CONVENZIS

Securing the Future of Healthcare

Navigating the Cybersecurity Landscape in the NHS

Welcome to the Securing the Future of Healthcare Conference!

20th September 2023
10:50am – 3:00pm
Virtual Event

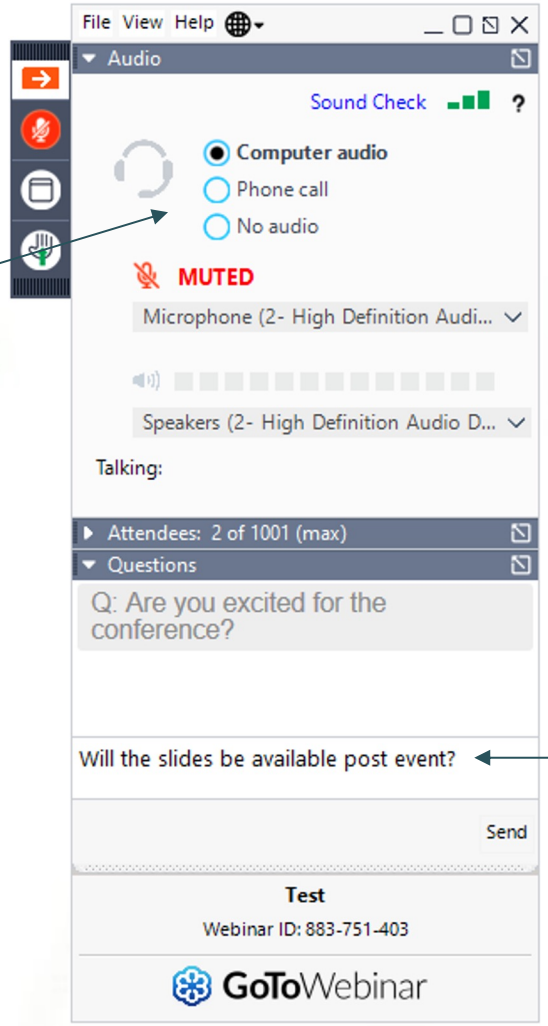
Securing the Future of Healthcare

Navigating the Cybersecurity Landscape in the NHS

Securing the Future of Healthcare Conference

CONVENZIS

Make sure you are connected via Computer Audio for the conference. You can test your audio via the 'Sound Check' tab.



If you have any questions or comments for Speakers across the day, please expand the Questions Section on the GoToWebinar panel. You will not be able to see each others questions.

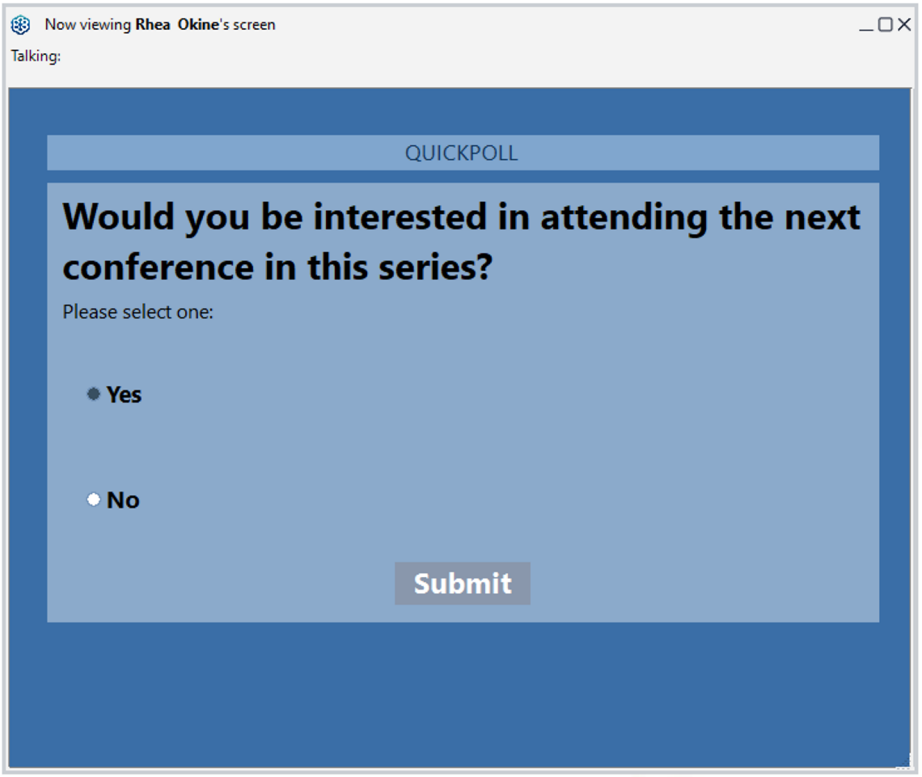
Securing the Future of Healthcare

NHS

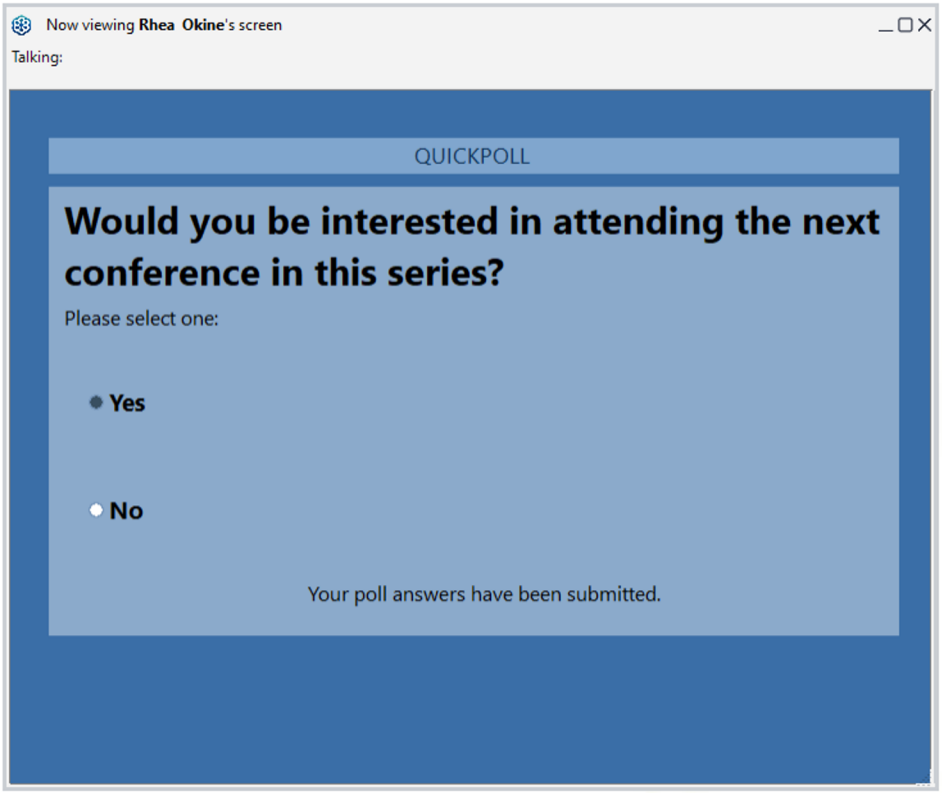
Navigating the Cybersecurity Landscape in the NHS

Securing the Future of Healthcare Conference

CONVENZIS



Click on **one** of the multiple choice options, then press '**Submit**'



Once **Submitted** your screen will look like this

CONVENZIS

Securing the Future of Healthcare

Navigating the Cybersecurity Landscape in the NHS

Speaking Now…

Mr Charles Sammut

Deputy Director Cyber Security - UK Health and Security Agency

CONVENZIS

Up Next…

zscaler™

CONVENZIS

Securing the Future of Healthcare

Navigating the Cybersecurity Landscape in the NHS

Speaking Now…

Johnathon Murden

Lead Technologist NHS - Zscaler

CONVENZIS

Up Next…

rubrik

CONVENZIS

Securing the Future of Healthcare

Navigating the Cybersecurity Landscape in the NHS

Speaking Now…

Robert Priest

Systems Engineer for the UK Public Sector - Rubrik

CONVENZIS

Securing the Future of Healthcare

Navigating the Cybersecurity Landscape in the NHS

Speaking Now…

Mike Culshaw

CTO - Pennine Care FT

CONVENZIS

Comfort Break

CONVENZIS

Up Next…

FORESCOUT

CONVENZIS

Securing the Future of Healthcare

Navigating the Cybersecurity Landscape in the NHS

Speaking Now…

Daniel Trivellato

VP OT & IoMT Solutions - Forescout

FORESCOUT

Automated Cybersecurity Across Your Digital Terrain

STAYING AHEAD OF COMPLIANCE AND THREATS, IN A SUSTAINABLE WAY

Daniel Trivellato – VP of OT & Healthcare Solutions

NHS

Who is Forescout?

Over 20 years of cybersecurity expertise...

- Headquartered in San Jose, California
- Employees in over 30 countries
- Leader in threat research and intelligence, especially active in OT & IOT

Over 3000 customers globally...

- 30% of Fortune 100, 25% of Global 2K
- Expertise across Utilities, Financial, Insurance, Government, and Healthcare industries

Trusted and Proven...

- 190+ original vulnerabilities discovered by Forescout Vedere Labs including Project Memoria (97 new vulnerabilities impacting 400+ vendors) and OT:ICEFALL (56 vulnerabilities affecting devices from 10 vendors)
- Millions of end points deployed in US DoD Comply-to-Connect Program
- Diverse customer case studies and recognized by numerous industry awards

Managing cyber risk through automation and data-powered insights.

FORESCOUT

Common Customer Challenges

NHS

Visibility is lagging behind attack surface growth

75%

OF NHS TRUSTS REPORT **WIDENING VISIBILITY GAPS IN END-USER** AND **IOT/ IOMT ASSETS.**

Attackers are targeting unmanaged systems

35%

OF NHS TRUSTS HAD **IOT/ IOMT** DEVICES **TARGETED DIRECTLY** OR **AS PART OF A LARGER ATTACK.**

Budgets and resource not growing inline with threats

450x

UP TO 450x ALERTS PER HOUR MANAGED BY SECOPS TEAMS.

Evolving standards, frameworks & regulations

National Cyber Security Centre

CYBER ESSENTIALS PLUS

NHS Digital

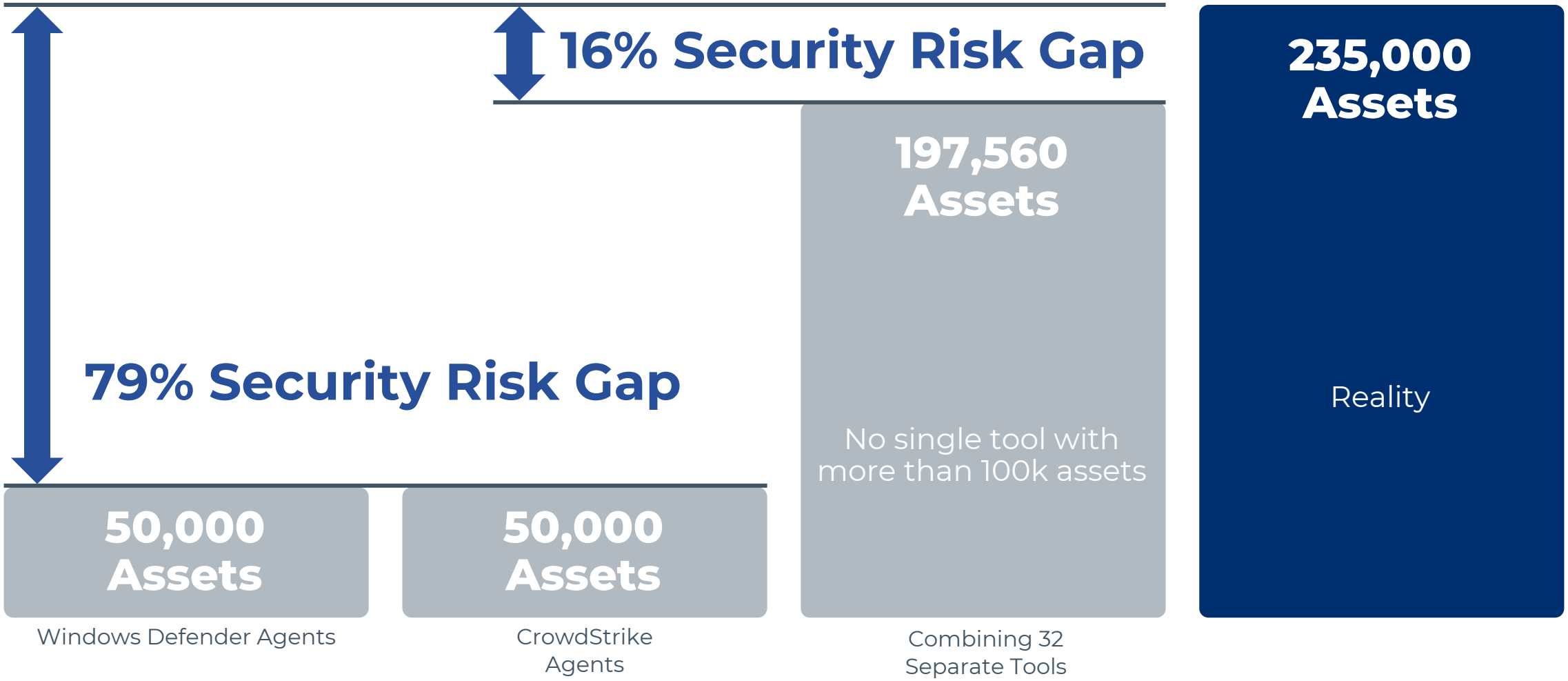
ITIL®

ISO

LACK **GOVERNANCE TOOLS** TO **ASSESS** AND **ENFORCE COMPLIANCE**

1. Cybersecurity Asset Management Trends 2021 - Enterprise Strategy Group | 2. The State of IoT/OT Cybersecurity in the Enterprise - Ponemon Institute | 3. Top Security and Risk Management Trends 2021 - Gartner

The Struggle to Achieve Visibility:
Real-World Example from a Forescout Customer



Forescout (Medical) Research

The 5 Riskiest Connected Devices in 2023

July 13, 2023

Healthcare is the riskiest industry in 2023. Devices in healthcare are more likely to have dangerous ports, such as Telnet, SSH and RDP open.
IT network infrastructure and security appliances are the most exposed devices on the internet. They are followed by IoT devices such as IP cameras (23%), NAS (7%) and VoIP (3%).

https://www.forescout.com/blog/riskiest-connected-devices-it-iot-ot-iomt/

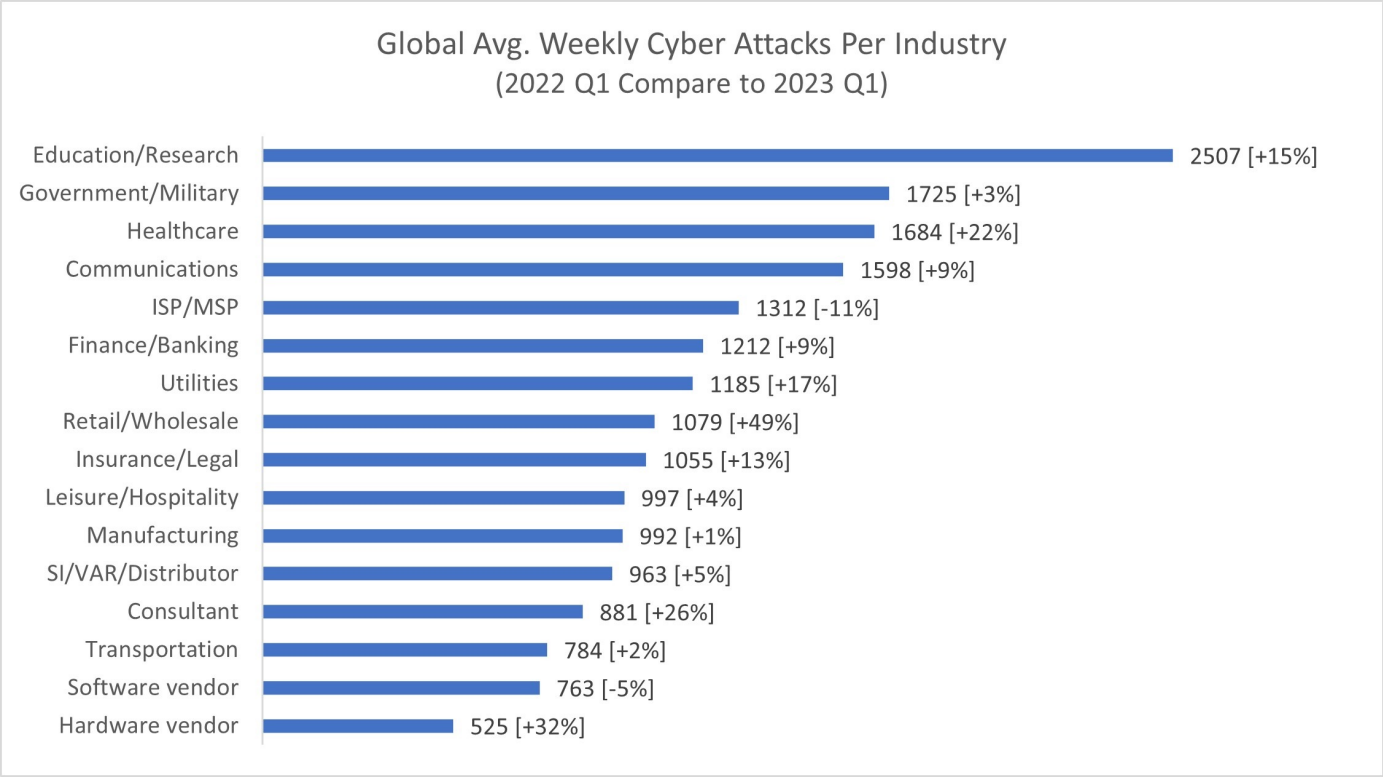
Internet Exposure of Medical Devices and Systems

