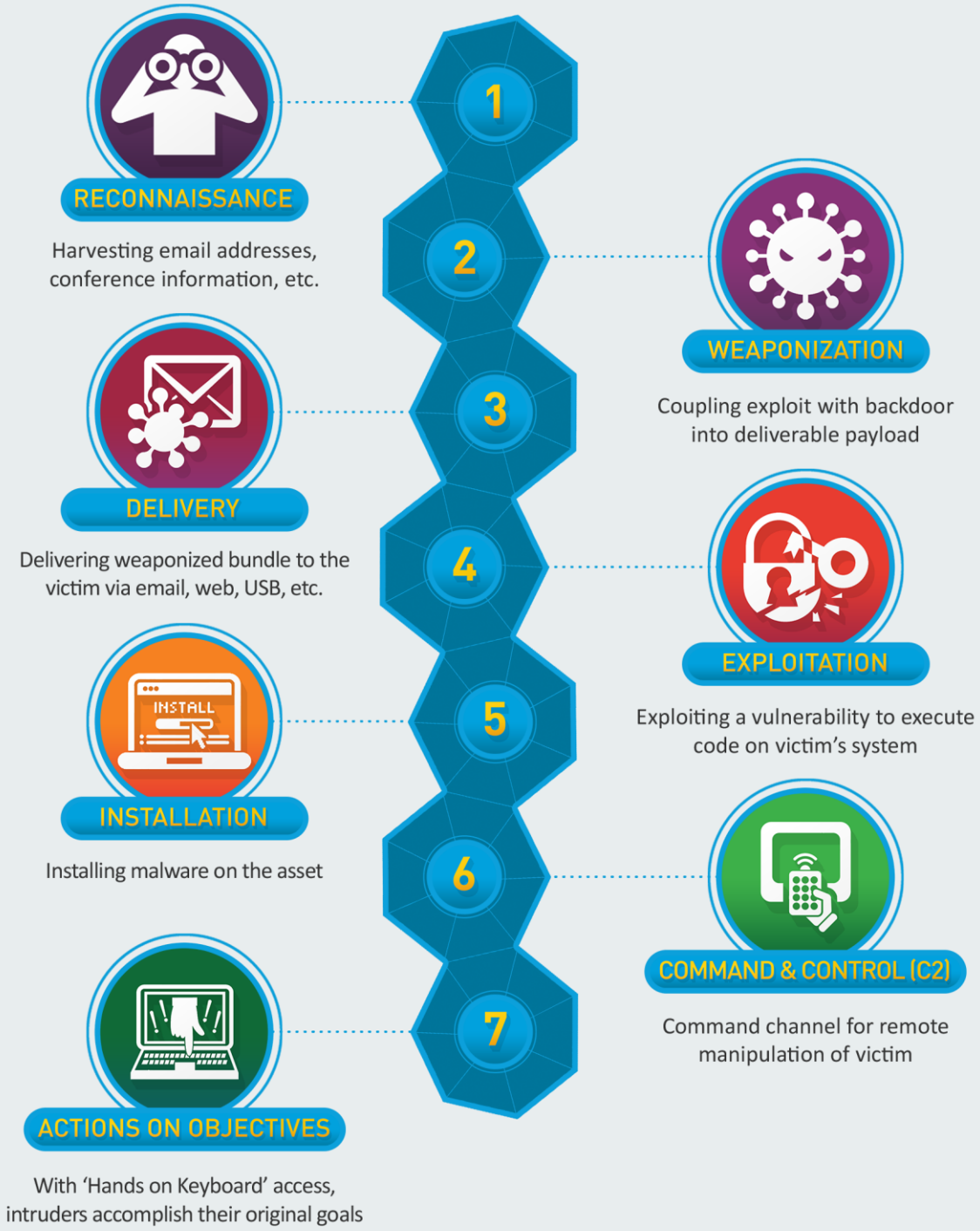
Source: DSPToolkit

The Human Link…

- Recent high-profile incidents exploited human behaviours.
- Social engineering / Phishing still being seen as entry points.
- Our fear of missing out, emotions and predictable behaviours put us at risk.

Cyber Kill Chain

(Source: Lockheed Martin)



Phishing

E-mail Phishing	Voice Phishing (Vishing)
SMS / Messenger Phishing (Smishing)	QR Code Phishing (Quishing)
Spear Phishing (specific targets)	Whaling (high profile targets)

Finding your inner cyber defender and having a ‘hacker’ mindset

What can we do?

Take control of your digital presence!

&

Become your own auditor!

E-mail: The ‘Skeleton Key’ of online accounts

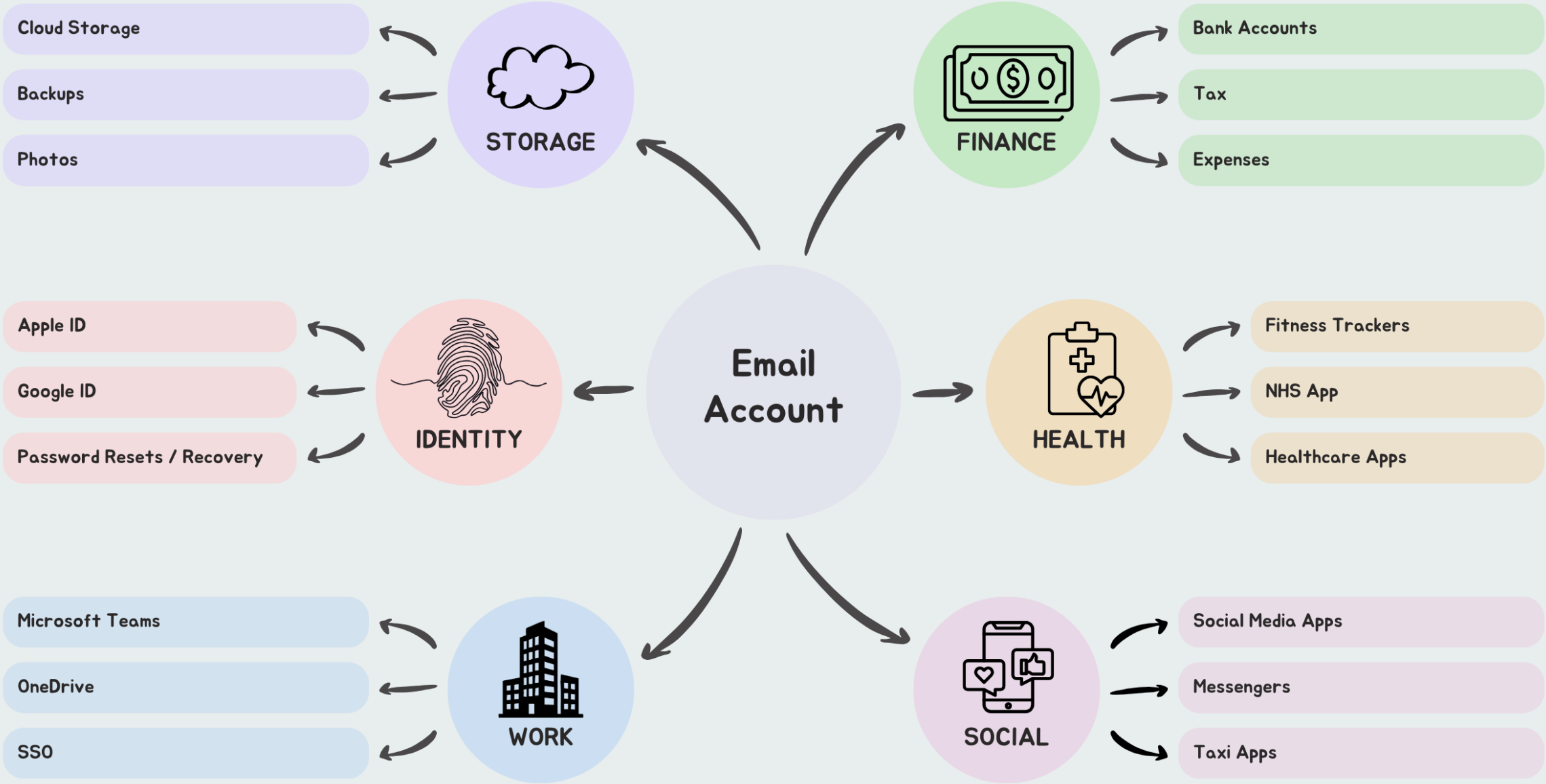
Backbone of all our online accounts.