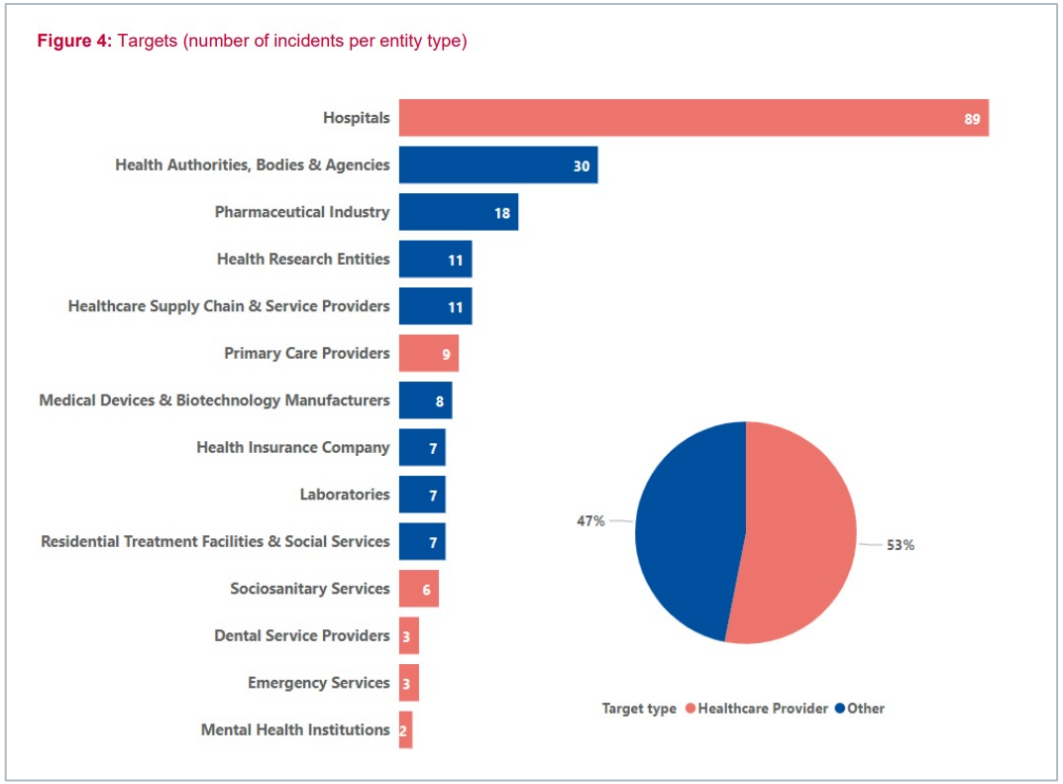
Sept. 26, 2022

Forescout Research aka Vedere Labs, found more than 7,000 exposed medical devices and systems on the internet, including PACS, healthcare integration engines, EMRs and medication dispensing systems.

https://www.forescout.com/blog/fbi-notice-underscores-cyberthreats-posed-by-medical-devices-and-iomt-risk-management-can-help/

A Sector Under Increased Attack





A rise in healthcare cyber attacks calls for zero trust | **World Economic Forum** (weforum.org)

Health Threat Landscape — **ENISA** (europa.eu)

Evolving Compliance Requirements

CAF – Principles

This page gives you an overview of
CAF guidance covers.

Objective A: Managing s

Appropriate organisational structu
understand, assess and systemati
information systems supporting es

A1 Governance

Putting in place the policies and proces
the security of network and informatio

A2 Risk management

Identification, assessment and underst
overall organisational approach to risk

A3 Asset management

Determining and understanding all sys
essential functions.

A4 Supply chain

Understanding and managing the secu
arise from dependencies on external s

Principle: A3 Asset Management

Everything required to deliver, maintain or support networks and information systems necessary for the operation of essential functions is determined and understood. This includes data, people and systems, as well as any supporting infrastructure (such as power or cooling).

A3.a Asset Management

Not achieved	Achieved
At least one of the following statements is true	**All the following statements are true**
Inventories of assets relevant to the essential function are incomplete, non-existent, or inadequately detailed.	All assets relevant to the secure operation of essential functions are identified and inventoried (at a suitable level of detail). The inventory is kept up-to-date.
Only certain domains or types of asset are documented and understood. Dependencies between assets are not understood (such as the dependencies between IT and OT).	Dependencies on supporting infrastructure (e.g. power, cooling etc) are recognised and recorded.
Information assets, which could include personally identifiable information or other sensitive information, are stored for long periods of time with no clear business need or retention policy.	You have prioritised your assets according to their importance to the operation of the essential function.
Knowledge critical to the management, operation, or recovery of essential functions is held by one or two key individuals with no succession plan.	You have assigned responsibility for managing physical assets.
Asset inventories are neglected and out of date.	Assets relevant to essential functions are managed with cyber security in mind throughout their lifecycle, from creation through to eventual decommissioning or disposal.

curity even
s remain effecti
otential to affect, essential functio

and track the effectiveness of existing

and information systems.

pact of cyber security

pact of a cyber security incident or
g the restoration of those functions

ation processes in place.

lessons to improve the resilience of

YOU CAN'T SECURE WHAT YOU CAN'T SEE

MANAGE RISK

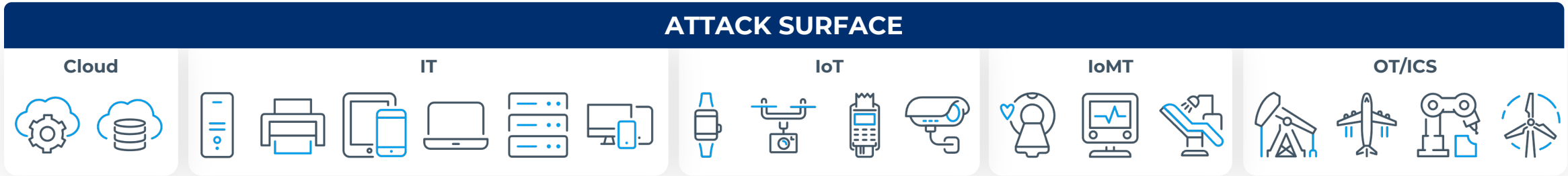
Minimize Attack Surface

GOVERN ACCESS

Ensure Compliance & Reduce Blast Radius

DETECT THREATS

Elevate SOC Performance



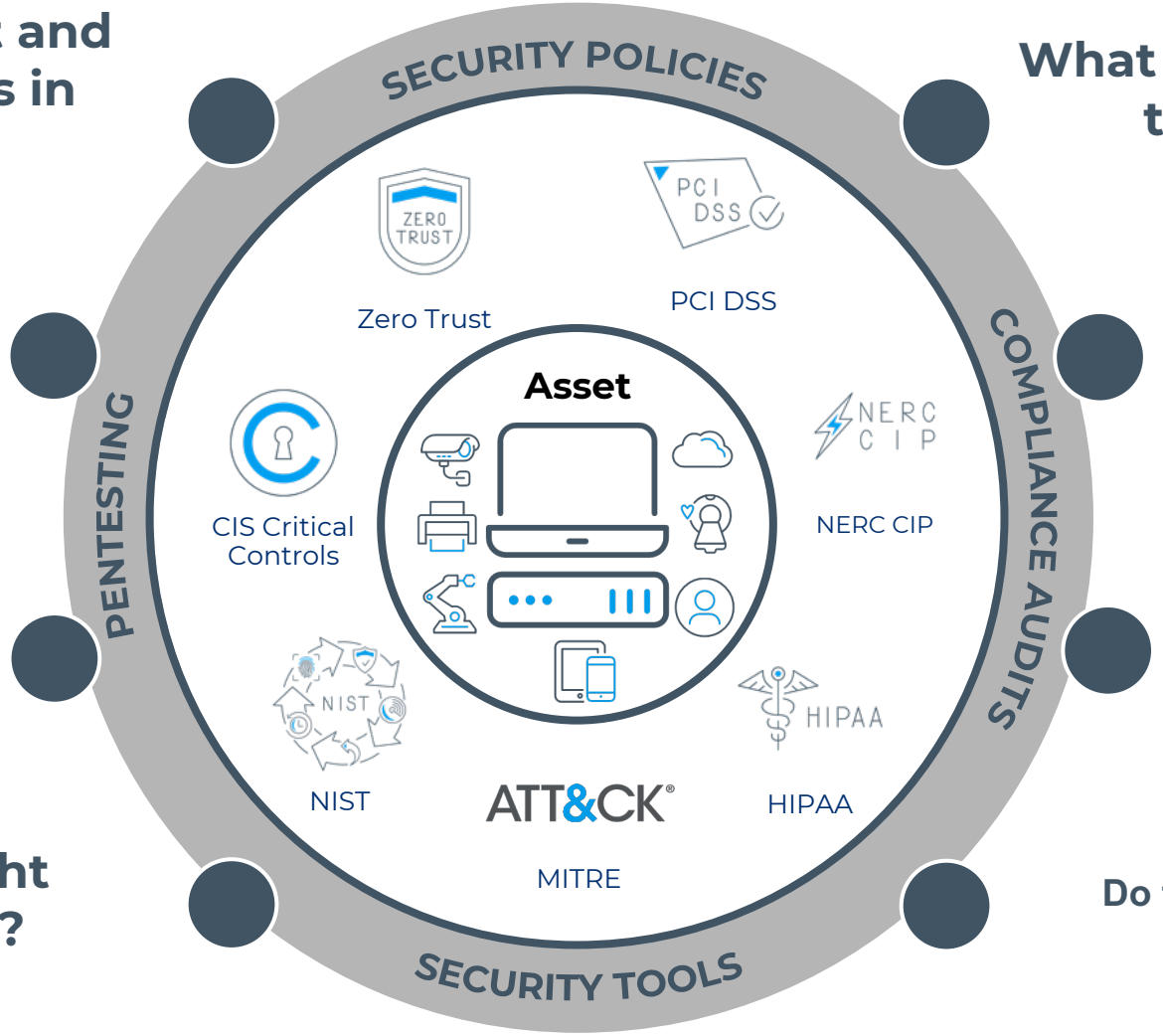
The Answers We Help Our Customers With

Can we contain a threat and reduce the blast radius in case of infection?

Are there active threats targeting them?

Are they communicating as expected?

Are they on the right network segment?



What assets are connected to your network?

How are they connected or authenticated?

Do they meet security & compliance standards?

Do they present any risks to the business?

FORESCOUT

Case Studies

NHS Fife

DAYS
to achieve full visibility into OT and unknown devices

36%
more devices discovered than expected

Hours
saved weekly in endpoint remediation

Scottish Naltional Healthcare System Gains OT Device Visibility with Forescout

HSC Health and Social Care

HOURS
is all it took to witness the power of the Forescout platform

CUSTOM
security policies using the Forescout platform

FASTER
incident response than ever before

Northern Trust Selects Forescout for Real-time Network Visibility and Control

CONVENZIS

Securing the Future of Healthcare

Navigating the Cybersecurity Landscape in the NHS

Speaking Now…

Michael Knight

Chief Technology Officer - NHS South, Central and West

SCW

NHS

Securing Primary Care

Michael Knight FBCS, CHCIO

Chief Technology Officer, NHS South, Central and West

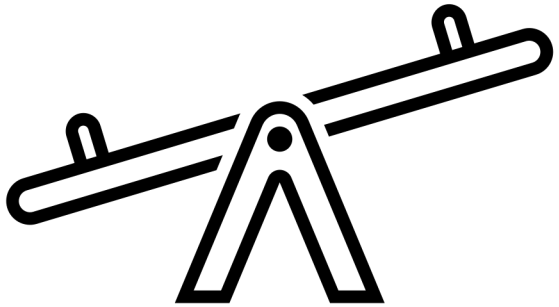
Joining the dots across health and care

Do the unglamorous well

- Patch it
- Replace it
- Access control it
- Put 3, 2, 1 backup approach in place
- Rehearse your incident management protocols

Managing Privileged Access

Legislative responsibility of a commissioner to provide assurance to NHS England



Independent contractor with a need to run their business

Enterprise approach to applications

Join up decision making across organisational boundaries

Drive greater maturity within supplier community

Use existing frameworks e.g. DTAC

Network segmentation

Increasing need for collaboration at Neighbourhood, Place and System Level

How to secure against unmanaged devices?

Focus on skills

The first rule of Dunning-Kruger club…….

Key takeaways…

Get the basics right…you reduce your vulnerability

Manage privileged access…you reduce the potential impact of compromised account

Manage third party apps…you reduce your supply chain risk

Segment networks…you reduce the threat of lateral movement and risks that are associated to being a partner

Train your people…you reduce your likelihood of compromise

SCW

contact@scwcsu.nhs.uk | scwcsu.nhs.uk | @NHSscw

CONVENZIS

Up Next…

illumio

CONVENZIS

Securing the Future of Healthcare

Navigating the Cybersecurity Landscape in the NHS

Speaking Now…

Trevor Dearing

Global Director of Critical Infrastructure Solutions - Illumio

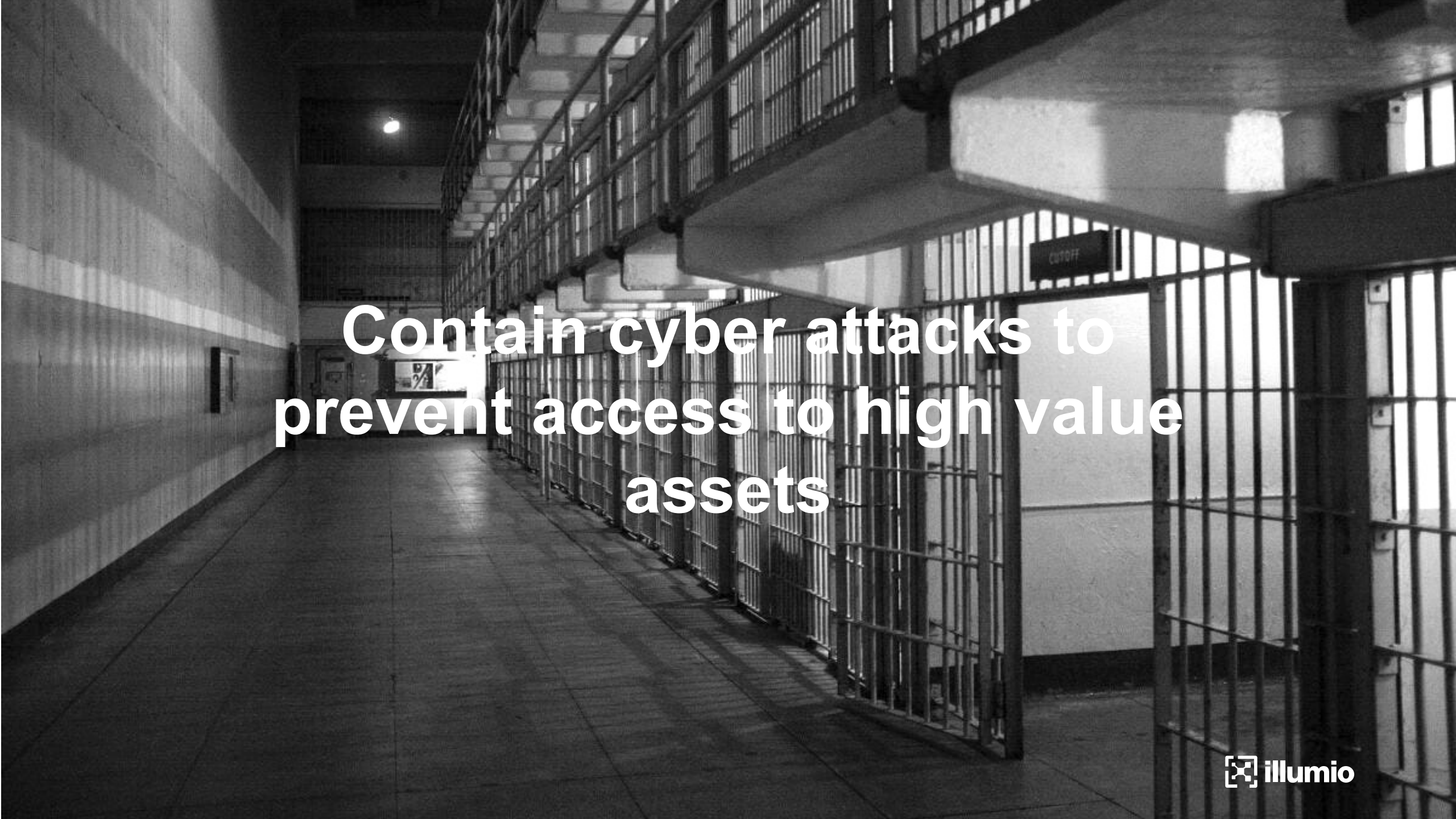
illumio

Using Zero Trust to Improve Cyber-resilience

Trevor Dearing
Director of Critical Infrastructure Solutions

Helping organisations maintain services while under attack

illumio



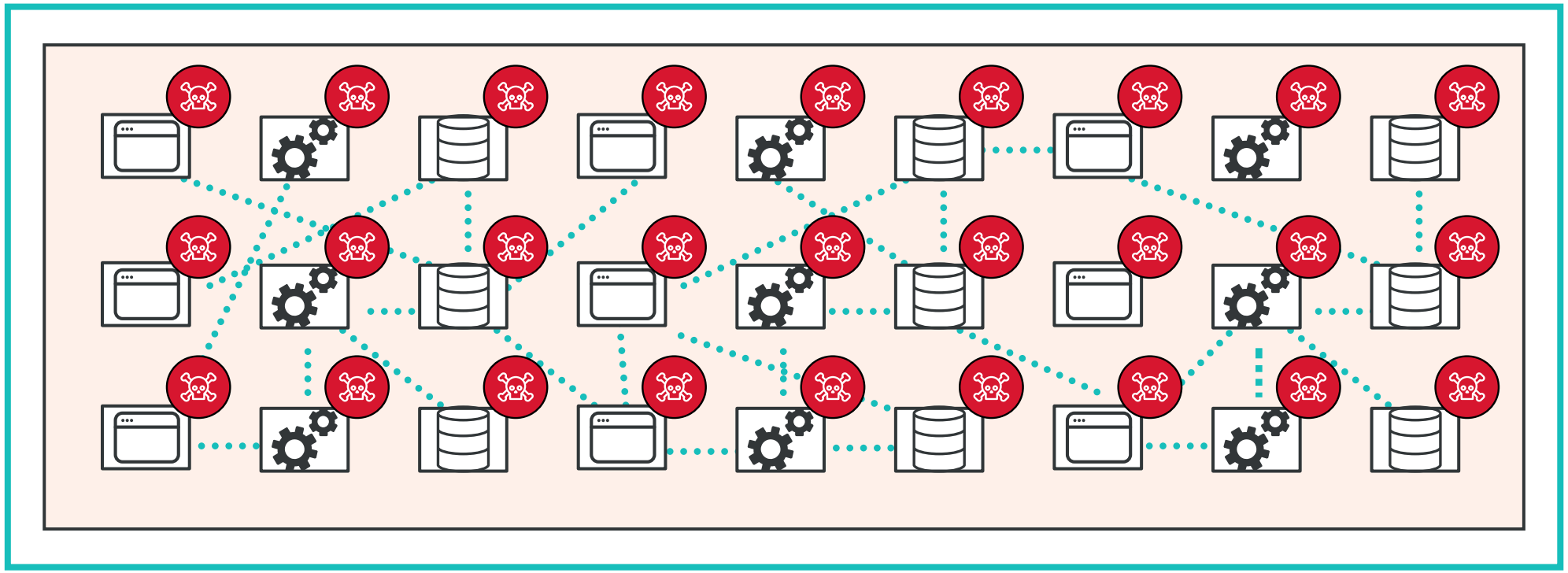
Contain cyber attacks to prevent access to high value assets

illumio

Use Zero Trust Segmentation to Provide Least Privilege Access to Assets

illumio

Attackers Need Lateral Movement

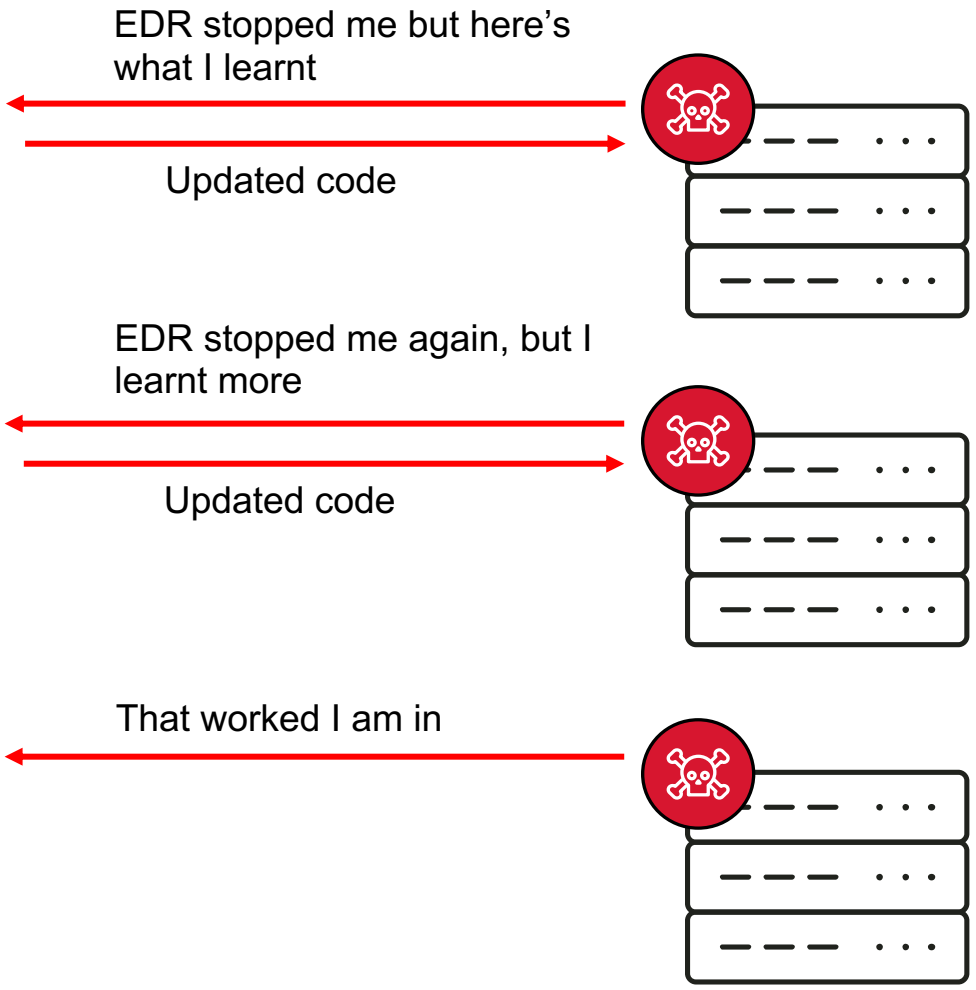


70% of ransomware traffic uses RDP

Q: Why is this becoming a bigger issue?

A: Artificial Intelligence

AI Regenerative Phone Home Morphing



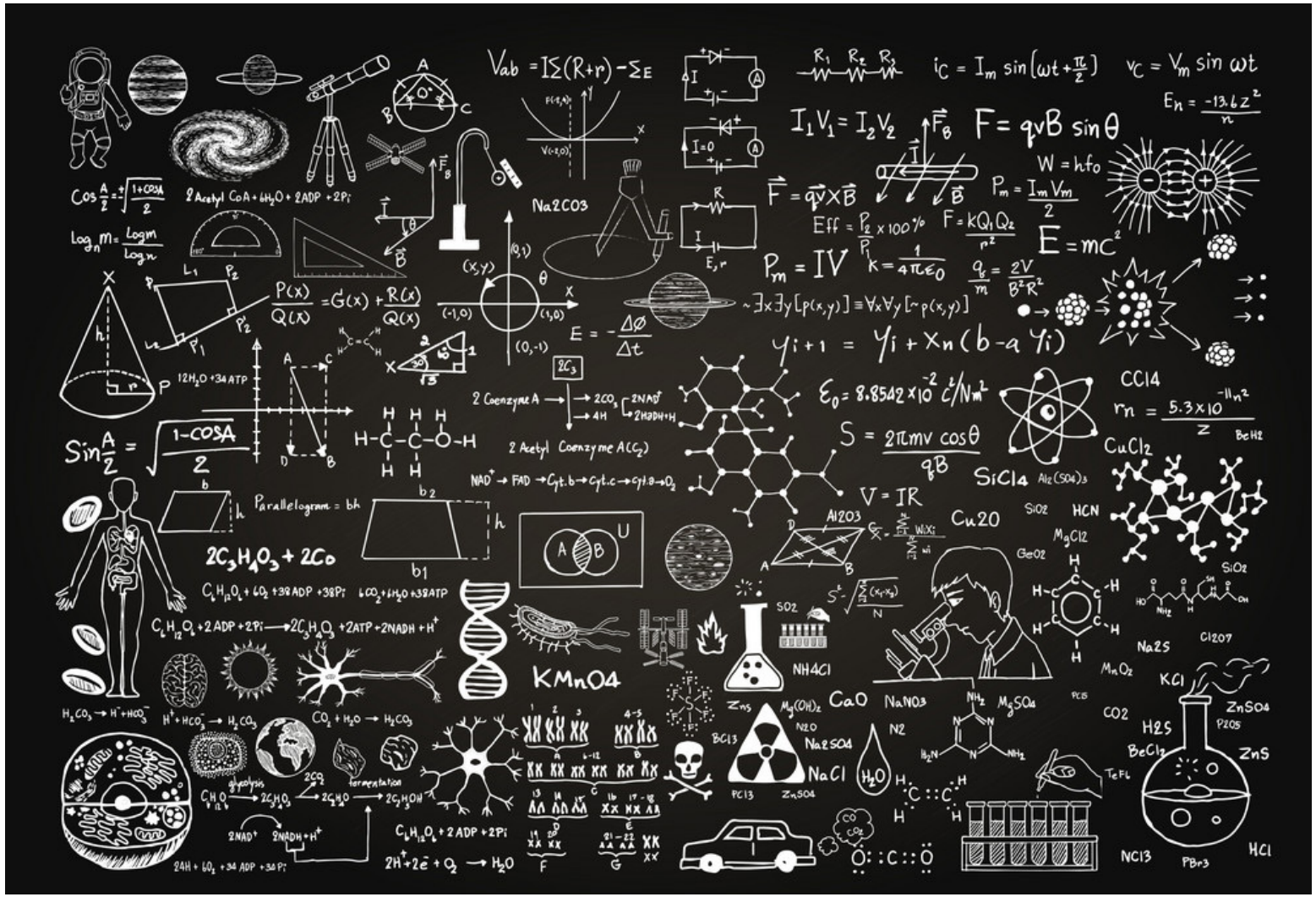
The answer is NOT more AI

It is more basic than that

- Reduce the learning surface
- Control access to resources
- Contain an attack
- Recover securely

The answer is Zero Trust

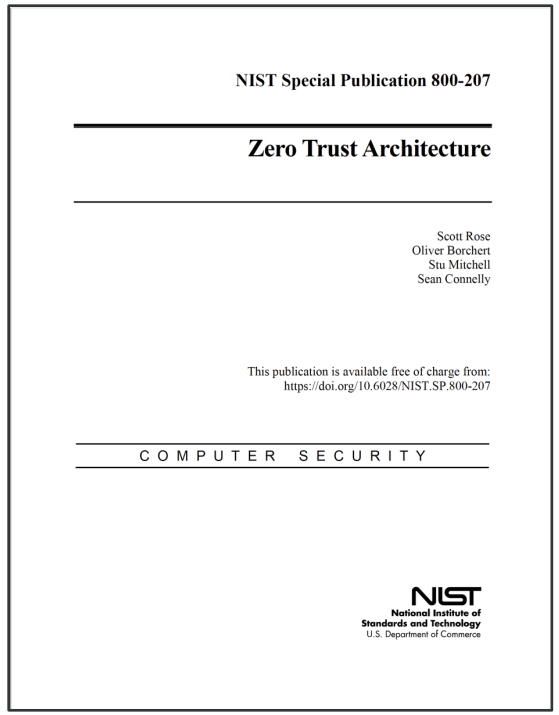
Where to Start with Zero Trust?



National Cyber Security Centre - **Zero Trust Architecture Design Principles**

1. Know your architecture
2. Know your user and device identities
3. Assess user behaviour
4. Use policies to authorize requests
5. Authenticate and authorize everywhere
6. Focus your monitoring on users, device and services
7. Don’t trust any network, including your own
8. Choose services which have been designed for zero trust

Recommended Reading - NIST



NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NIST Cyber Security Framework

What is Zero Trust?

"an evolving set of cybersecurity paradigms that move defences from static, network-based perimeters to focus on users, assets, and resources."

National Institute for Standards & Technology (NIST)

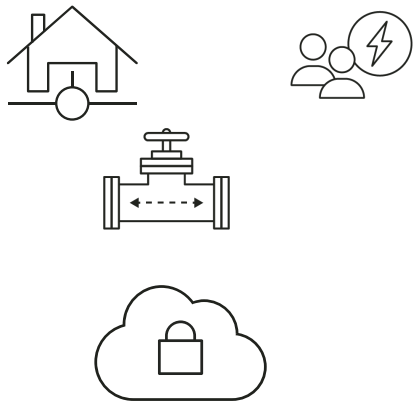
Zero Trust changes the security paradigm.

Instead of trying to identify thousands of **bad** things and stopping them.

Identify the few **good** things and allow them.

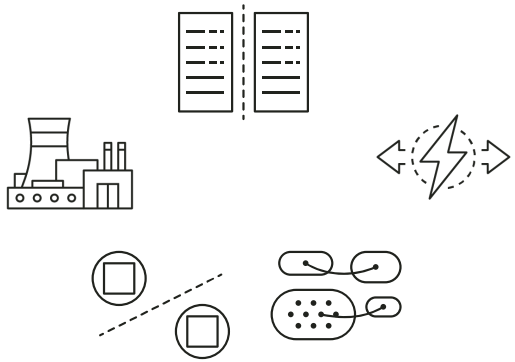
Zero Trust Taxonomy

Zero Trust Network Access



Next generation perimeter to securely identify and verify connectivity based on identity