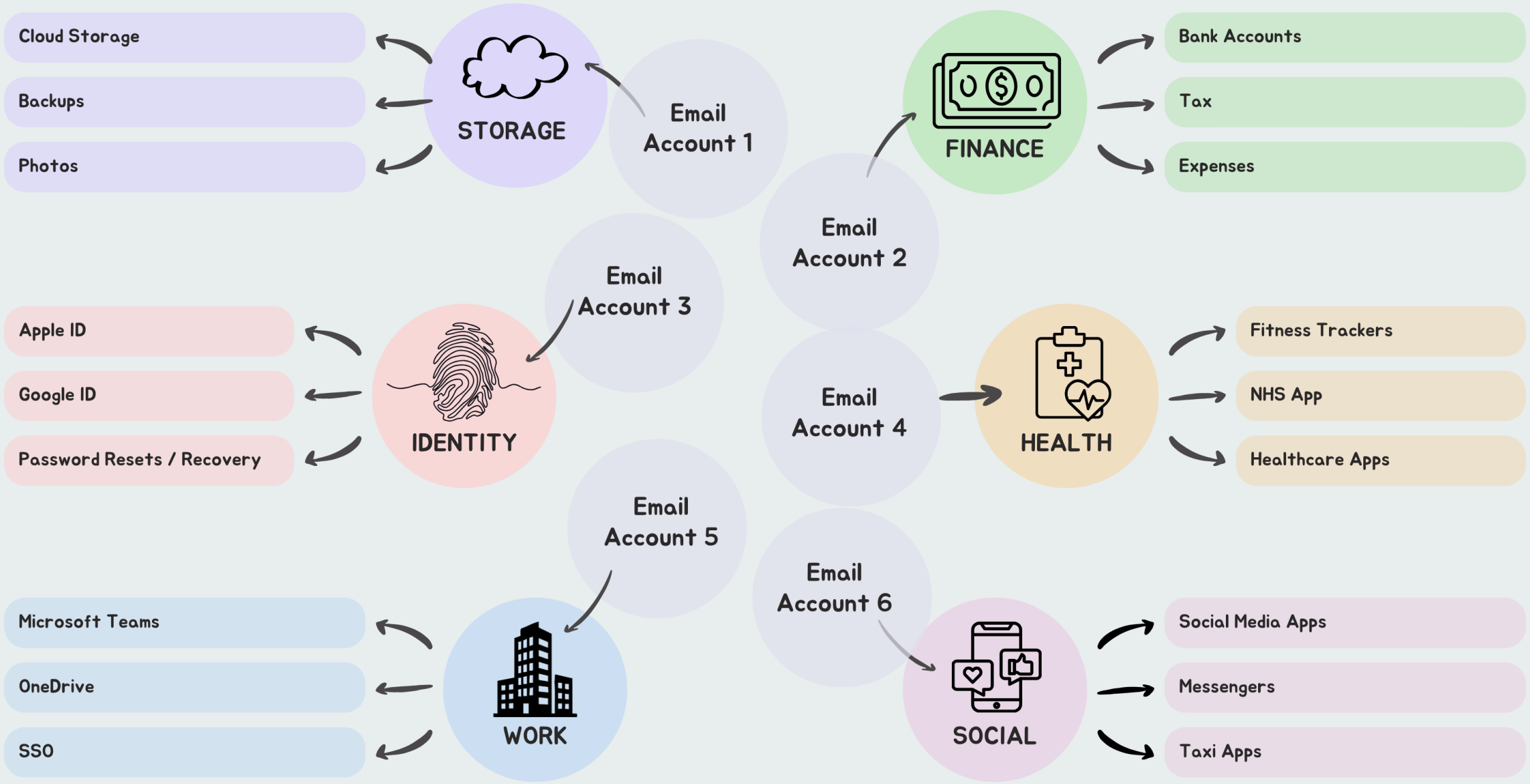
Both work and personal accounts must be protected.

Gateway to your digital identity.

Often used to breach online banking, social media etc.

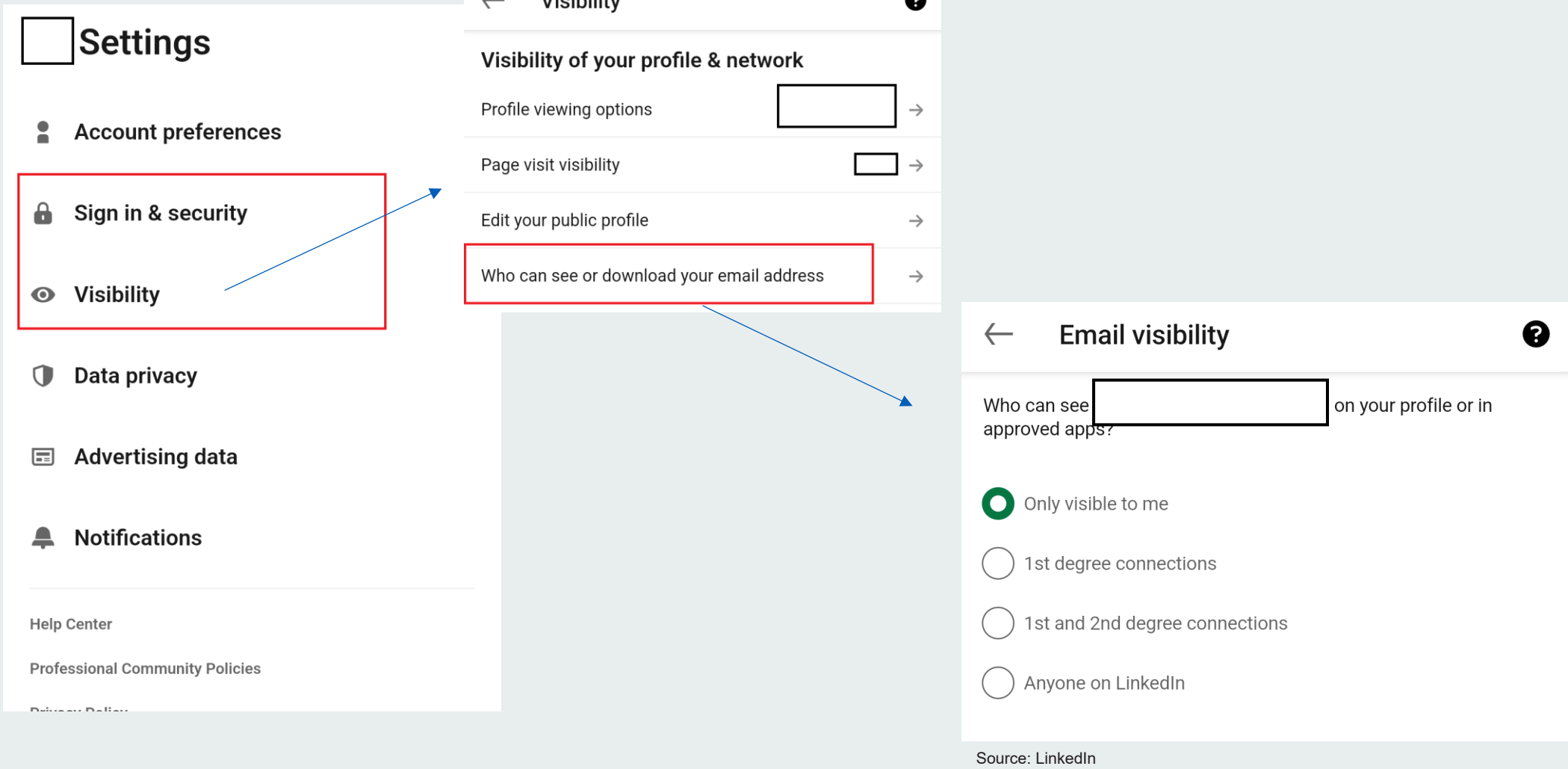
Used by threat actors for persistence.


Email Account
STORAGE
Cloud Storage
Backups
Photos
FINANCE
Bank Accounts
Tax
Expenses
IDENTITY
Apple ID
Google ID
Password Resets / Recovery
HEALTH
Fitness Trackers
NHS App
Healthcare Apps
WORK
Microsoft Teams
OneDrive
SSO
SOCIAL
Social Media Apps
Messengers
Taxi Apps


Cloud Storage
Backups
Photos
STORAGE
Email Account 1
FINANCE
Bank Accounts
Tax
Expenses
Email Account 2
Email Account 3
Apple ID
Google ID
Password Resets / Recovery
IDENTITY
Email Account 4
HEALTH
Fitness Trackers
NHS App
Healthcare Apps
Email Account 5
Microsoft Teams
OneDrive
SSO
WORK
Email Account 6
SOCIAL
Social Media Apps
Messengers
Taxi Apps

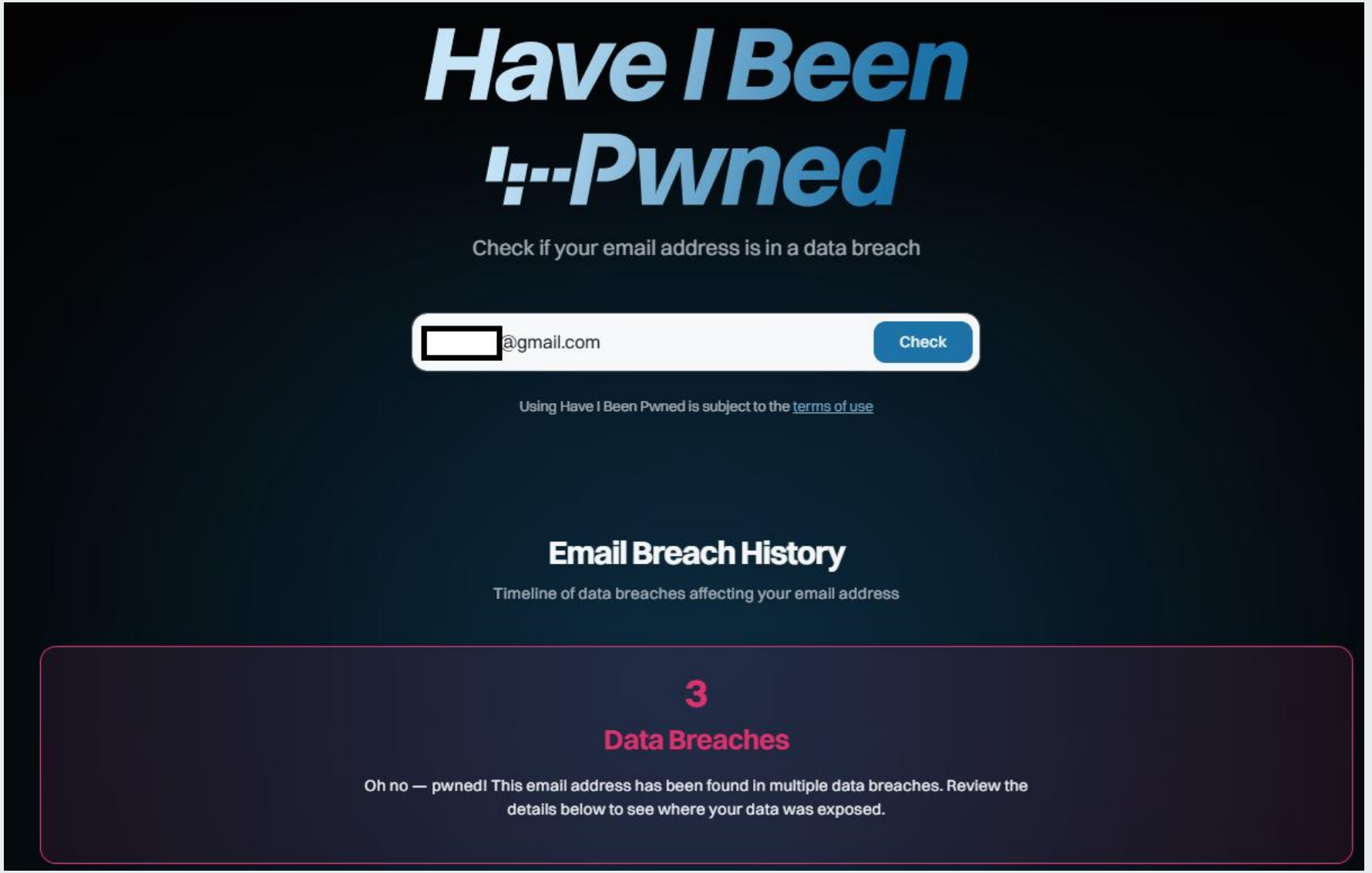
Would you publicly share your personal email address?