Zero Trust Segmentation

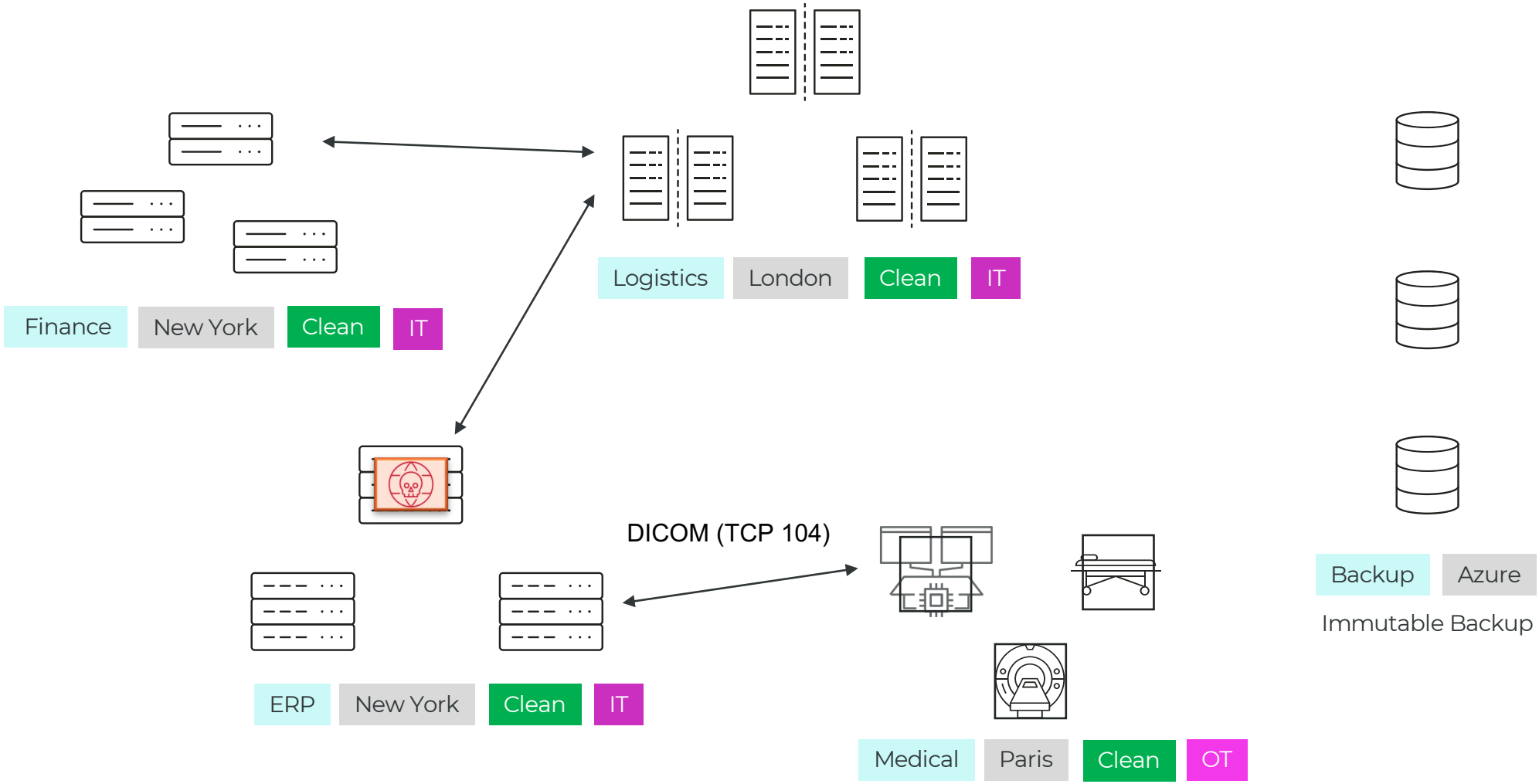


Mapping interdependencies and separating applications, IT & OT systems

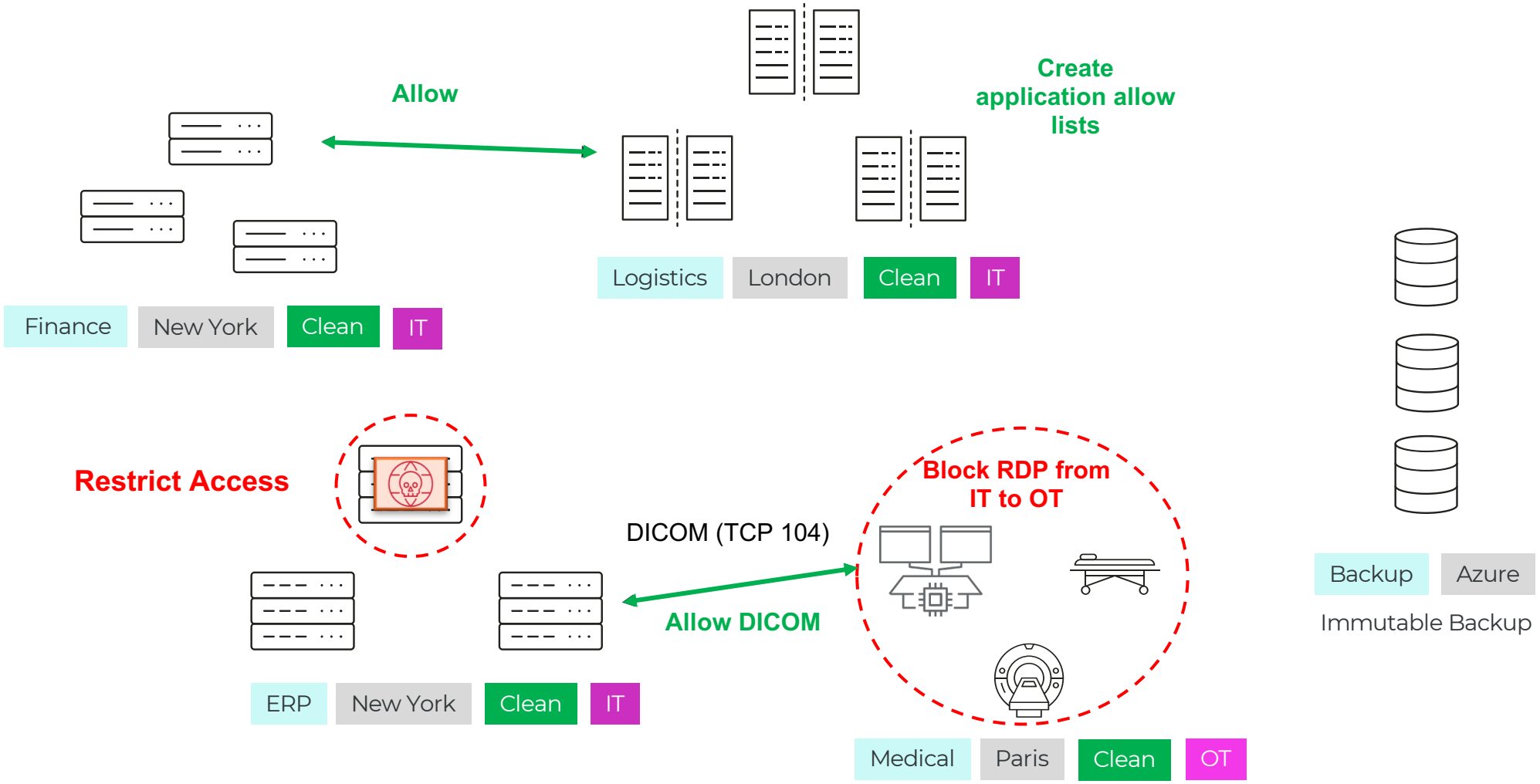
Zero Trust Data Security

Reliable and dependable data backup and restoration

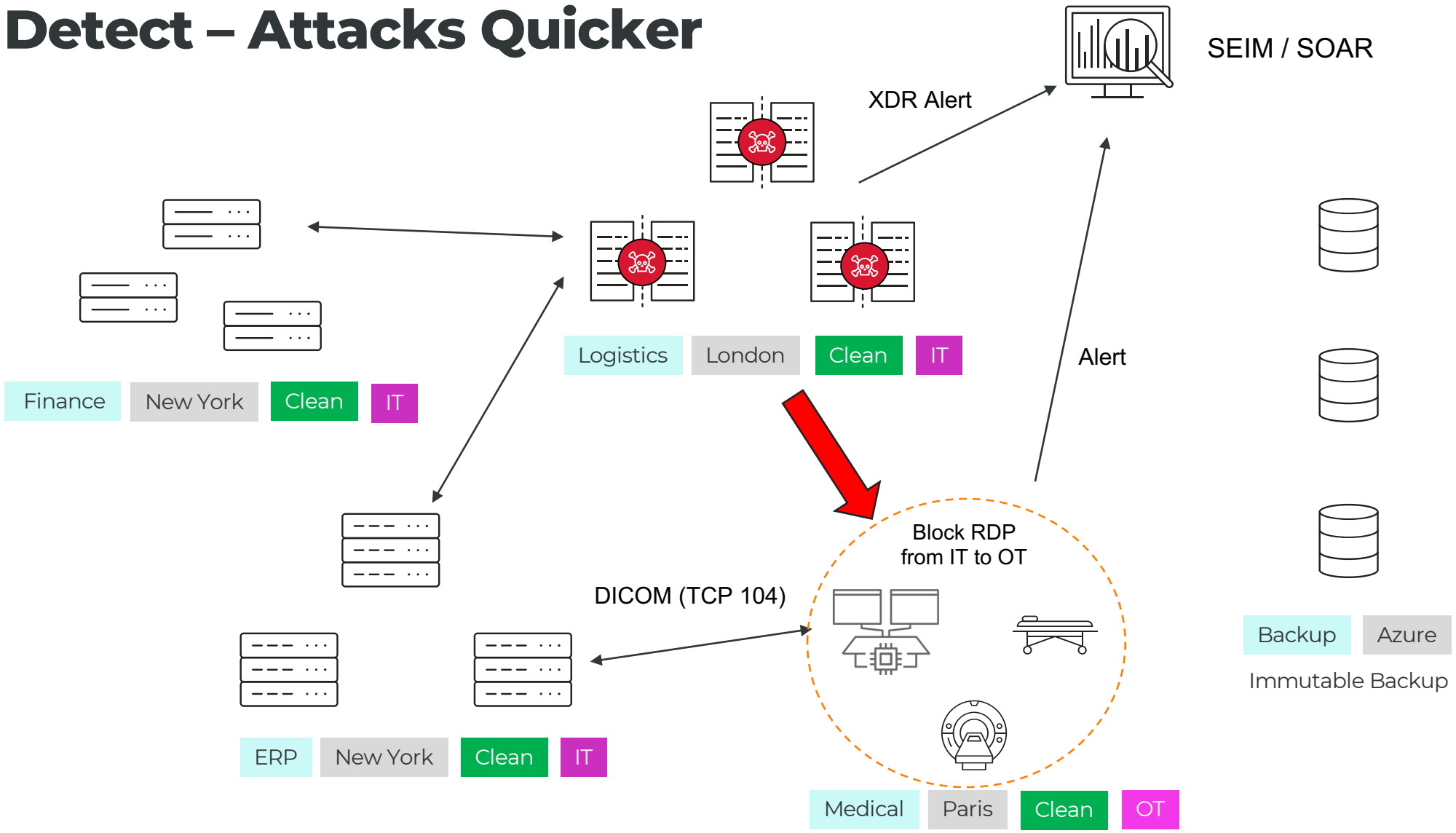
Identify – Assets, Vulnerabilities & Connections