Example: Email Visibility Settings



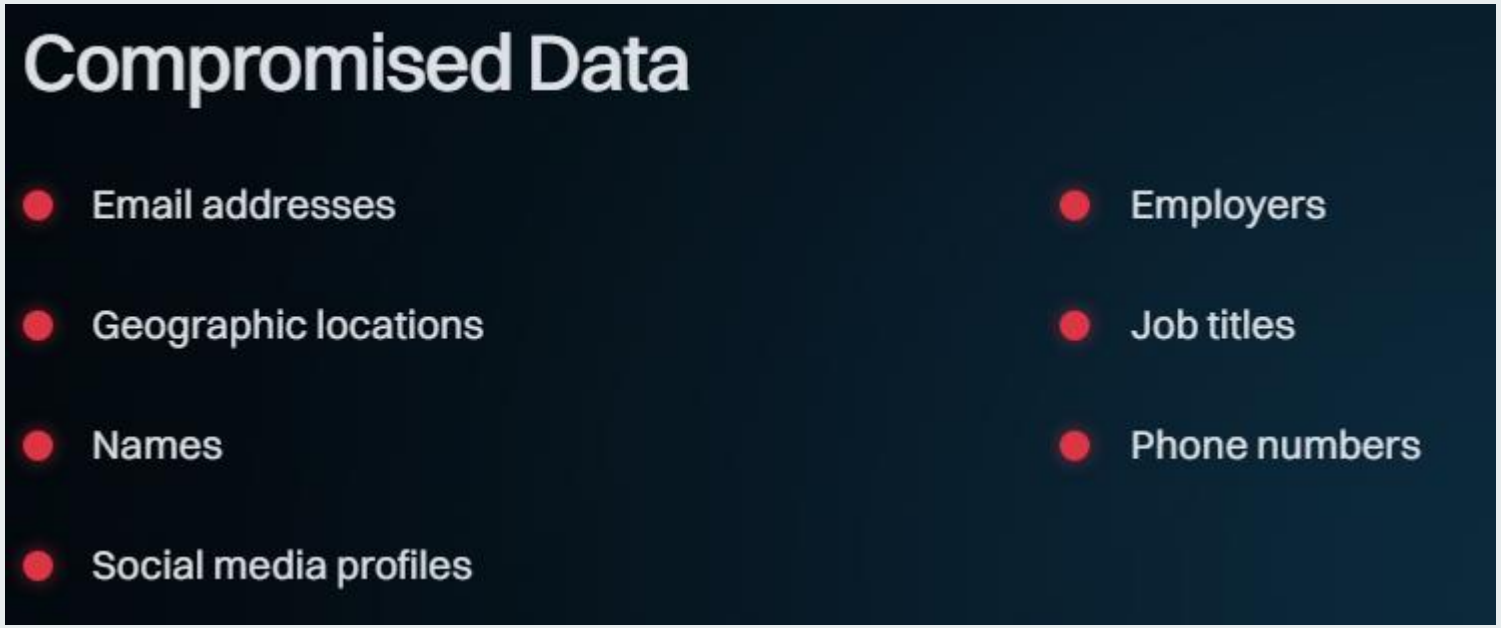
Source: LinkedIn

Email Recon: Seeking the bigger picture



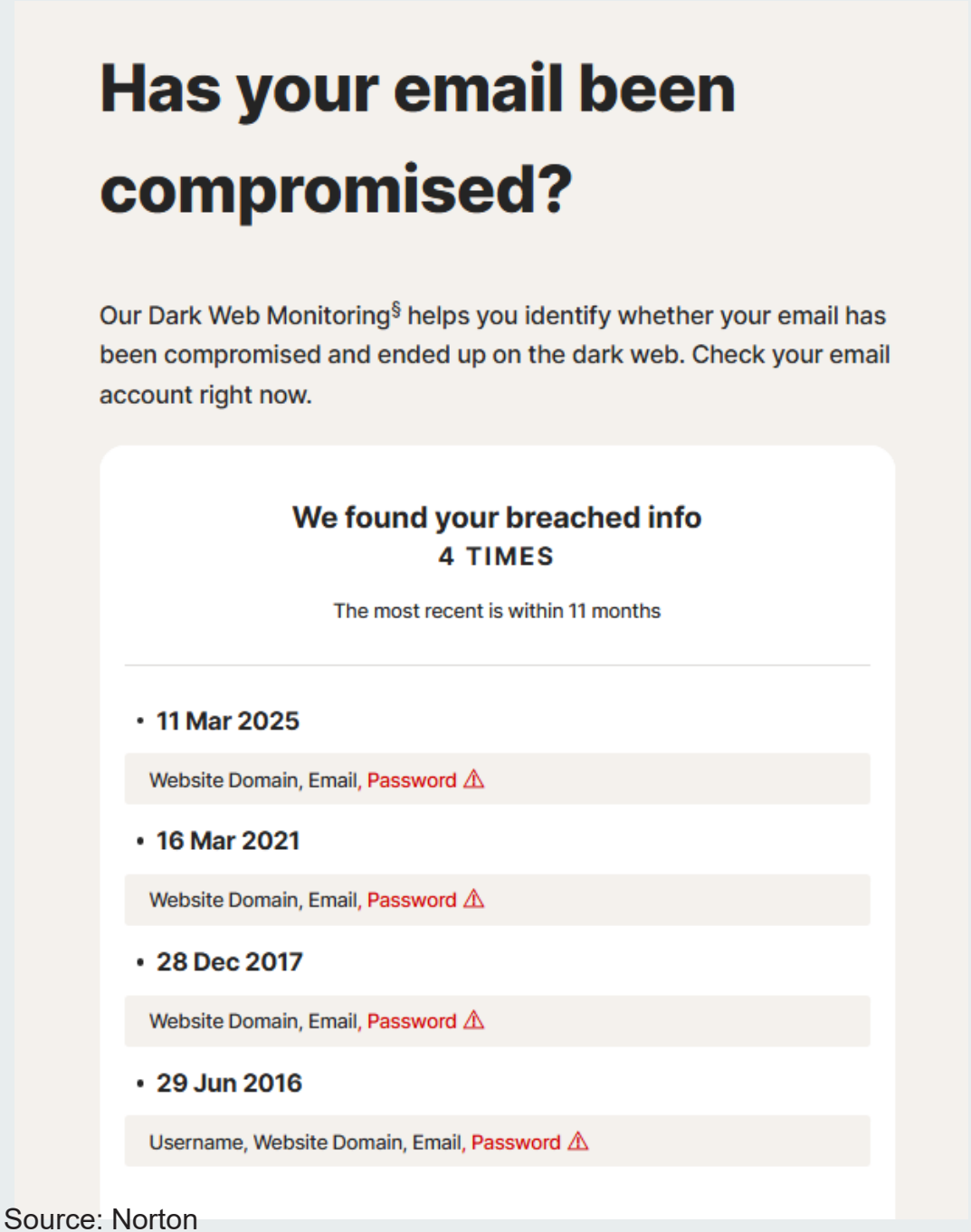
Source: haveibeenpwned.com

Bigger picture continued.



Source: haveibeenpwned

- Which services does the target use (or has used)?
- What hobbies do they have?
- Could I find their old passwords on publicly available data breach lists? (password reuse?)
- Makes spear phishing easier…



Source: Norton

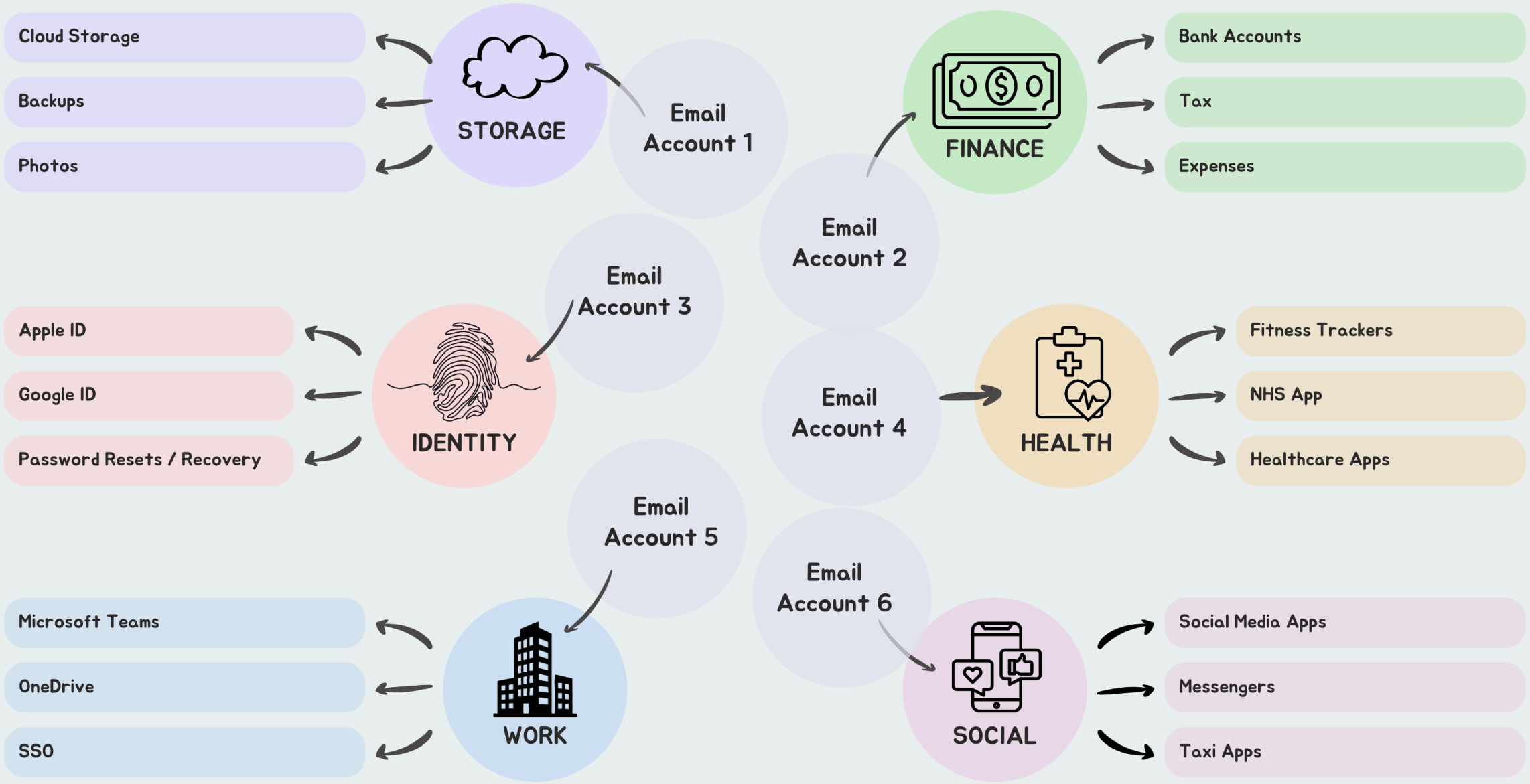
- Many security products have built in leak checkers as well!
- Highlights the importance of using unique passwords.
- No one is immune.

What can you do?

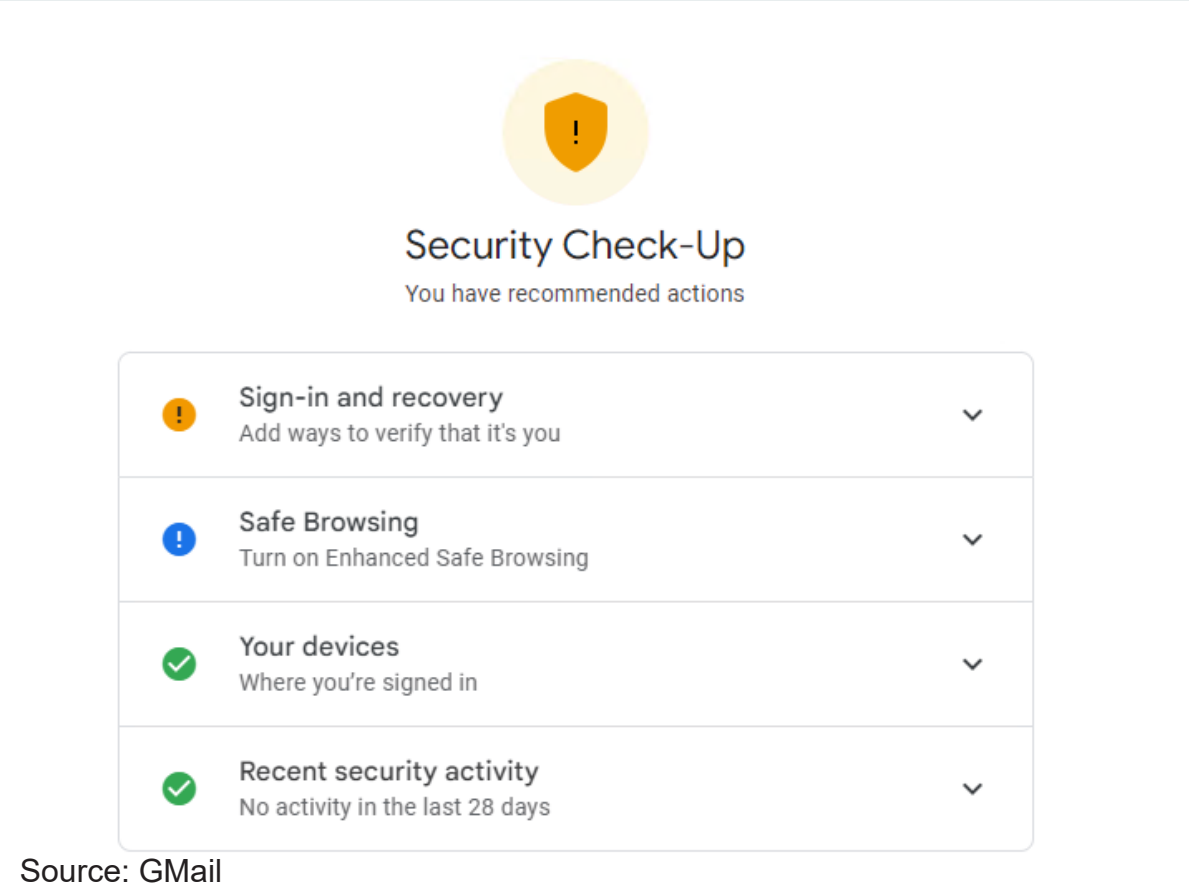
Aim to minimise risk and reduce attack surface.

Create your own email mind map. Keep control.

Consider using multiple email addresses for different services (or email aliases if supported).


Cloud Storage
Backups
Photos
STORAGE
Email Account 1
FINANCE
Bank Accounts
Tax
Expenses
Email Account 2
Email Account 3
Apple ID
Google ID
Password Resets / Recovery
IDENTITY
Email Account 4
HEALTH
Fitness Trackers
NHS App
Healthcare Apps
Email Account 5
Microsoft Teams
OneDrive
SSO
WORK
Email Account 6
SOCIAL
Social Media Apps
Messengers
Taxi Apps

Security Checkups



Source: GMail

- Perform monthly security audits of your email accounts.
- Review sign-in activity. Do you recognise these devices?
- Enable Multifactor Authentication (MFA).
- Check recovery data. Do you even use that number?
- Use unique / complex passwords. (PW Manager?)

Social Media – What am I looking for?

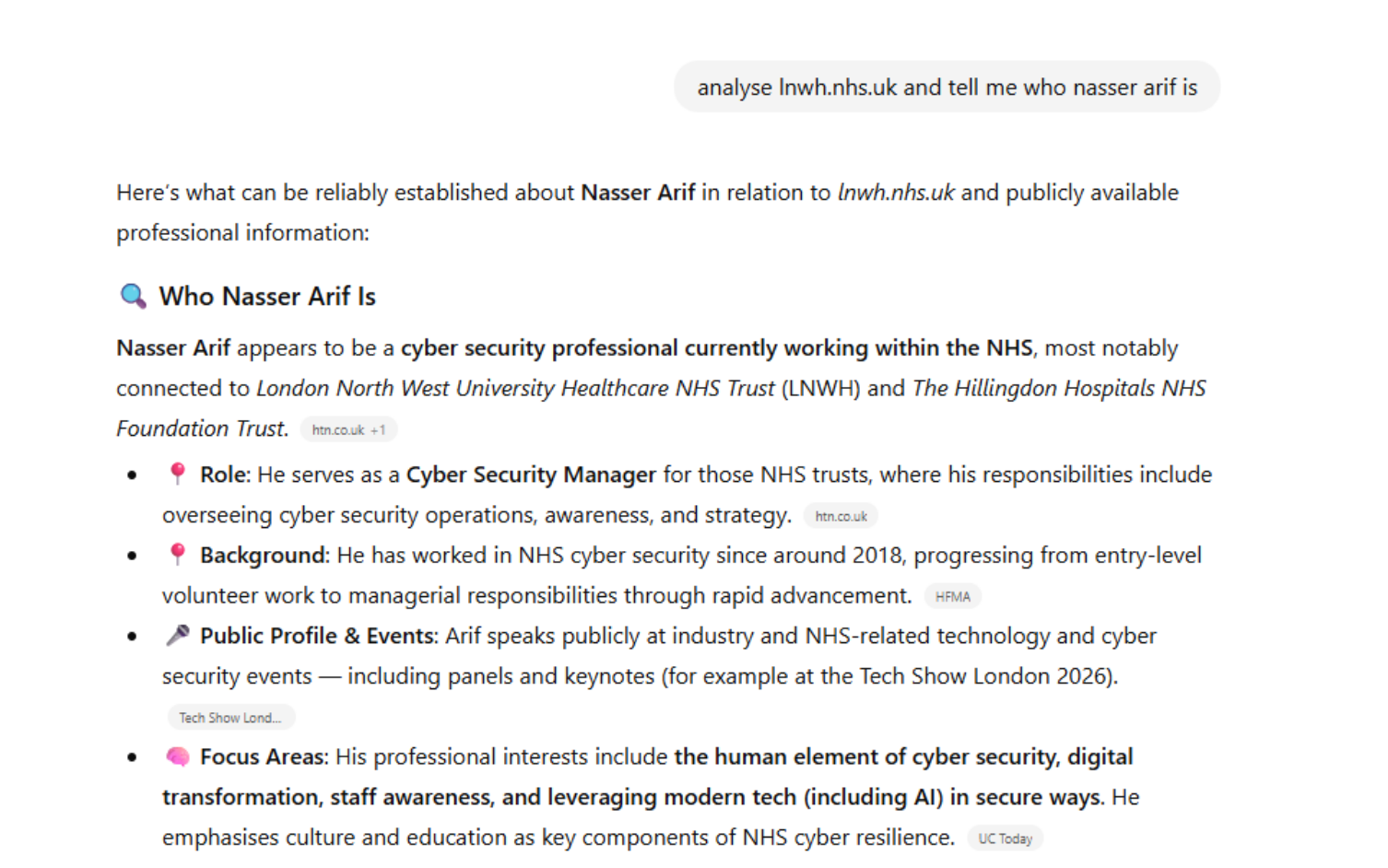
- Location data
- Names (including your pets)
- Birthdays
- Hobbies / Interests
- Romantic interests
- Friends
- Workplace
- Spending habits

Anything that helps me build a picture of the target

Social Media Apps

- Enable MFA / 2SV on **ALL** accounts.
- Unique passwords.
- Review / edit account recovery options.
- Regularly review active sessions and connected apps.
- Consider setting accounts to private.