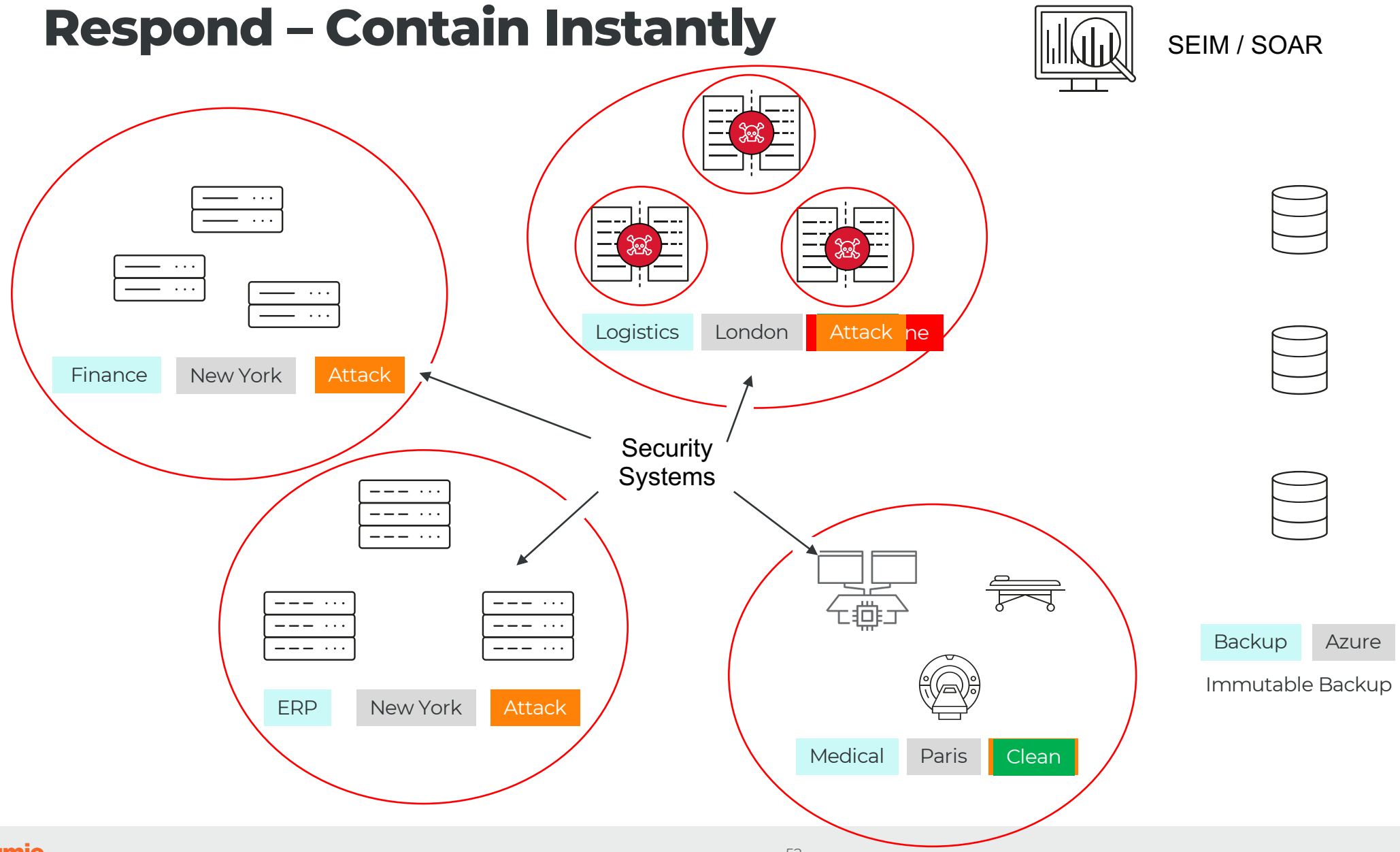
Drastically Reduce the Attack Surface



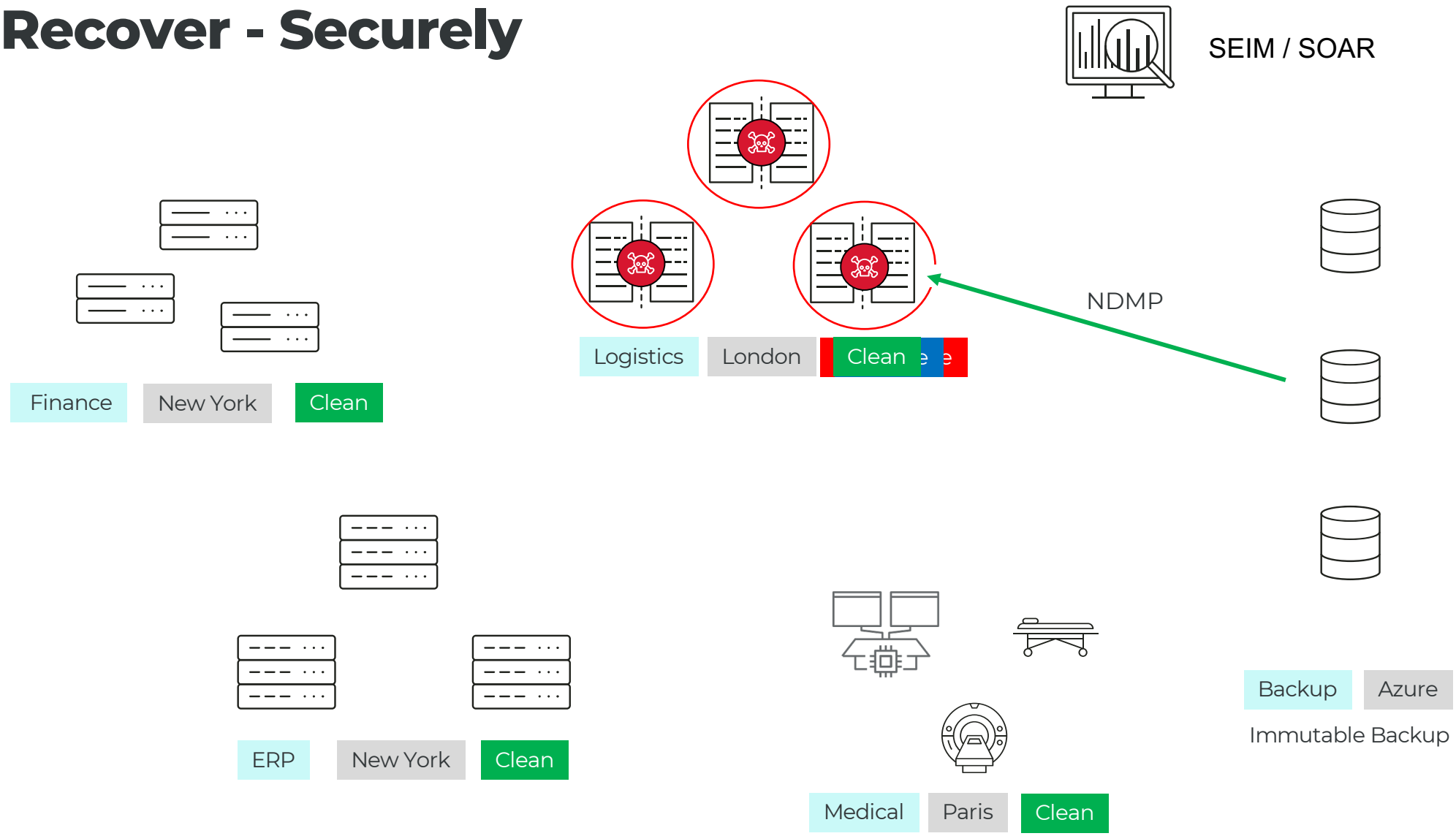
Detect – Attacks Quicker



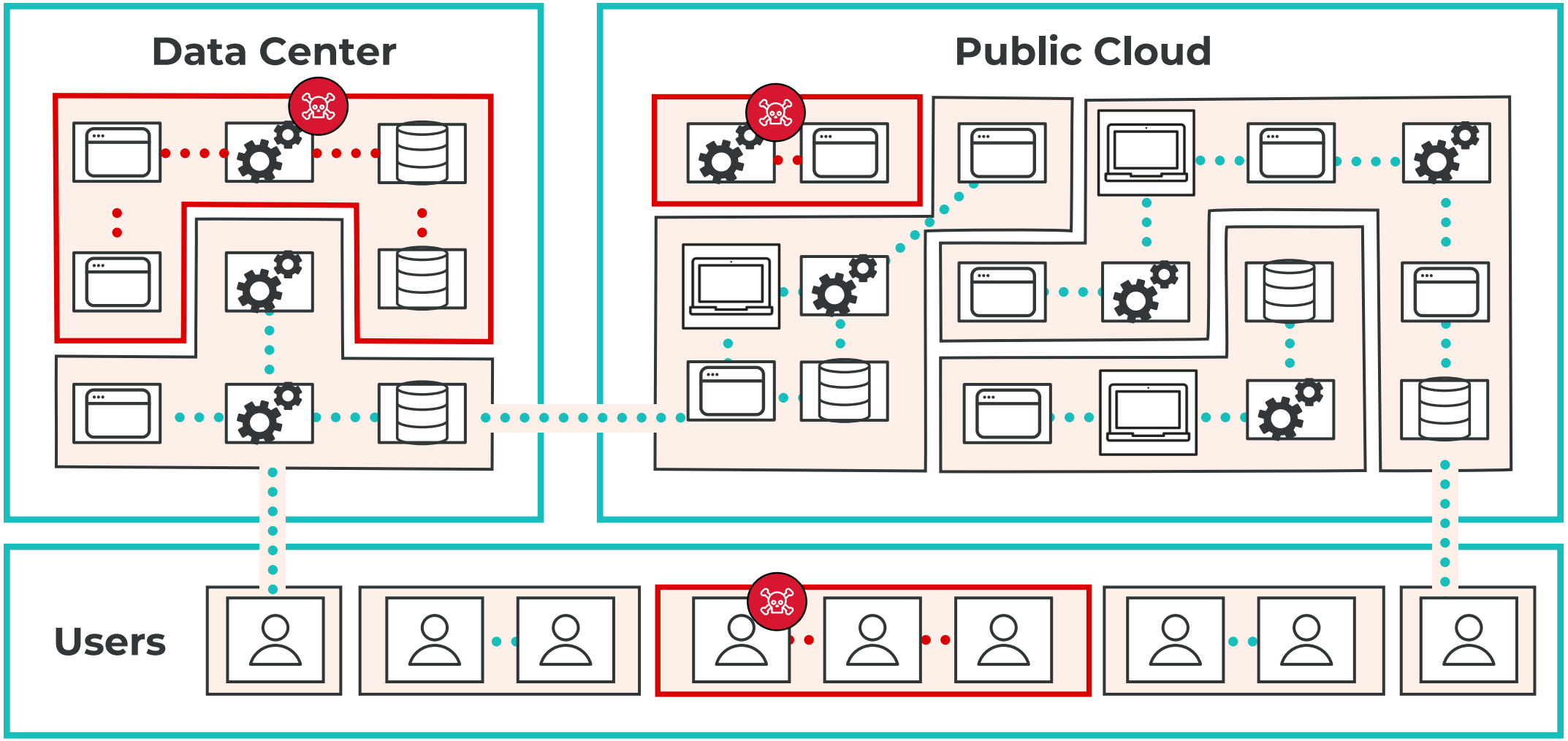
Respond – Contain Instantly



Recover - Securely



Maintaining Services



illumio

Thank you!

CONVENZIS

Up Next…

Heimdal®

CONVENZIS

Securing the Future of Healthcare

Navigating the Cybersecurity Landscape in the NHS

Speaking Now…

Mr Morten Kjaersgaard
CEO - Heimdal

Simon Sleightholm
Information Assurance & Security Manager - Northumbria Healthcare NHS Foundation Trust

Heimdal®

XDR Unleashed:

Strengthening NHS Cybersecurity with Heimdal

Securing the Future of Healthcare: Navigating the Cybersecurity Landscape in the NHS | 20 Sept, 2023

Morten Kjaersgaard
CEO, Heimdal

"Security Unification lies at the heart of fostering a robust organizational culture in healthcare.

15,000 customers worldwide including healthcare organizations benefit from our seamless security platform."

From the Media

NHS ransomware attack response criticised

17 April 2018

NHS 111 software outage confirmed as cyber-attack

6 August 2022

A software outage affecting the NHS 111 service was caused by a cyber-attack, it has been confirmed.

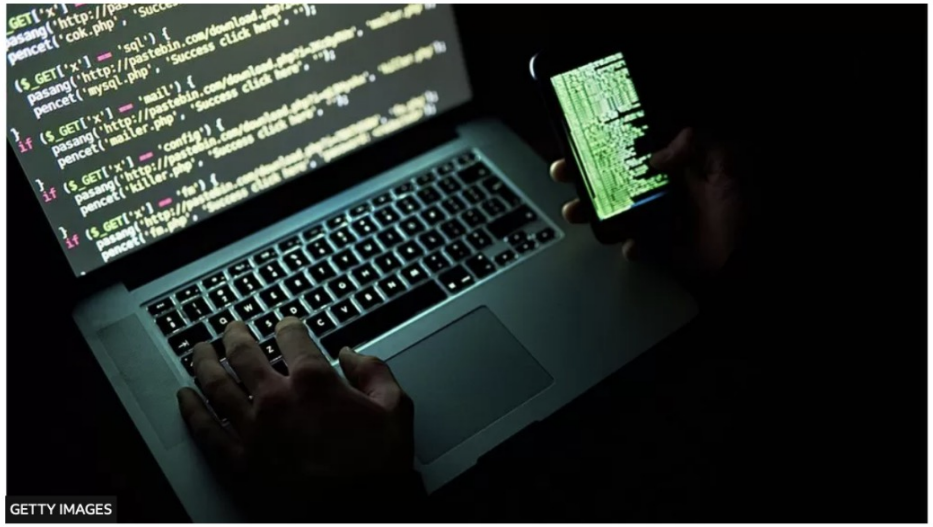
Advanced, a firm providing digital services for NHS 111, said the attack was spotted at 07:00 BST on Thursday.

The attack targeted the system used to refer patients for care, including ambulances being dispatched, out-of-hours appointment bookings and emergency prescriptions.

But the NHS said disruption was minimal.

Cyber-attack targets IT firm used by Northern Ireland's health service

11 August 2022



By Marie-Louise Connolly
BBC News NI Health Correspondent

NI health officials have shut down the health system's access to an IT company's services after the firm was affected by a cyber-attack.

NHS cyber-attack: GPs and hospitals hit by ransomware

13 May 2017

The ransomware involved has been defeated before, reports the BBC's Chris Foxx

NHS services across England and Scotland have been hit by a large-scale cyber-attack that has disrupted hospital and GP appointments.

NHS IT supplier held to ransom by hackers

11 August 2022

Why the NHS is a Prime Cybersecurity Target

The NHS exhibits what we would describe as a sizable cyberattack surface—an expansive perimeter—due to its status as a substantial sector with a considerable population of individuals and an extensive array of devices.

The risks are extremely elevated:

- **Digital patient records**
- **Downtime is not an option**
- **Ransomware attacks**
- **Patient priority**

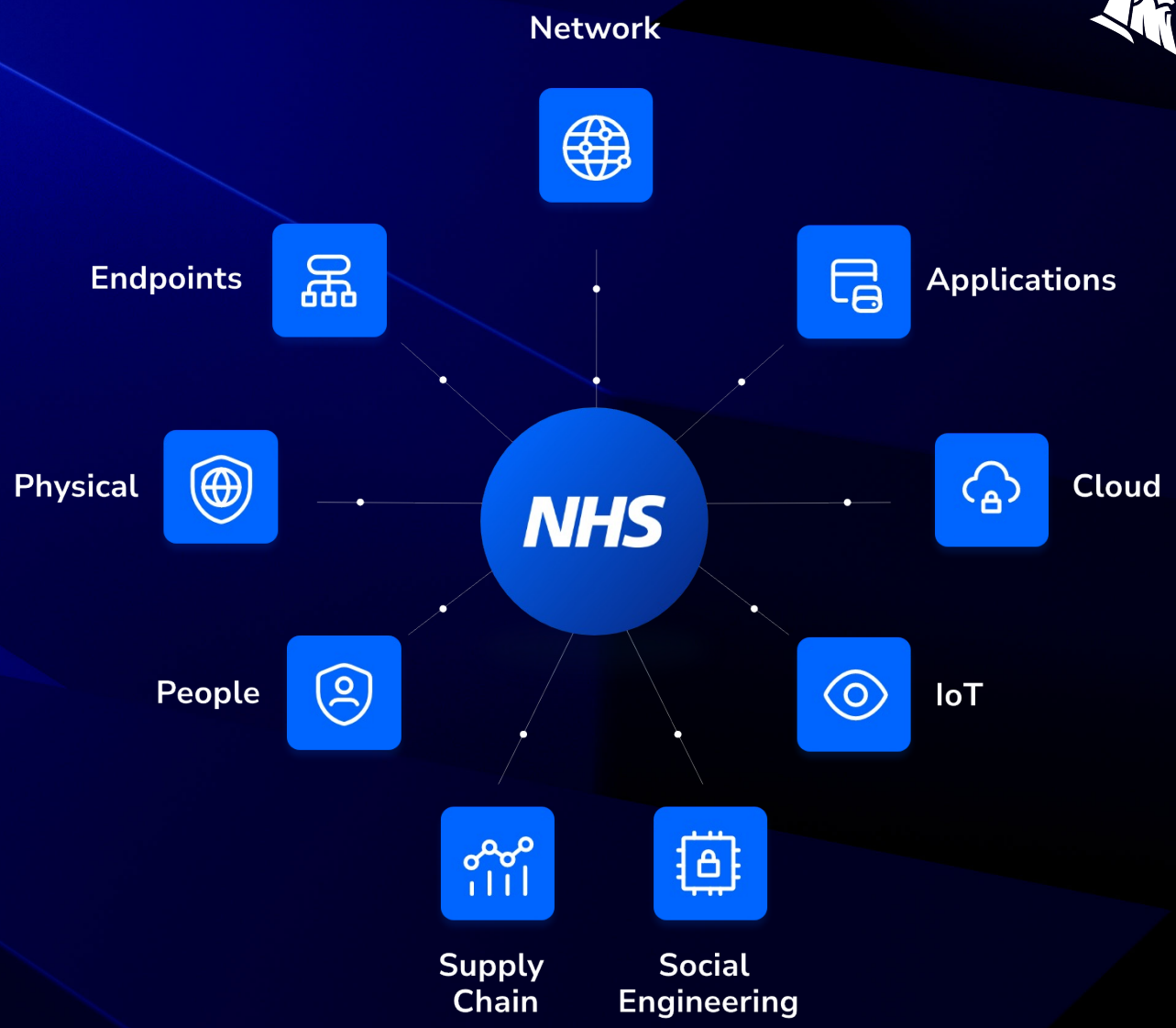
Heimdal Intel: From our Analysts

Over the past three months, the total analysed traffic requests from just two healthcare clients have exceeded 3.3 million.

- **3.3M Suspicious connections**
- **490K Attacks Thwarted**
- **152K Patches Delivered**
- **13K Vulnerabilities Closed**

Navigating the Vast Attack Surface:

Routes & Risks for NHS Cybersecurity



Introducing Heimdal:
Your Healthcare Cybersecurity Shield

Comprehensive Protection

Reduce Complexity

Streamline Compliance

Why Partner with **Heimdal**

- ✓ **Healthcare Industry Expertise**
- ✓ **Comprehensive Protection**
- ✓ **Specialist in Ransomware Defence**
- ✓ **Maintain Regulatory Compliance**
- ✓ **Simplify Management**
- ✓ **Proactive Threat Mitigation**
- ✓ **Cost Efficiency**
- ✓ **24/7 Support**

NETWORK computing AWARDS 2023 WINNER CLOUD BASED SOLUTION OF THE YEAR

Expert Insights Top Solution 2023

SOURCEFORGE Top Performer Summer 2023

computing Security Excellence Awards 2023 WINNER Risk Management Award

SOURCEFORGE ★★★★★

Expert Insights ★★★★½

Capterra ★★★★½

Gartner peerinsights ★★★★★

Heimdal XDR:

Powered by our Unified Security Platform

With the Heimdal XDR, you can eliminate the complexity of managing multiple security solutions and gain the peace of mind that comes with having a comprehensive, integrated approach to cybersecurity.

"Front Row Security like a Swiss Knife."

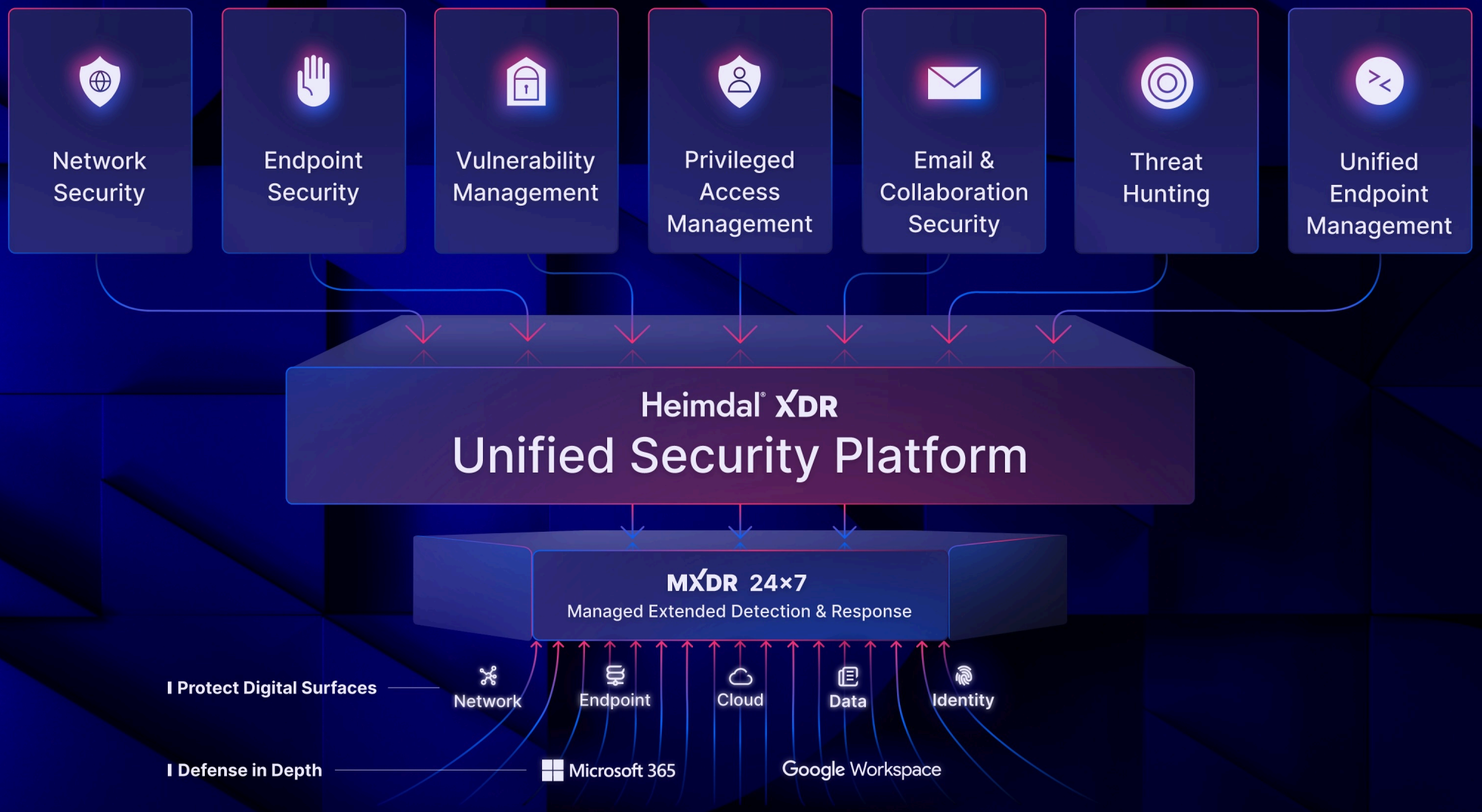
Solid security foundation with a wide coverage without compromise on your environment.

- Stephan V, Head of Group IT

Heimdal XDR

- ✓ Widest XDR suite, 10-in-1 award-winning solutions
- ✓ Unified console for all products across attack surfaces
- ✓ Gen-AI threat intelligence
- ✓ MITRE ATT&CK techniques hunting supported
- ✓ Deep, native uni-lateral telemetry between products, inventory, users and processes
- ✓ Worlds only all-in-one Threat Hunting and Platform
- ✓ Optional on-demand Managed SOC services

Heimdal for Healthcare – Comprehensive Protection Suite



Heimdal for Healthcare – The Essentials

Network Security
- DNS Security - Network
- Cloud Ransomware Protection

Endpoint Security
- DNS Security - Endpoint
- Next-Gen Antivirus, Firewall & MDM
- Ransomware Encryption Protection

Vulnerability Management
- Patch & Asset Management
- Infinity Management

Privileged Access Management

Email & Collaboration Security

Threat Hunting

Unified Endpoint Management

Heimdal® XDR
Unified Security Platform

MXDR 24×7
Managed Extended Detection & Response

- Protect Digital Surfaces
- Defense in Depth

Network | Endpoint | Cloud | Data | Identity

Microsoft 365 | Google Workspace

Heimdal for Healthcare – One Platform. Total Security.