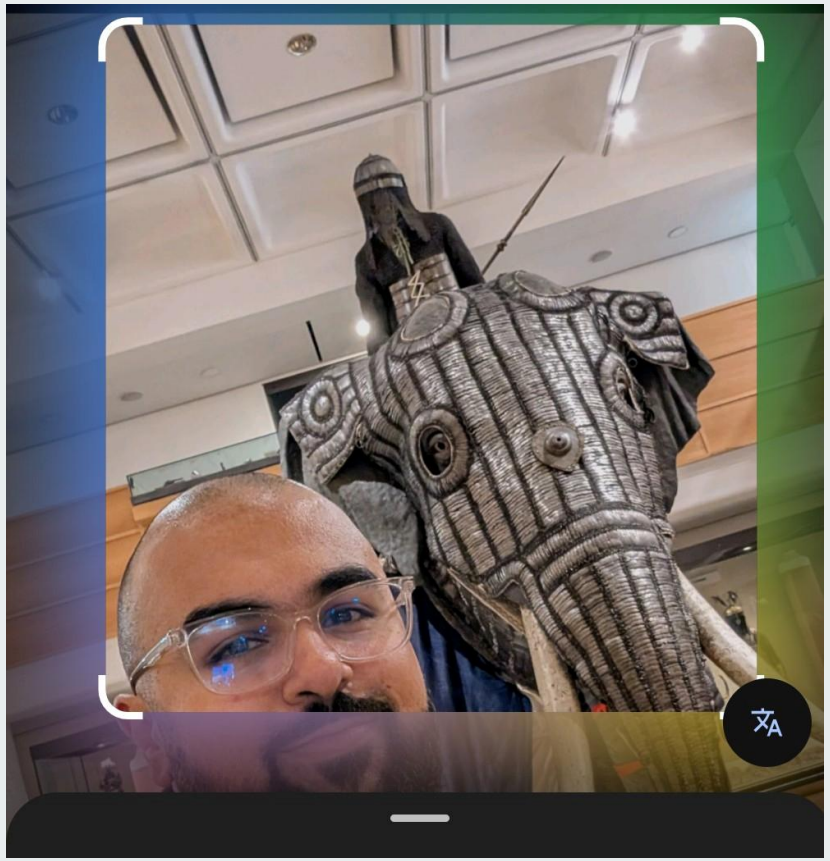
A.I Recon: Public Website Analysis



Source: ChatGPT

- Analysing public websites and social media profiles.
- Anyone can do this.
- No specific cyber tooling required.

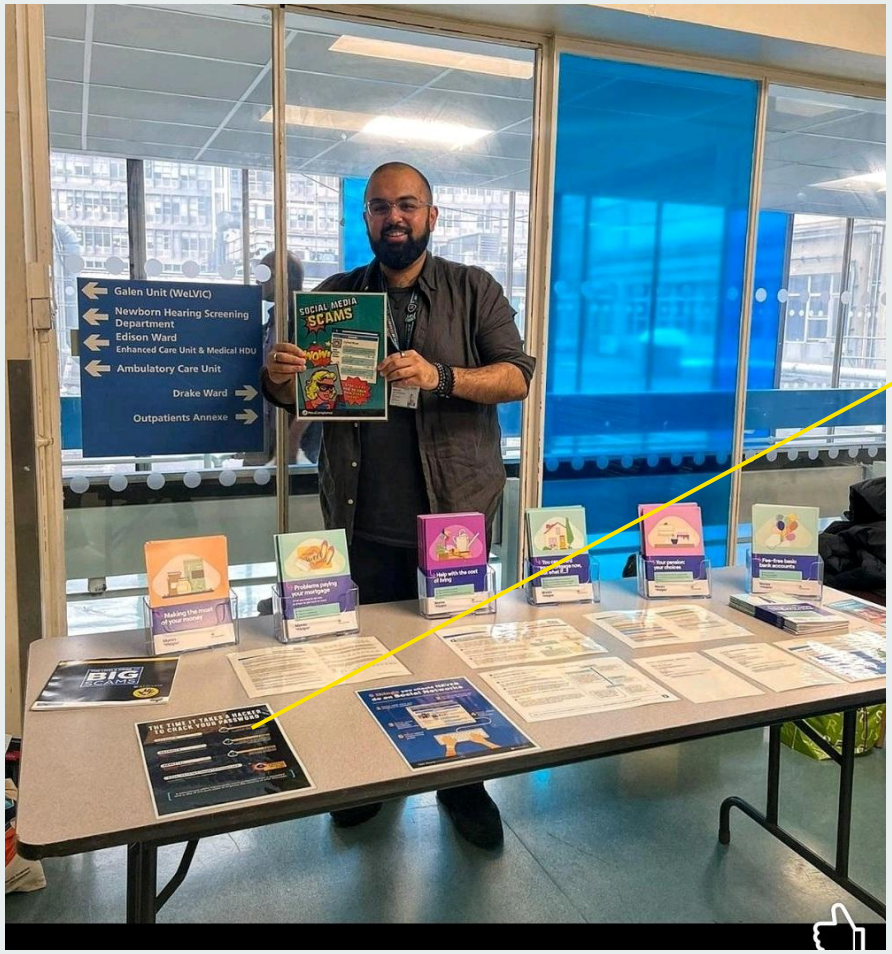
A.I image analysis (1)



This image shows a person next to a historic exhibit.

- The object is a full suit of Indian war elephant armor from the late 16th century.
- It consists of over 8,400 linked metal plates and weighs nearly 160 kg.
- This specific piece is exceptionally rare and is housed in the Royal Armouries Museum in Leeds, England.

A.I image analysis (2)



This image is a chart displaying how quickly hackers break passwords based on their complexity.

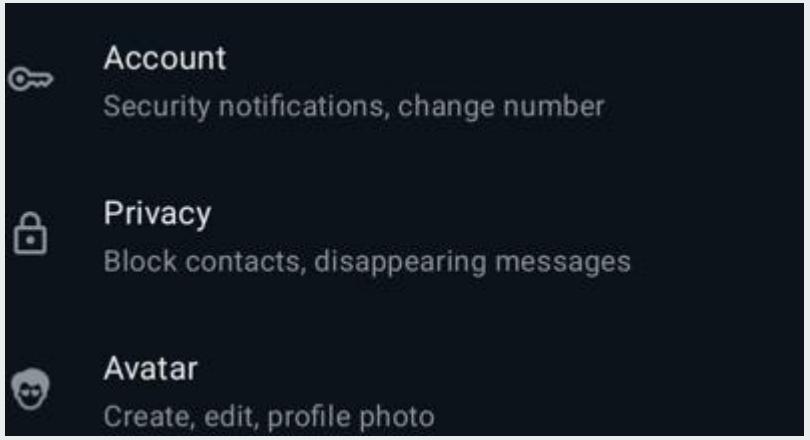
- Passwords that are short and simple can be crack instantly by modern hacking techniques.
- Increasing password length significantly increase

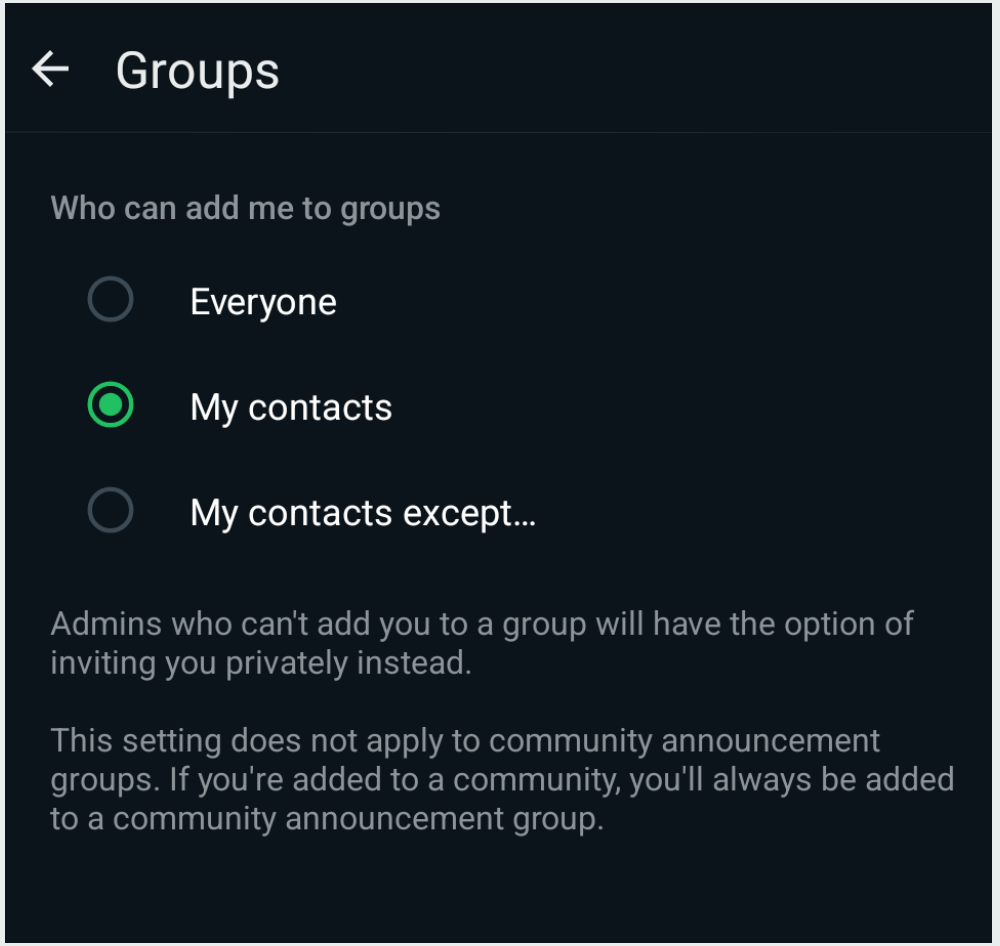
If I had your phone number…

- Could I see your profile photo on messenger apps?
- Could I add you to malicious group chats and send you files?
- Could I ‘smish’ you?
- Could I look it up in data breaches and link it to an email?