Network Security
- DNS Security - Network
- Cloud Ransomware Protection

Endpoint Security
- DNS Security - Endpoint
- Next-Gen Antivirus, Firewall & MDM
- Ransomware Encryption Protection

Vulnerability Management
- Patch & Asset Management
- Infinity Management

Privileged Access Management
- Privilege Elevation & Delegation Management
- Application Control

Email & Collaboration Security
- Email Security
- Email Fraud Prevention

Threat Hunting
- Threat-hunting & Action Center

Unified Endpoint Management
- Remote Desktop
- BitLocker Management*

*coming soon

Heimdal® XDR
Unified Security Platform

MXDR 24×7
Managed Extended Detection & Response

- Protect Digital Surfaces
- Defense in Depth

Network | Endpoint | Cloud | Data | Identity

Microsoft 365 | Google Workspace

NHS Trusts: Stand Strong Against the Rising Tide of Ransomware Threats

Join the ranks of other NHS Trusts and fortify your defences against ransomware attacks with Heimdal.

- Bolster your defences with potent ransomware protection
- Safeguard your organization from disruptions and lateral spread
- Ensure compliance with legal & industry regulations

SCAN ME

Complimentary Protection Pack

Co-Speaker:

Simon Sleightholm,

NHS Northumbria, Information Assurance & Security Manager

- Your experience with Heimdal as a customer
- Talk us through the implementation you had
- How has your day to day with Heimdal been

Heimdal®

Thank You

Q&A

CONVENZIS

Securing the Future of Healthcare

Navigating the Cybersecurity Landscape in the NHS

Speaking Now…

Tej Gudka

Head of Cyber Security - NHS Arden & GEM CSU

NHS
Arden and
Greater East Midlands
Commissioning Support Unit

The importance of Multi Factor Authentication for NHS organisations

Tej Gudka
NHS Arden & GEM CSU

Navigating the cybersecurity landscape in the NHS

www.ardengemcsu.nhs.uk

Arden&GEM
Health and social care systems support

Session overview

- Introduction to Multi Factor Authentication (MFA)
- NHS MFA Policy launch
- Our implementation approach – NHS Mail
- Our progression
- Overcoming challenges
- Lessons learned
- Questions

About NHS Arden & GEM CSU

NHS
Arden and
Greater East Midlands
Commissioning Support Unit

OUR CUSTOMERS

90+

Working with a customer base of 90+ organisations across health and care systems

- NHSE
- ICSs
- ICBs
- Trusts
- Primary Care
- Local Authorities

OUR BUSINESS

£95m
Turnover 2021/22

£34m
Generated in new business 2021/22

OUR PEOPLE

1,000+
Multidisciplinary staff

OUR IT SERVICE

Health Business Awards 2021 WINNER

Winners in the Healthcare IT category for developing a national system

Providing day-to-day IT support to over:

60,000 devices

25,000 users

500 sites

Cyber security team of **7**

Helping systems to:

- Accelerate digital transformation
- Scale digital diagnostics
- Embed resilient connectivity solutions

OUR ACCREDITATIONS

INVESTORS IN PEOPLE® We invest in people Gold

INVESTORS IN PEOPLE® We invest in wellbeing Gold

ISO 9001 ISOQAR REGISTERED alcumus.com UKAS MANAGEMENT SYSTEMS 0026

ISO 14001 ISOQAR REGISTERED alcumus.com UKAS MANAGEMENT SYSTEMS 0026

CYBER ESSENTIALS CERTIFIED PLUS

What is MFA – Multi Factor Authentication

MFA is something you know (password), something they have (mobile device) or something they are (biometric)

Something you know
Username, Password, memorable information

It protects against unauthorized access
Can prevent 99.9% of account compromise attacks

Something you have
Mobile device, Fido2 token, Smartcard

Multi?
at least two different factors (know, have, are)

Something you are
Fingerprint, Retina scan, Facial features

The benefits of MFA

MFA is an easy to use and effective method of protecting accounts and systems from unauthorised access

It significantly increases the security of accounts and systems
making it more difficult for bad actors to gain access

It protects against password-based attacks
including phishing and the exploitation of harvested passwords

It improves security for remote access
providing an additional layer of security in a time of increased need for remote access

It complies with security requirements
for certifications such as Cyber Essentials / DSPT

It protects patient information
reducing the risk of unauthorised access or data breaches

It offers stronger protection
when compared to using just a password

The challenges of MFA

MFA needs careful planning, consideration and ensure stakeholders are included in design, implementation and feedback

Slowing users down
Making it more difficult for users to login

Cost
Finding the right solution within budgetary constraints

Ensuring it complies with security requirements
Cryptography / Best practice

Understanding the Scope
Which areas are most at risk – External facing services

Situations where it can be difficult to implement
Prisons, Mental Health settings

Auditing
Ensuring checks are in place to check efficacy and it is not being by-passed

NHS MFA Policy

NHS
Arden and Greater East Midlands
Commissioning Support Unit

MFA Policy Objective & Requirement

2

- Promote MFA to manage risks of user credential compromises:
- MUST enforce on all remote user access to systems
- MUST enforce on user privileged user account to externally hosted systems
- SHOULD enforce on all privileged user access to all other systems

1

NHS England MFA Documentation

- MFA Policy – here
- MFA Guide – here
- MFA Enforcement Intent - click here

Arden&GEM
Health and social care systems support

NHS MFA Policy

Arden and Greater East Midlands Commissioning Support Unit

4 MFA Enforcement Intent

- Detailed action Plan by 29th February 2023
- Full compliance by 30th June 2024

3 MFA Guide

- Details MFA Policy Objectives and Requirements
- Exceptions
- All are permitted factors, choosing factors – SMS, Fido
- Further guidance from NCSC, NIST, CISA etc.

Arden&GEM
Health and social care systems support

NHS Mail MFA - Our planning

NHS
Arden and Greater East Midlands
Commissioning Support Unit

2 Technical options appraisal

- Selected the Microsoft Authenticator app with an SMS backup option
- Tested NHS Smartcards and FIDO2 tokens

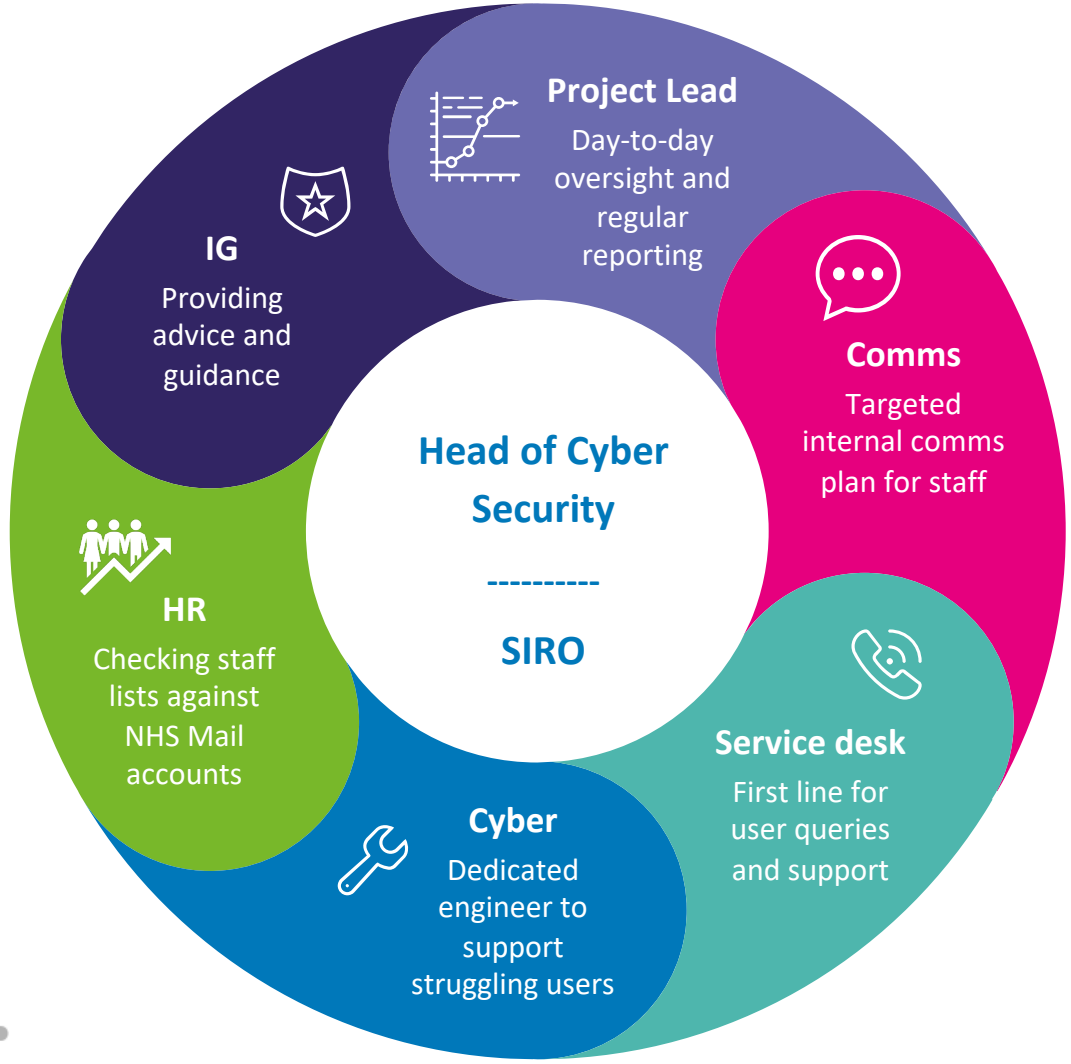
1 edback paper presented to Exec

- Turning on MFA across NHS Mail was recommended
- The process and potential challenges were discussed and agreed with our Senior Information Risk Owner (SIRO)

Arden&GEM
Health and social care systems support

Our implementation approach – multidisciplinary

The multidisciplinary project team was designed to bring together all of the **key stakeholders** throughout the organisation.



> ***As the executive-level owner of information risk, I am responsible for ensuring that information threats and vulnerabilities within the organisation are identified and mitigated against. The cyber security team did an efficient and effective job of implementing MFA, not only by supporting a wide range of users to enable stronger protection within their NHS Mail accounts but also by increasing understanding of why this protection is needed in the first place.***

Helen Seth, Director of Business Intelligence and Provider Management and SIRO at NHS Arden & GEM CSU

Our implementation approach - targeted

We decided to pursue a two-stage approach to implementation which targeted those colleagues at heightened risk first, before rolling out to the wider staff group

1. Teams at heightened risk

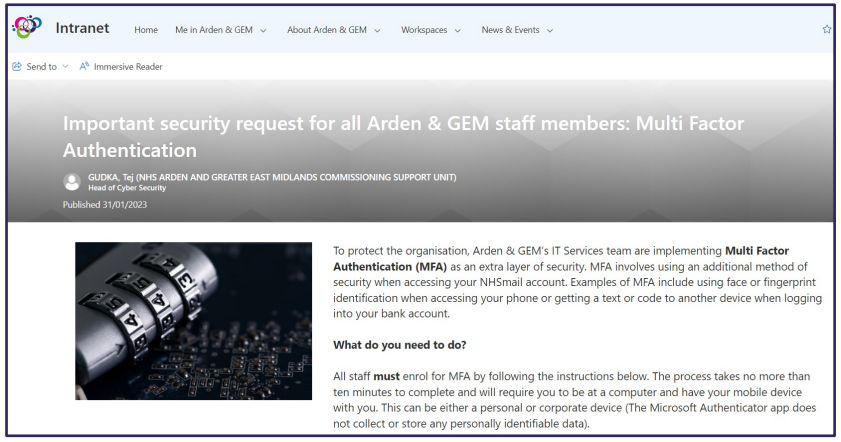
We initially targeted colleagues in the following teams who were assessed as being at heightened risk from cyber threats:

- Finance
- HR
- Procurement.

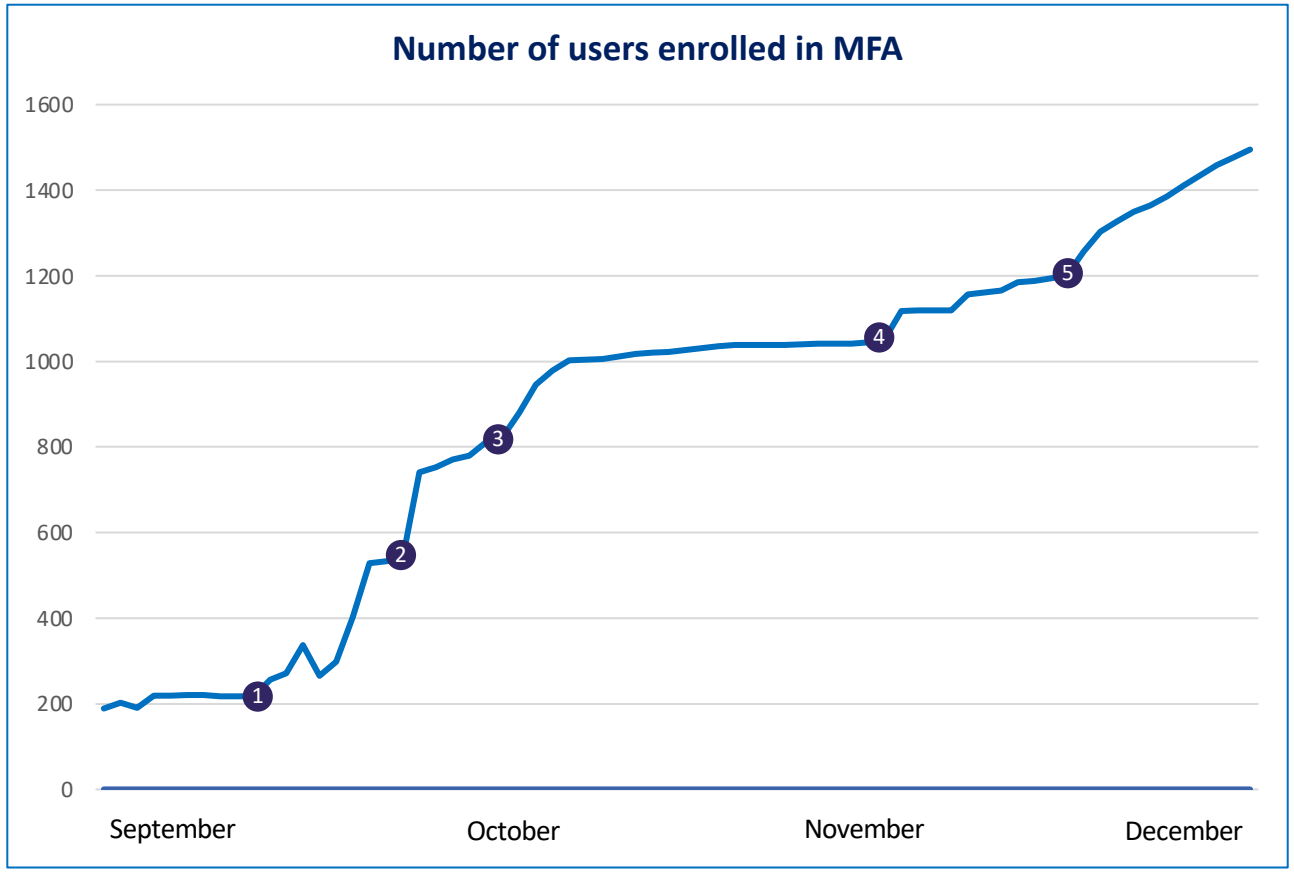
2. Entire organisation

We then created a 3-month plan for the rest of the organisation, including:

- An intranet page with FAQs section
- An all user email inviting staff to enrol with MFA with clear instructions and a deadline
- Targeted emails, sent at two-weekly intervals, to those users who didn't enrol by the deadline
- Further targeted emails, copying in line managers
- A final reminder from the Head of Cyber Security reiterating the importance of this project
- An agreed cut-off date, at which point MFA functionality was turned on automatically.



Our progress



- 1500 staff members enrolled in MFA over the three-month project
- Before the rollout commenced 189 staff members such as local administrators (LoA) and Cyber Security staff had already enrolled.

1. Comms plan commenced with intranet page and internal news story
2. First targeted email sent to all users
3. Second targeted email sent to remaining users
4. Email sent to remaining users and their line manager
5. MFA is enforced for 30 users per day.

Overcoming challenges

Arden and Greater East Midlands Commissioning Support Unit

COLLEAGUE RESISTANCE

Some colleagues were resistant to using their personal mobile devices for the MFA process

Share guidance (Multi-Factor Authentication (MFA) – NHSmail Support)

Getting support – SIRO / Exec / SLT

Reinforce the benefits

MAINTAINING COMPLIANCE

MFA cannot yet be turned on by default in NHS Mail accounts as individuals need to accept the UAP

New starter policies - changes

Monthly audits – unenrolment review, new starters checks

Arden&GEM
Health and social care systems support

Lessons learned

Build MFA into your policies

Work with HR on new starter policies and procedures

Monthly audit processes

Know your 'why'

Communicate the benefits of MFA

A key 'why' for us was a near miss incident

Appraise technology options

MS Auth App / SMS / FIDO2 / Smartcard

Secure senior buy in

At Exec level / from your SIRO / SLT

Work closely with your comms team

Have a tiered approach to contacting staff

Start with people with the greatest risk

In particular those teams responsible for finance/payment tasks

Any questions?

Get in touch with us at:

www.ardengemcsu.nhs.uk

@ardengem

contact.ardengem@nhs.net

Arden&GEM
Health and social care systems support

CONVENZIS

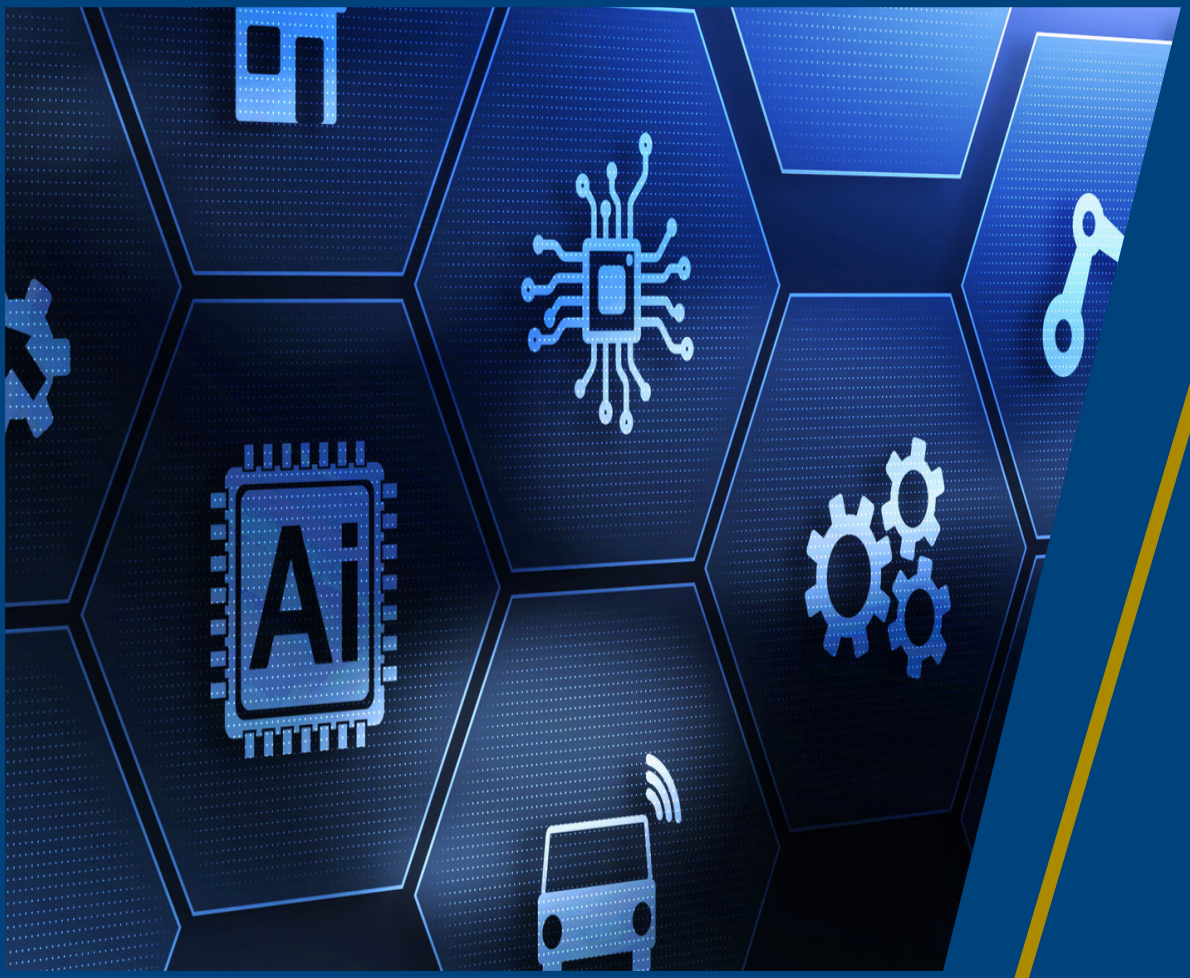
Securing the Future of Healthcare

Navigating the Cybersecurity Landscape in the NHS

Speaking Now…

Andy Williams

Interim Chief Digital Officer/Digital and Innovation Lead/Managing Director - Harrogate and District NHS Foundation Trust/ Leeds Teaching Hospitals NHS Trust/ AHLC Solutions Limited



AHLC Solutions

SECURING THE FUTURE OF HEALTHCARE: NAVIGATING THE CYBERSECURITY LANDSCAPE IN THE NHS

The Impending Cyber Pandemic in Health and Social Care: Are We Prepared?

Andy Williams, 20th September 2023

Our Company

AHLC Solutions

Who we are

A digital health and social care solution agency working in collaboration and committed to supporting the adoption, implementation and spread of innovation within and across the sector.

What we do

Support NHS, Public, Private and Supplier Sectors

Facilitate Adoption and Spread of UK and International Technologies

Collaborate through Partnerships and Community

Promote Innovation through Engagement and Events

Andy Williams

Founder and Executive Director

- Interim Chief Digital Officer, Harrogate NHS Foundation Trust
- Interim Chief Digital Officer, Humber and North Yorkshire ICB
- Digital Advisor for 'Building the Leeds Way', Hospitals of the Future
- Digital Strategy Advisor

Lambros Lambrou

Chief Technology Officer

- A highly motivated and accomplished TOGAF 8 certified Principal Architect
- 25 years of experience and a proven track record of delivering across multiple large-scale organisations
- Led the technical workstream of the National Pathology Imaging Programme, delivering the centralised capability to facilitate Digitisation of Pathology services across seven Acute Trusts in West Yorkshire

Louise Sinclair

Communications and Engagement Officer

- An award-winning senior marketing professional adept at translating complex organisational strategy into focused, impactful and measurable brand, marketing and communications campaigns.
- Ability to create strong and trusted relationships with natural diplomacy and people skills at all levels of stakeholders, including board level.
- Worked across numerous private and public sectors including health, technology, sport, charities, retail, B2B and financial services.

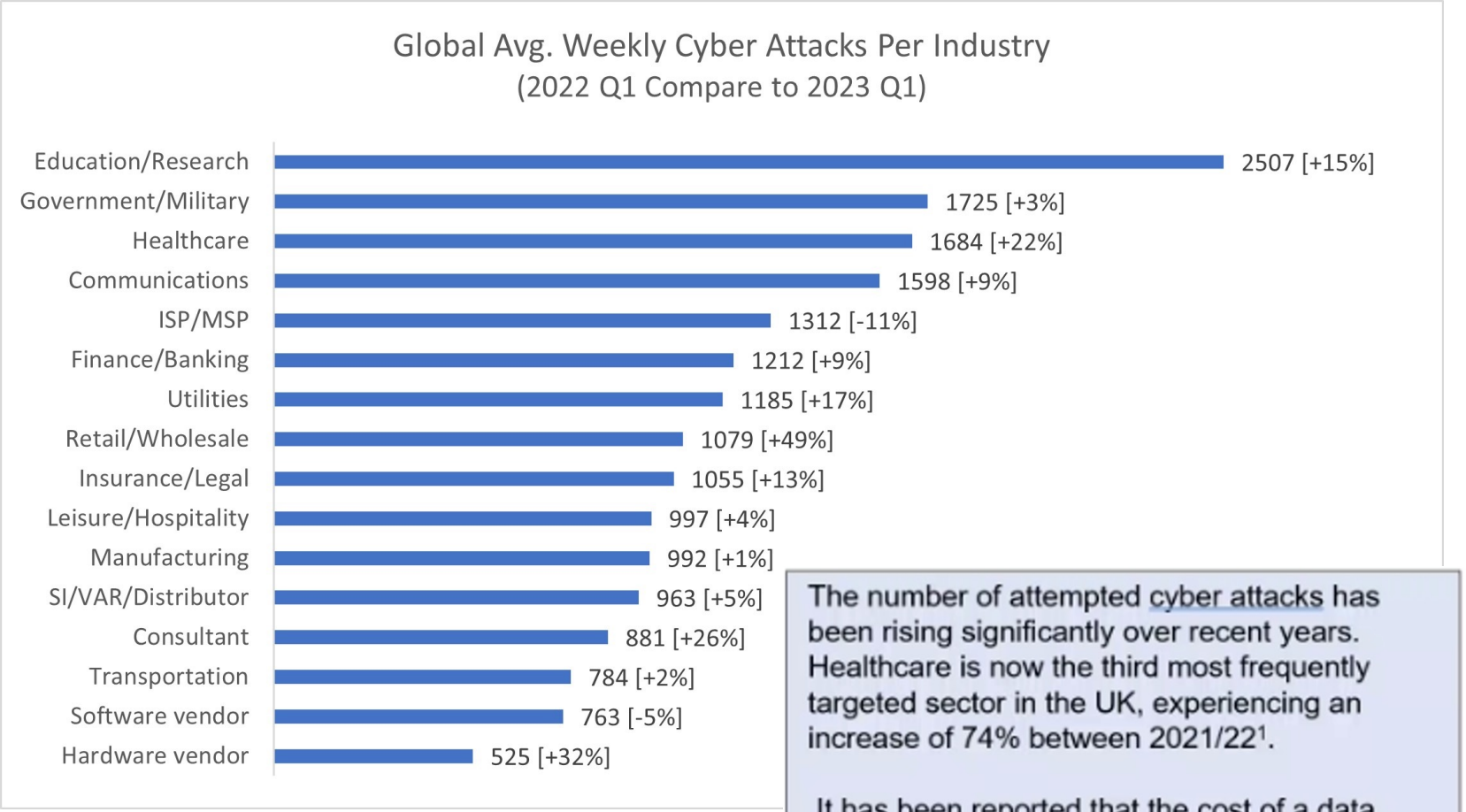
Rachel Marshall

Executive Project Officer

- Over 25 years' experience providing business and project office support to a range of industries.
- Underpins the successful and smooth running of back office functions and also delivering support for various project based activities. Services include:
  - Project Management Office support
  - Project and event management

1. On the Rise

- In today's interconnected world, whether we realise it or not the threat of a cyber-attack happens every day to every sector.
- Health and care is no exception; in fact, it is scarily on the rise!
- Our reliance on technology and the eerie prowess of hackers has given rise to a real cyber pandemic.
- This session aims to shed light on the importance of preparing for cyber-attacks for the health and care sector and key steps to mitigate the risk.



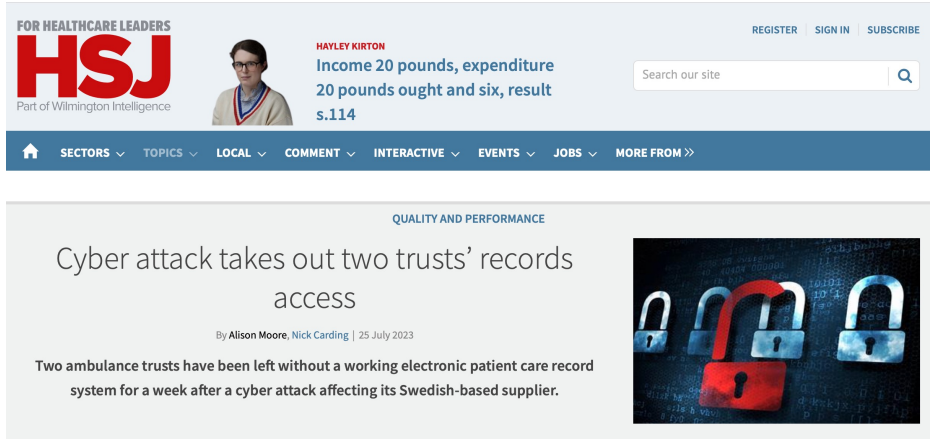
The number of attempted cyber attacks has been rising significantly over recent years. Healthcare is now the third most frequently targeted sector in the UK, experiencing an increase of 74% between 2021/22[1].

It has been reported that the cost of a data breach in the healthcare sector has increased by 53.2% since 2020, at an average cost of £8.5 million[2].

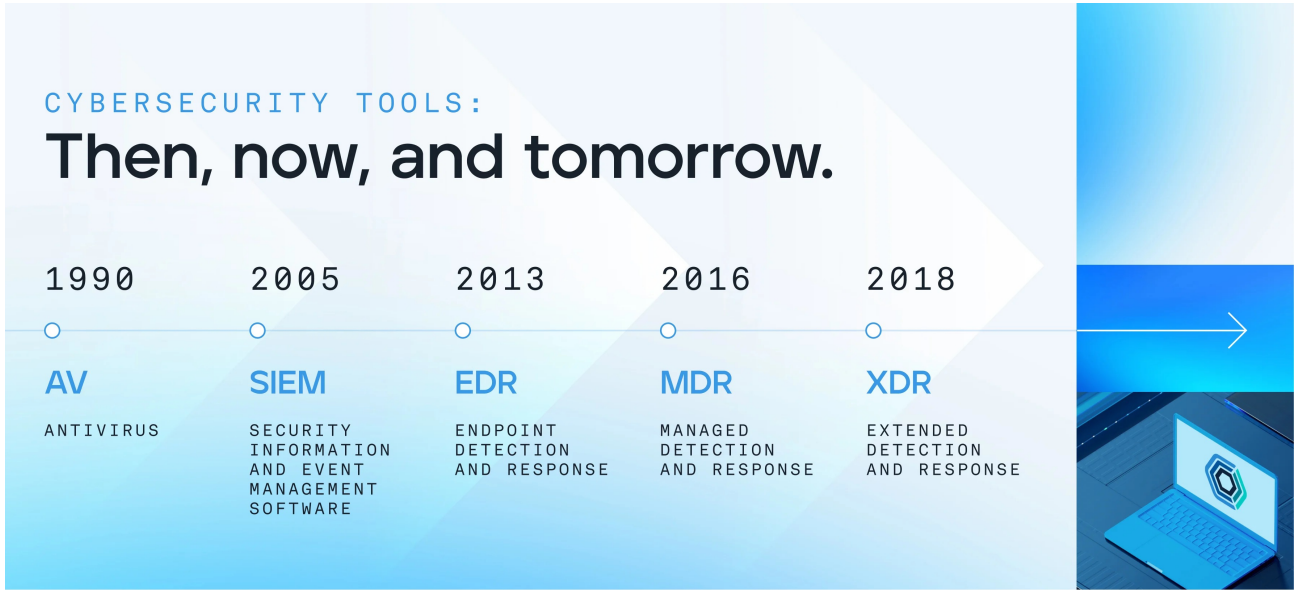
The NCSC dealt with 777 incidents (2021) an increase on last year (2020) - of which 20% were linked to the health sector[3].

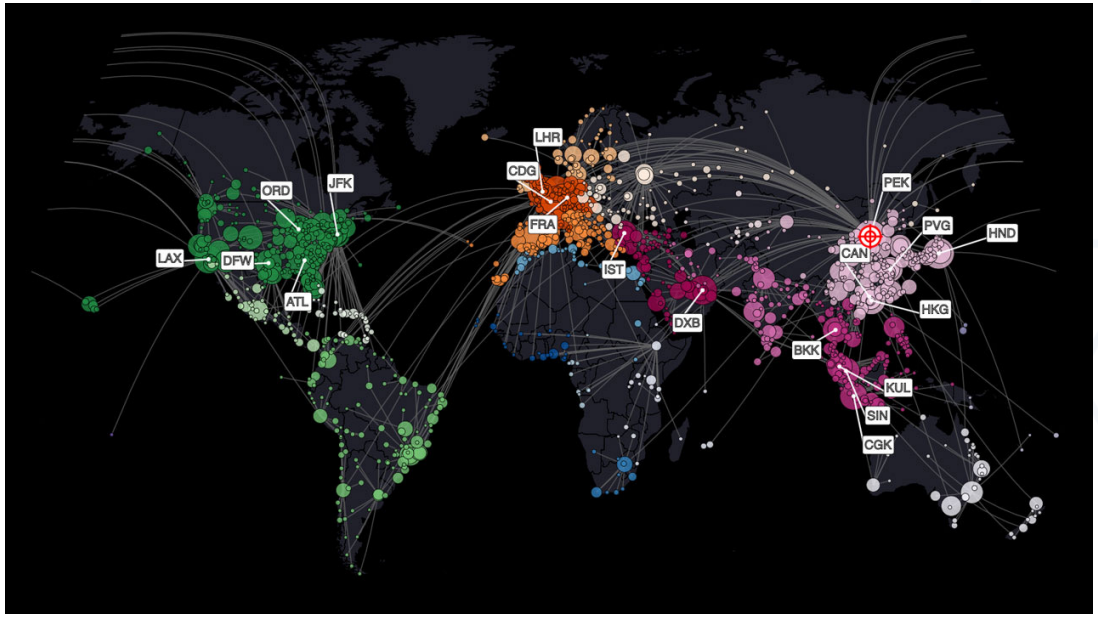
2. The Inevitability of Cyber-Attacks:

- We are acutely aware pandemics strike unexpectedly.
- Cyber-attacks are no different. It’s not a matter of if, but when.
- Only recently the BBC, British Airways and Boots were hit by a cyber breach with employee contact and bank details exposed.
- The healthcare sector, with its vast amounts of sensitive patient data and critical infrastructure, is an attractive target for the malicious actors seeking financial gain or disruptive power.