Example: Check YOUR Group Controls

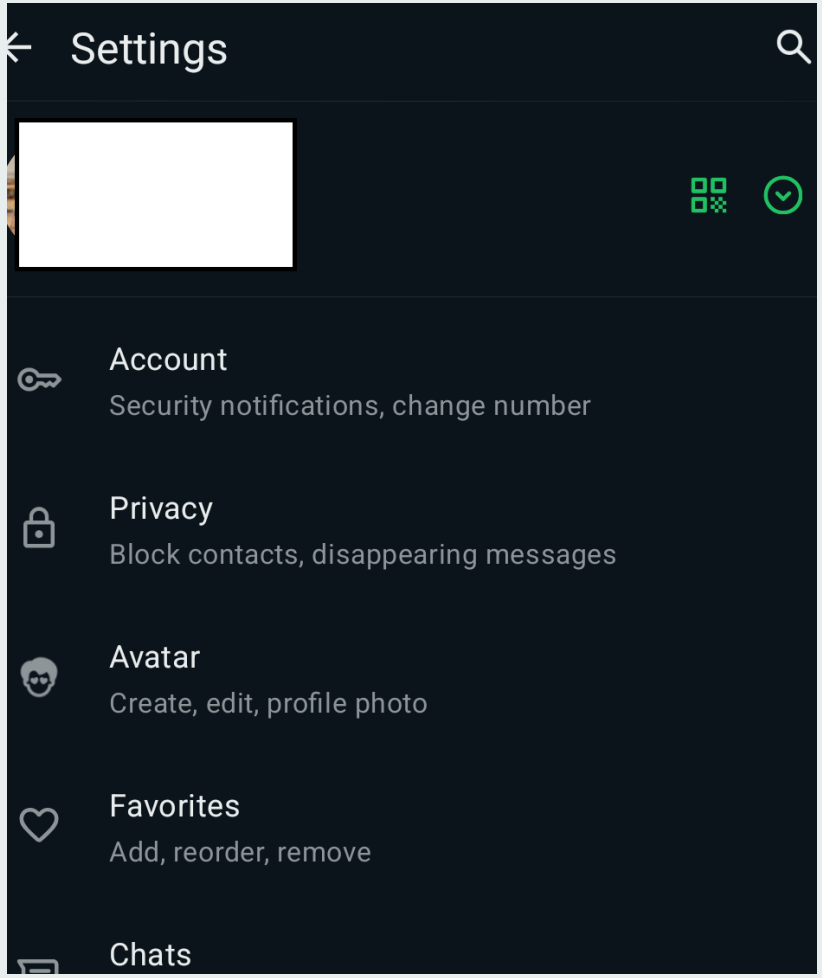
- Stop random people from adding you to group chats.
- Groups are often abused by spammers.

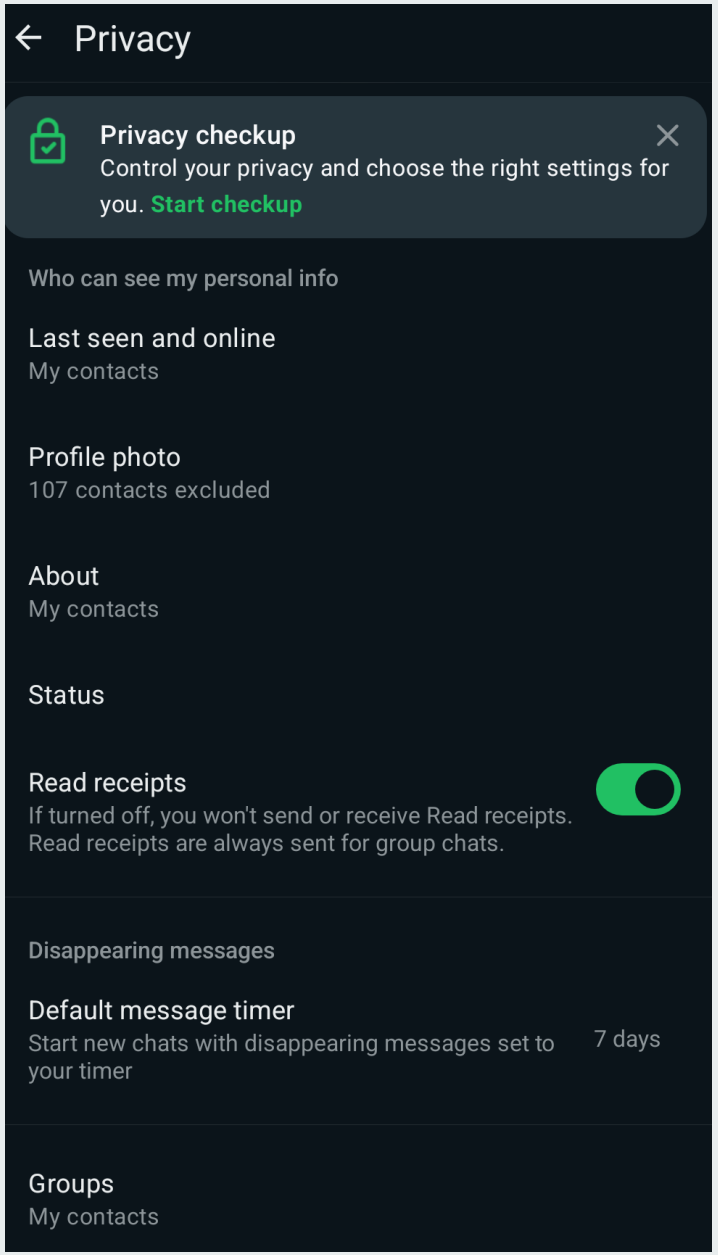




Source: WhatsApp

Example: Privacy





Source: WhatsApp

Vishing…

- Take time to think before you act.
- Do not fall for the sense of urgency!
- Independently verify before acting.
- Rise of deepfakes?

Recon: Job Adverts

- What are we sharing in job adverts?
- What could someone do with that information?
- Are the ad's providing too much detail?
- Including your contact details?

Key Takeaways

- Map out your own digital footprint (email mind maps, password managers). Hacker mindset.
- Regularly audit your own accounts.
- Consider separating your accounts based on sensitivity of data.
- Minimise risk where you can.

What does the future hold?

Any Questions? (follow me)

Slido

Please scan the QR Code on the screen. This will take you through to Slido, where you can interact with us.

SCAN ME

CONVENZIS

Case Study

Heimdal®

Case Study

Adam Pilton
Cyber Security Advisor
Heimdal Security

Heimdal®

Proving Cyber Readiness

Turning NHS Security Expectations into Operational Control

25th February 2026

www.heimdalsecurity.com

Heimdal®

Adam Pilton

Cyber Security Advisor

With 15 years in law enforcement, Adam's final role was as a Detective Sergeant leading the Covert operations and Cyber Crime teams.

Adam has worked with multi-national businesses developing their people and processes to improve their cyber security maturity.

Heimdal®

Case Study

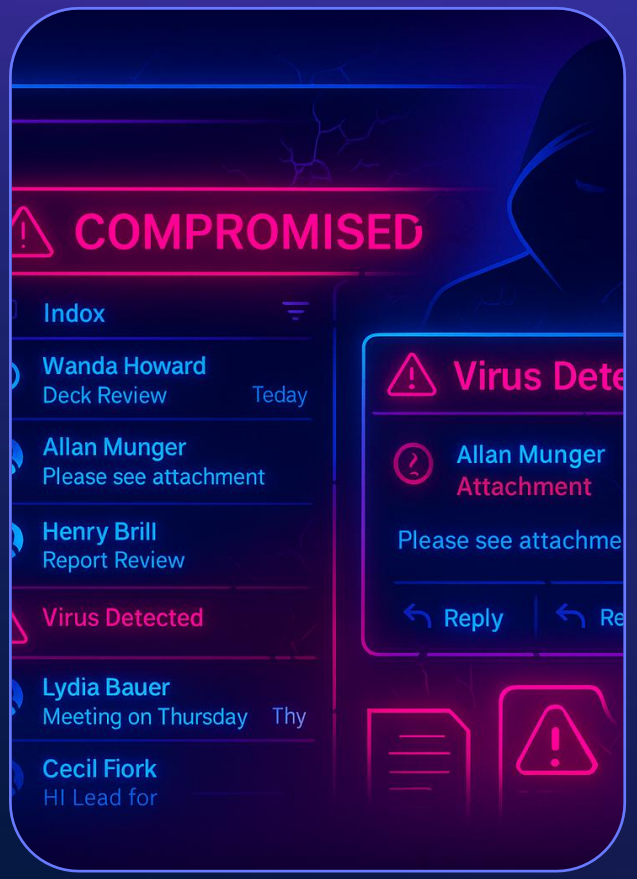
Lessons from a Breached Solicitor Email and Inheritance Theft

Lessons from a Breached Solicitor

Heimdal®

The Solicitor

The Mistake



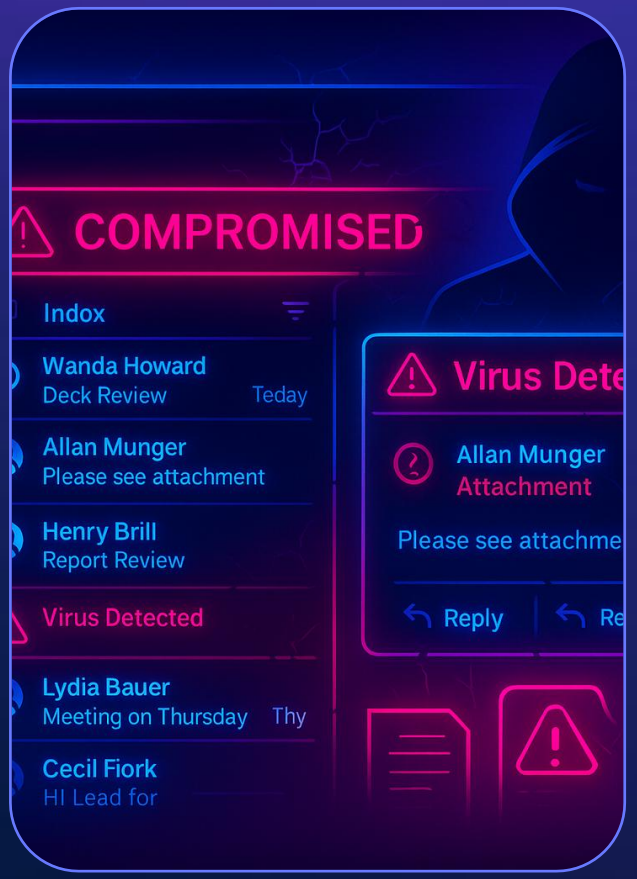
The Attack Unfolds

Lessons from a Breached Solicitor

Heimdal®

The Solicitor

The Mistake



The Attack Unfolds

Lessons from a Breached Solicitor

Heimdal®

The Solicitor

The Mistake

The Attack Unfolds

Lessons from a Breached Solicitor

Lessons from a Breached Solicitor

Heimdal®

The Switch

The Consequences

Lessons from a Breached Solicitor

The sting

The Consequences

Shortcuts

Basics or Foundations?

Foundations Are Harder Than We Admit

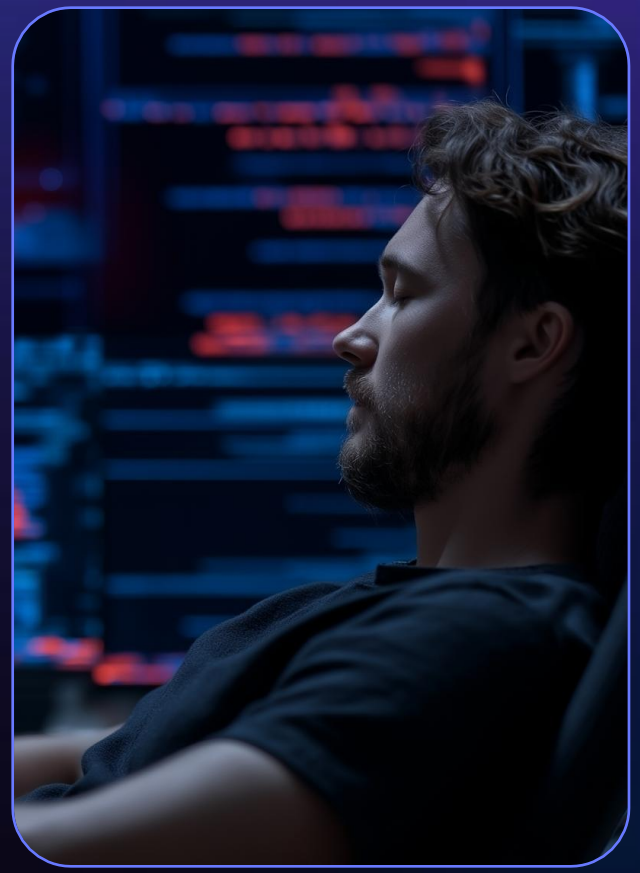
The Stall Points

Foundations Are Harder Than We Admit

Tool Proliferation Creates Noise

The Stall Points

The sting

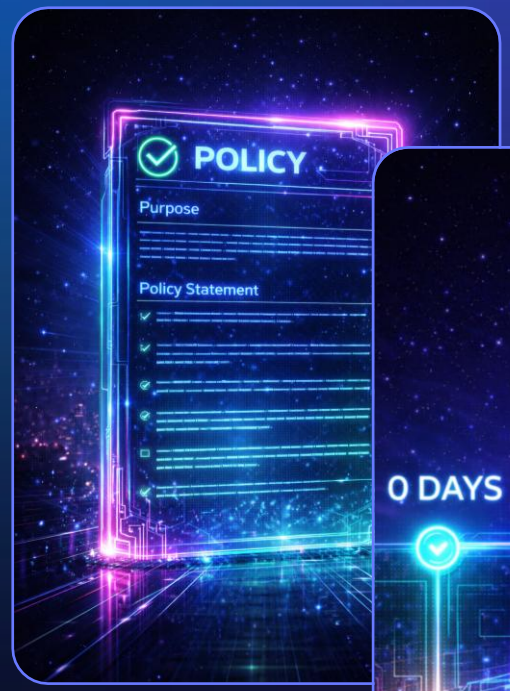


Tool Proliferation Creates Noise

Compliance Becomes the Destination

Defensible Assurance

Heimdal®



Understand

Evidence

Controlled

Managed

Confident

Comfortable

SS

Heimdal®

The Role of Leadership

Heimdal®

Introducing Heimdal

Heimdal XDR: Security Across and Beyond Perimeters, Unifying Local & Cloud Environments

Heimdal®

Cloud Security

- M365 Email Security
- M365 User Security
- CASB (DNS Security – Network & Endpoint)
- CWPP for Cloud, Desktops & Servers
- Cloud Workspace Ransomware Protection

Network Security

- DNS Security - Network

Endpoint Security

- DNS Security – Endpoint
- Next-Gen Antivirus & Firewall
- Ransomware Encryption Protection Popular

Vulnerability Management

- Patch & Asset Management Popular
- Infinity Management

Privileged Access Management

- Privilege Elevation & Delegation Management Popular
- Privileged Account & Session Management
- Application Control - AppFencing™

Email & Collaboration Security

- Email Security 365
  | Email Security 365
  | Email Security ATP & Fraud Prevention

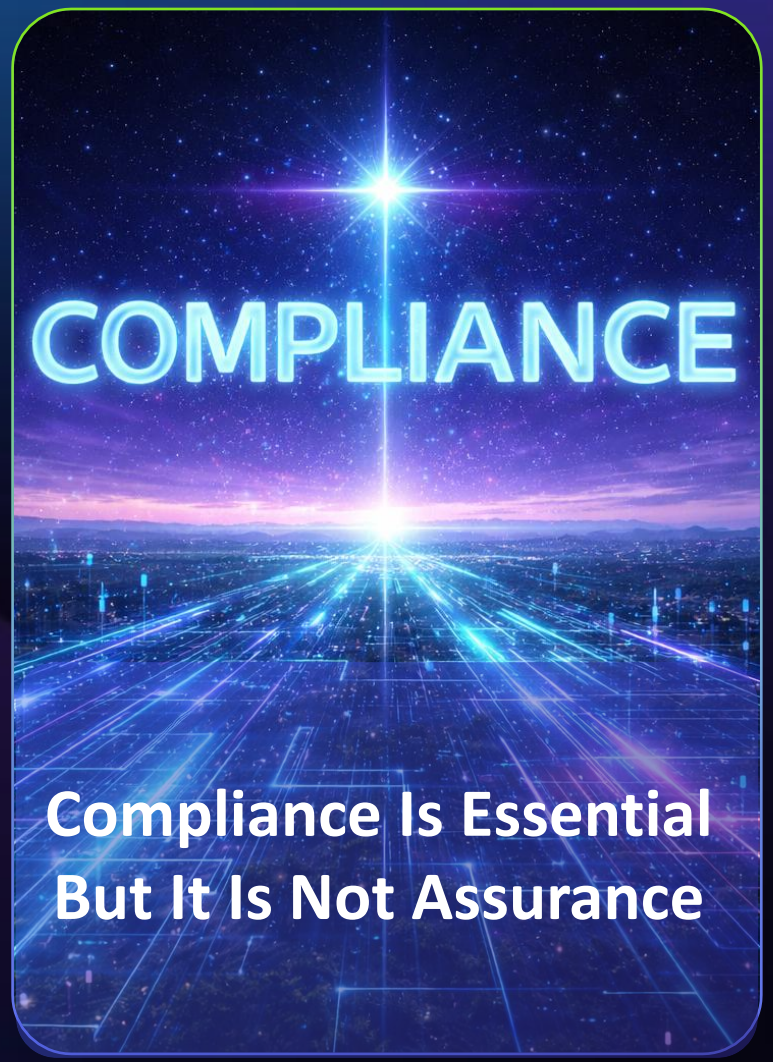
Threat Hunting

- Threat-hunting & Action Center
  | Estate Monitoring
  | User Monitoring (M365 Security)

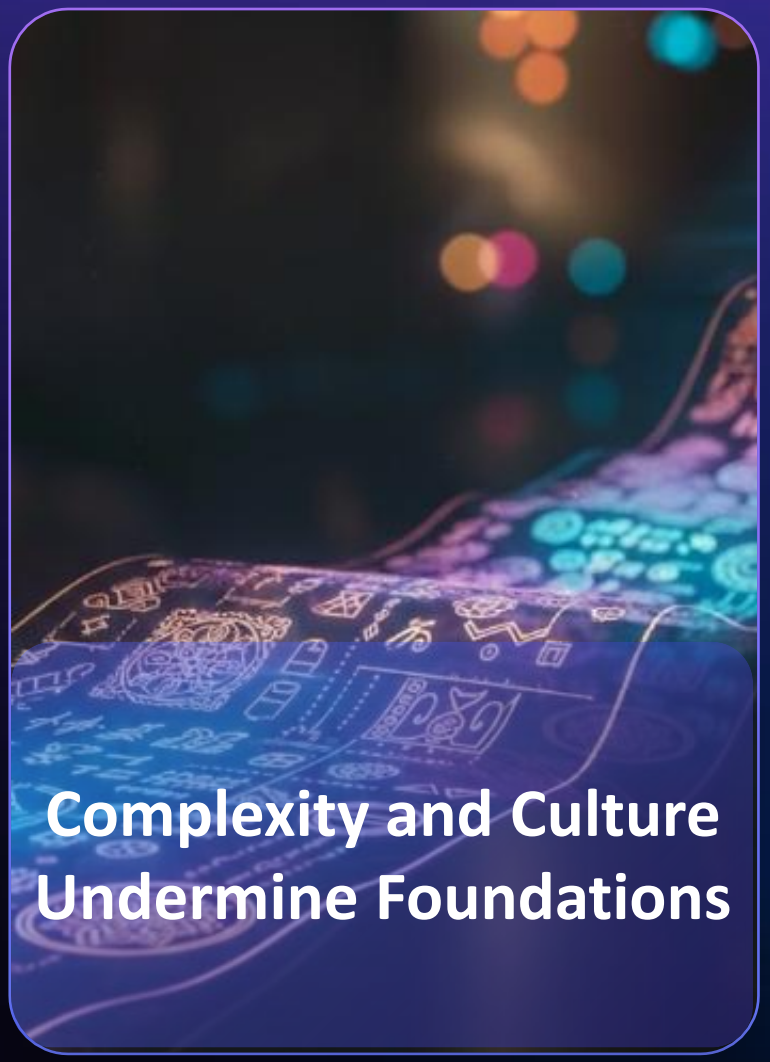
Unified Endpoint Management

- Remote Desktop
- BitLocker Management
- Scripting
- PXE Deployment
- USB Management

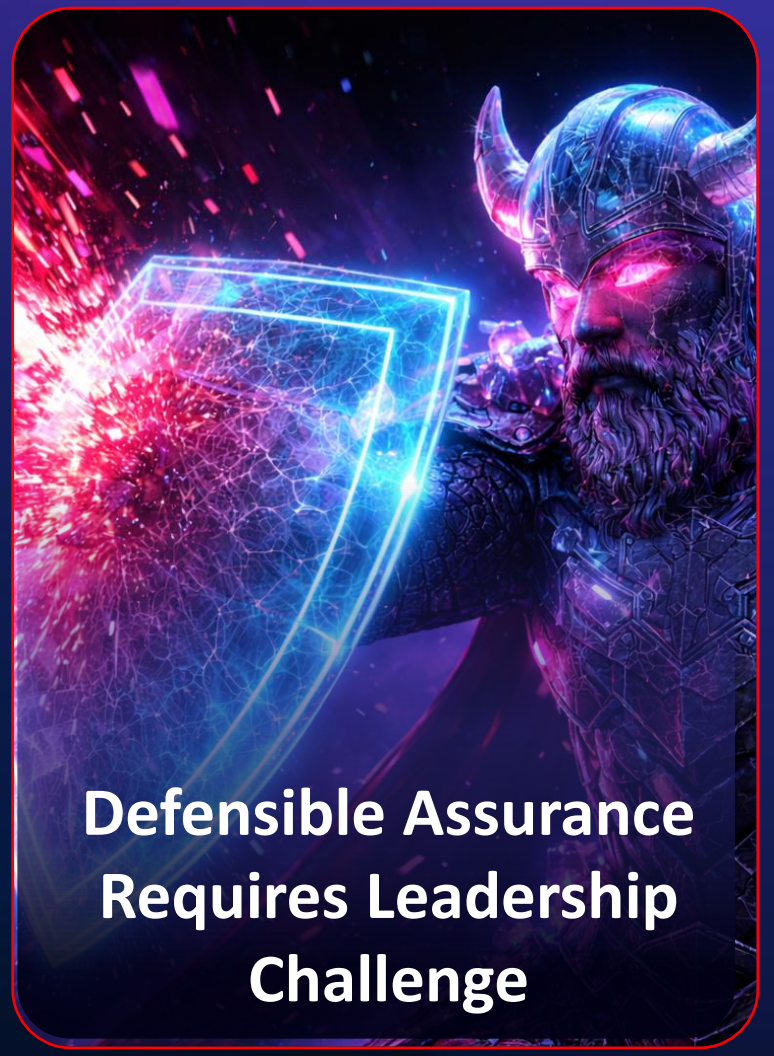
Heimdal®



Compliance Is Essential But It Is Not Assurance



Complexity and Culture Undermine Foundations



Defensible Assurance Requires Leadership Challenge

Heimdal®

Exclusive Offer

Heimdal Essentials for the NHS

Exclusive Convenzis NHS Offer: Heimdal Essentials for Healthcare

Heimdal®

Details:

- Choose any solution from our essential modules (e.g. Patch Mgmt.)
- Unified Endpoint Management (UEM) Included:
  - ✓ BitLocker Management
  - ✓ USB Control
  - ✓ Scripting
- Exclusive Bonus: 6 Months Complimentary Remote Desktop
- Full Professional Services for Seamless Implementation

Pick Any Security Solution & Get Complimentary UEM + 6 Months Remote Desktop

Endpoint Security

- ✓ Next-Gen Antivirus, XTP & Firewall
- ✓ Ransomware Encryption Protection

Vulnerability Management

- ✓ Patch & Asset Management

Privileged Access Management

- ✓ Privilege Elevation & Delegation Management
- ✓ Application Control - AppFencing™

Unified Endpoint Management

- ✓ Remote Desktop
- ✓ BitLocker Management
- ✓ Scripting
- ✓ USB Control

Heimdal®

Threat Watch LIVE

March

3rd March 2026

www.heimdalsecurity.com

Slido

Please scan the QR Code on the screen. This will take you through to Slido, where you can interact with us.

SCAN ME

Skill Clinic

Jessica Figueras
Director & Co-Founder
CxB - Cyber Governance for Boards

Cyber Governance for Boards

Board-level cyber governance

Jessica Figueras
CEO and co-founder

About CxB

Founded by four non-executive directors, we support boards to raise their game in cyber governance through training, peer insights, assessment and mentoring.

www.cxb.org.uk

Olu Odeniyi
NED, Kent Community Health NHS Foundation Trust

Jessica Figueras
NED, University of Westminster

Martyn Croft
NED, Reliance Bank

David Jones
Chair, DVLA

cxb
Cyber Governance for Boards

1. A complex, fast-moving, existential risk that's hard to understand, hard to predict and impossible to manage

cxb
Cyber Governance for Boards

2. A compliance problem

cxb
Cyber Governance
for Boards

CAF-aligned DSPT, A1.a

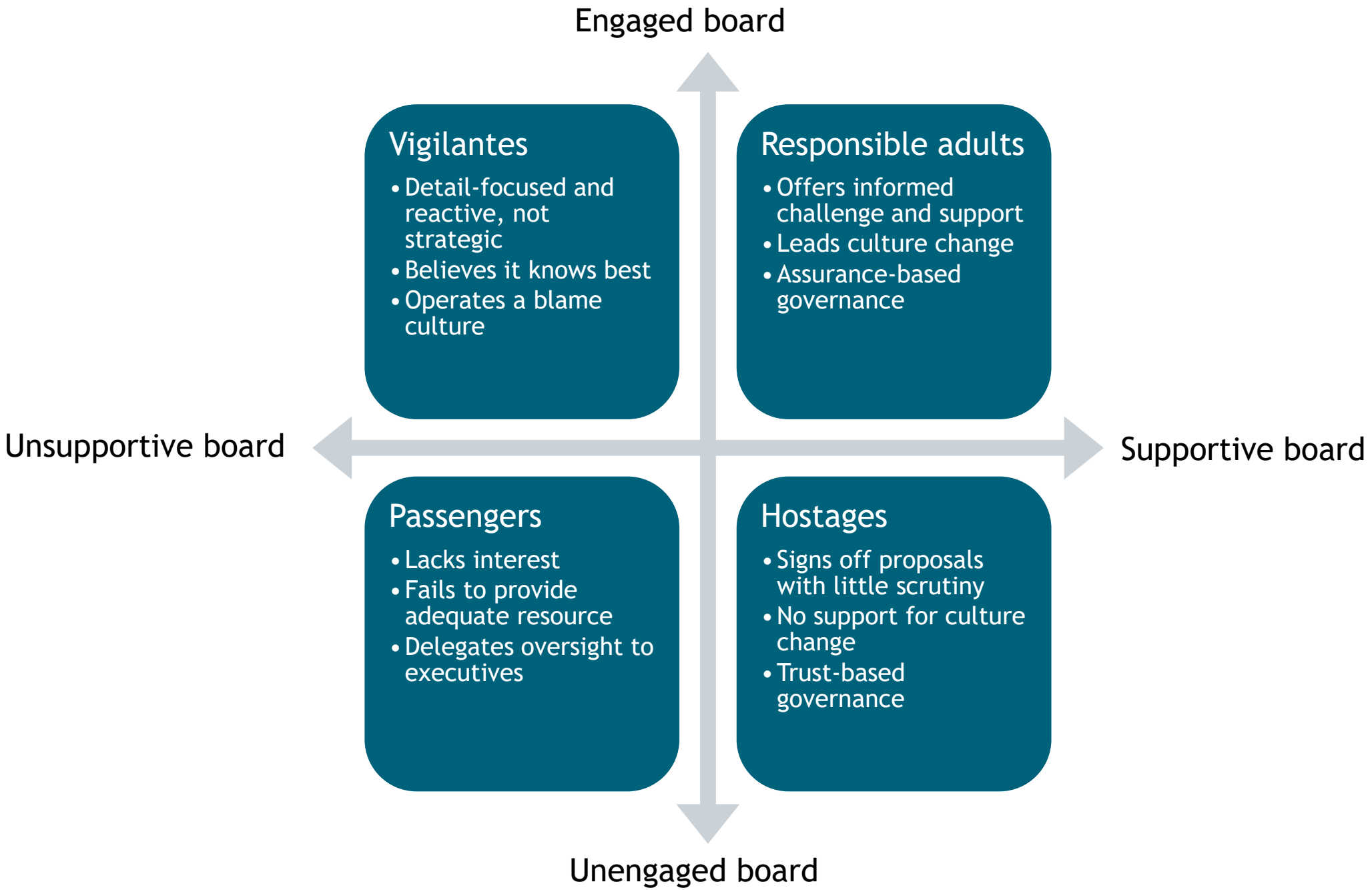
"You have effective organisational information assurance management led at board level and articulated clearly in corresponding policies."

1. Your organisation's **approach and policy** relating to the security and governance of information, systems and networks supporting the operation of your essential function(s) are **owned and managed at board level**. These are communicated, in a meaningful way, to risk management decision-makers across the organisation.

2. **Regular board discussions** on the security and governance of information, systems and networks supporting the operation of your essential function(s) take place, **based on timely and accurate information** and informed by expert guidance.

3. There are **board-level individuals who have overall accountability** for the security and governance of information, systems and networks (these may be the same person), who drive regular discussion at board level.

cxb
Cyber Governance for Boards



cxb
Cyber Governance for Boards

What you can do for your board

1. Ask for honest feedback on your reports.

2. Be nice. But not reassuring.

3. Every organisation trades off security against other benefits. Show these trade-offs to your board. Were they aware? How do they feel about it? That's their risk appetite, right there.

4. Support your board to increase its own maturity. We can help!

cxb
Cyber Governance for Boards

cxb

Cyber Governance for Boards

www.cxb.org.uk

info@cxb.org.uk

Slido

Please scan the QR Code on the screen. This will take you through to Slido, where you can interact with us.

SCAN ME

Panel Discussion

Dr Avi Mehra
Associate Partner & Clinical Safety Officer
IBM

Michelle Corrigan
Chief Executive Officer
Digital Care Hub

Dr Trudie Fell
CEO and Founder
BelleVie Care Home

Slido

Please scan the QR Code on the screen. This will take you through to Slido, where you can interact with us.

SCAN ME

Slido

Please scan the QR Code on the screen. This will take you through to Slido, where you can interact with us.

SCAN ME

Food, Drinks & Networking