3. Learning from the Past:





- Without doubt COVID highlighted the need for effective preparation and rapid response to unexpected crises.
- Unfortunately, as revealed by the COVID-19 inquiry, the healthcare sector was ill-prepared for the challenges it faced – we are equally as unprepared for a Cyber pandemic.
- The lessons learned should serve as a wake-up call to proactively address potential cyber threats to health and care.
- Why aren't we reacting in the same way – with focus and consistent action?

NHS England

Cyber Improvement Programme

Funding to ICS' for FY23/24

18th September 2023

Authored by:
Tim Chearman – Programme Lead

Cyber Improvement Programme

- Cyber Futures is now the Cyber Improvement Programme
- We last presented in Jul 2023 and said the business case would be submitted in the
- This hasn't happened due to request to reduce scope and we have now updated the Programme Business Case and submitted it to Transformation Directorate to comme approvals process.
- We are seeking your feedback

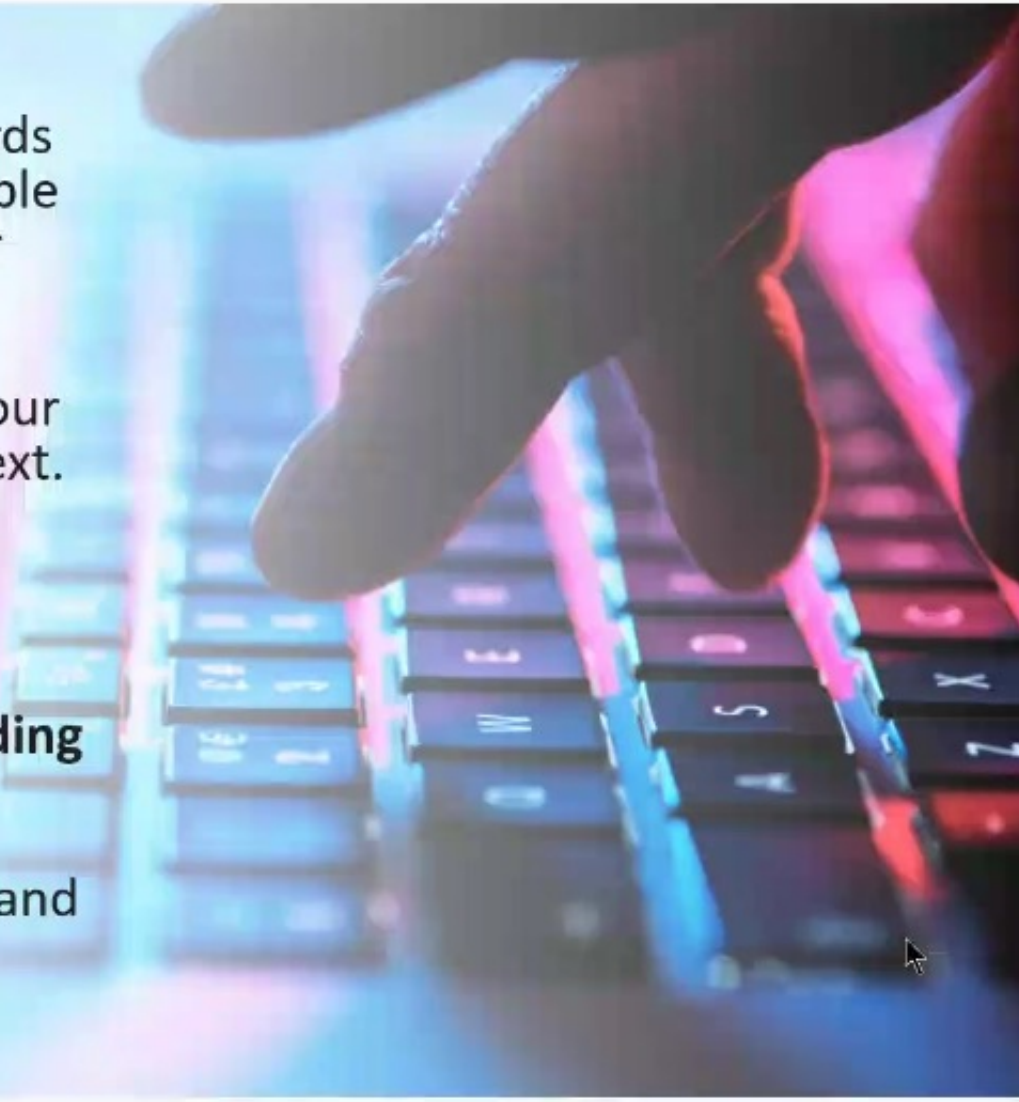
Cyber Improvements business case

As health and social care digitises, we face increasing risks from cyberattacks. **Patient safety** is at risk as we connect our critical infrastructure. **Patient privacy** can be exploited where care records are not adequately protected, and **patient trust** is fragile - if people believe their data is at risk, they are less likely to entrust it to our organisations.

Our recently published **cyber security strategy to 2030** sets out our ambitions and goals as a sector and the steps we need to take next. **Investment of £333m over the last six years** has increased the resilience of the health and social care sector, but we still have a long way to go.

NHS England has submitted a business case for £161.4m (excluding optimism bias and contingency)over the period FY23 – FY25 to deliver cyber security improvements across the health and care sector. This will set the foundation for the next five to ten years, and is intended to reach all health and social care organisations.

So what does this mean for you?



How will the business case impact you?

1. Focus on the greatest risks and harms

- **Making requirements simpler for health and social care organisations** through a single risk framework, updated DSPT process and clearly defined responsibilities for different organisations
- **Communicating risks** by improving our ability to monitor threat and risk and updating you on what steps to take to defend yourselves
- **Increasing estate visibility** through Microsoft defender for endpoint including dashboard to share data with local organisations

2. Defend as one

- Providing **capital & revenue investment funds** at ICB/provider level to reduce local risk and improve cyber capabilities
- **ICS support** through revenue funding in return for a series of Cyber commitments stated in MoU such as ensure cyber risks are properly and consistently recorded within the ICS and its constituent organisations and promote the adoption and implementation of nationally provided cyber support tools and intelligence
- Developing **standards, policies and guidance**
- Aligning **DSPT** to the cyber assurance framework
- Developing **National CSOC strategy, roadmap and capabilities**

How will the business case impact you?

3. People and culture

- **Training and recruiting dedicated ICB cyber security resources** as part of a local support system for health and social care providers
- **Developing and implementing cyber security training** for all staff
- **Building a secure culture** by developing and nurturing communities of interest

4. Build secure for the future

- **Improving supply chain resilience** through:
  - Identification of critical suppliers and development of an assurance framework & future model
  - Standardised contract & framework clauses
  - NHS E/ DHSC supplier risk intervention where feasible

5. Exemplary response and recovery

- **Developing an incident response strategy** including handbooks for different organisations
- Undertaking a **national cyber incident response exercise**
- Supporting **local cyber incident response exercises**

Limitations

- Capital funding with some revenue
- Technical debt is out of scope
- Focus still too much on secondary care
- Cyber skills are limited & expensive

KEY GAPS RELATED TO INCIDENTS

67%
- Logging and monitoring issues

25%
- User Training issues
- Firewall issues
- Tooling (EDR, security services, etc) issues

50%
- Configuration and Vulnerability Management issues

17%
- Asset Management issues

33%
- Issues with Multi-Factor Authentication
- Password Hygiene issues
- Joiners, Movers, Leavers Processes issues

8%
- Anti-virus issues

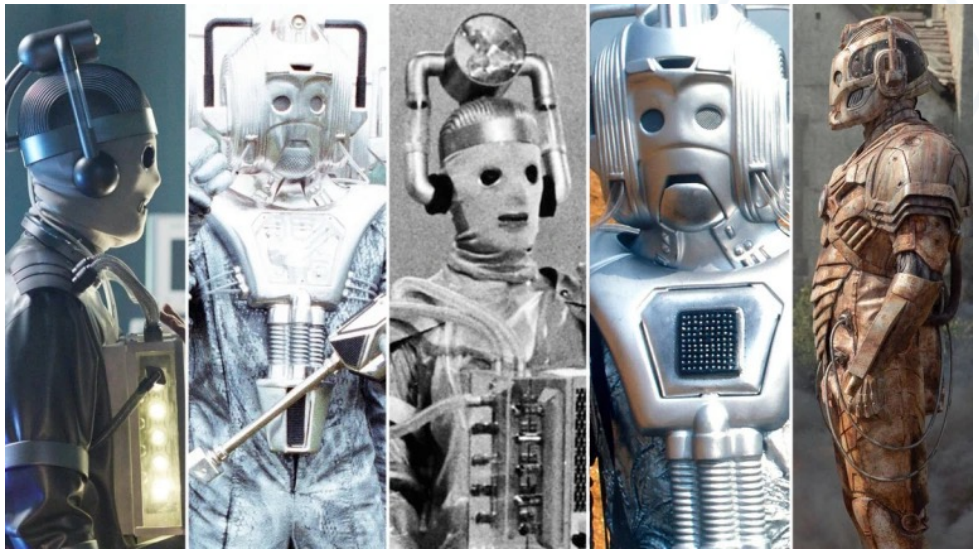
A threat-led approach to modelling cyber risk has been utilised to determine the defence measures that have the most impact on reducing the likelihood of relevant cyber threats.

4. Building Preparedness:

So, what can we do – here are 3 top tips to help prepare:

Experienced People:

- Building a skilled workforce, well-versed in cybersecurity practices is crucial.
- At an organisational level, individuals specialising in cybersecurity, such as Cyber Leads and Non-Functional or Pen Testing experts, should be appointed.
- Yes the experienced ones will be more expensive, but if you pay peanuts…it's about Value for Money, not Cost.
- Creating a network, fostering collaboration and investing in these professionals can take time but will prove invaluable for an effective response during a cyber crisis.



4. Building Preparedness:

So, what can we do – here are 3 top tips to help prepare:

Good Processes:

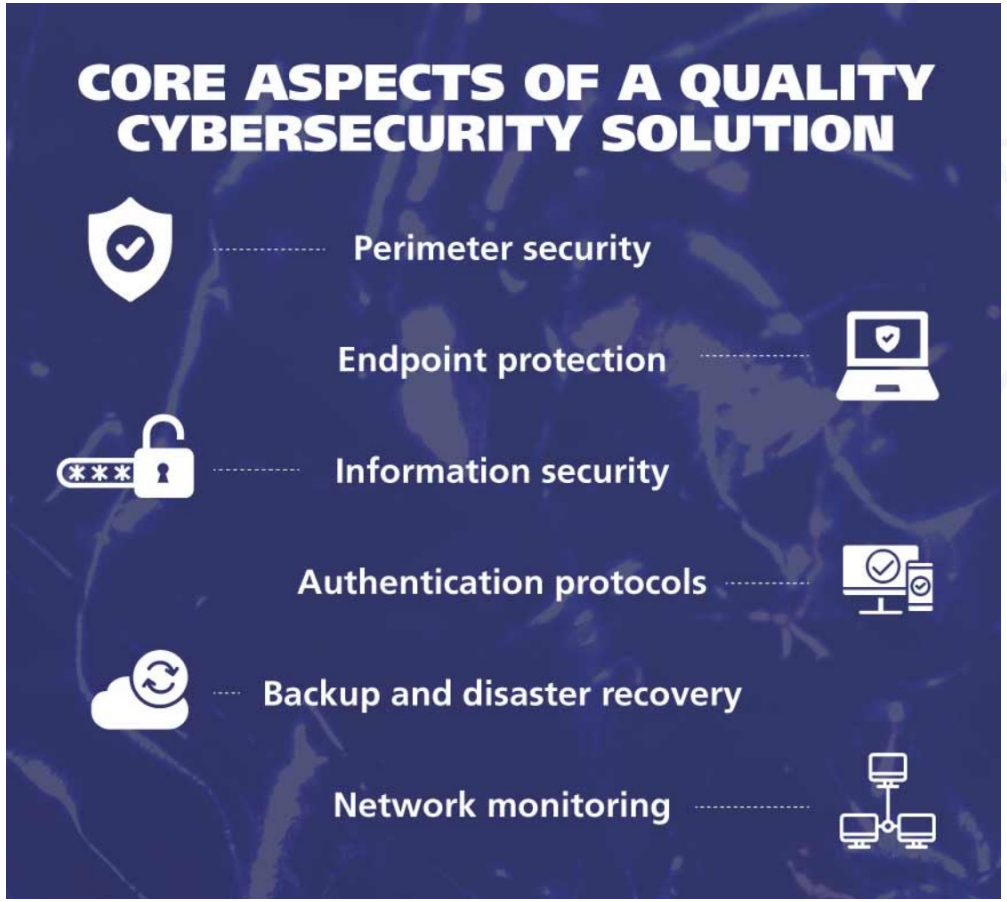
- Establishing battle plans and playbooks that outline flexible response strategies for various cyber-attack scenarios is essential.
- Regular cyber drills and simulations can help test the effectiveness of processes and identify areas for improvement.
- Again this is an investment in time and resource, but this proactive approach will ensure any organisation is better equipped to handle cyber incidents when they occur.
- The NHS can help each other here with shared learning on good practice and processes.

4. Building Preparedness:

So, what can we do – here are 3 top tips to help prepare:

Technological solutions:

- Implementing robust cybersecurity systems, including regular software updates and patches, is imperative.
- Having a dedicated cyber strategy with defined timelines (e.g., DTAC/DSTP) can ensure technology infrastructure is up to date and resilient against ever evolving threats.
- This includes securing medical devices, networks, and data repositories to safeguard patient information.



5. Understanding the Risks:

- While the adoption of artificial intelligence (AI) in healthcare offers appeal and a potential quick fix, it can also introduces potential risks.

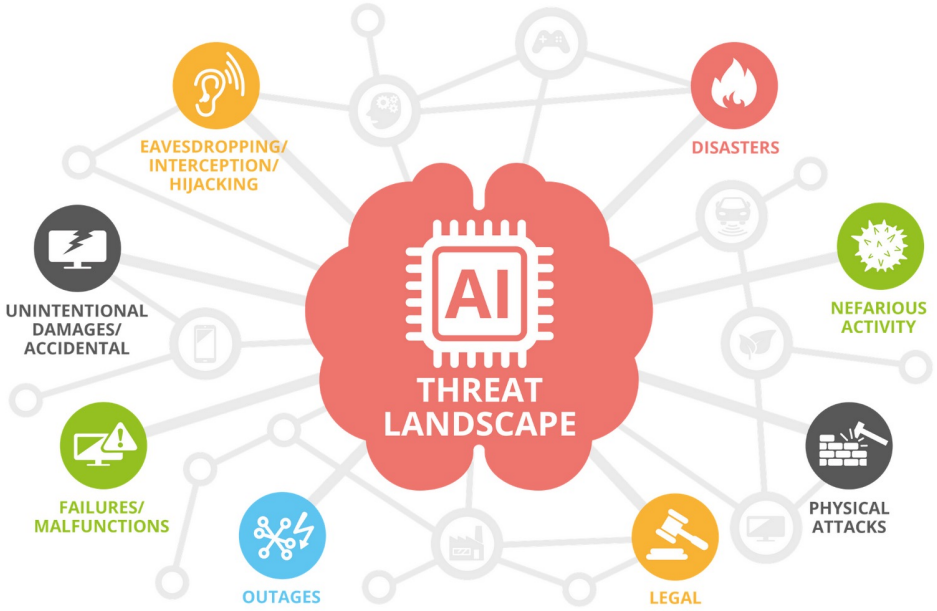
- Rapidly introducing AI without proper scrutiny, control, and understanding may lead to vulnerabilities that could be exploited by cybercriminals.

- Time: How much time is going to be wasted reacting to events rather than being proactive?

- Cost: How much will it cost to remedy any problems ratherr than putting preventative measures in place?

- Quality / Safety: How will it affect patient services and care when critical systems are unavailable or data lost?

- It's mundane, but we do need to constantly review and mitigate these risks – ultimately this is about patient safety so maintaining the integrity of healthcare systems is vital.



6. Conclusion:

- We all know cyber risks are real and present.
- The creation of the National Cyber Security Centre and the growing number of cyber jobs now in the NHS is a huge step forward.
- However, we need to ensure these skilled professionals have time to continually learn, network with peers and have executive support.
- The creation and review of robust processes, prioritisation of technological patching can help organisations to strengthen their cybersecurity posture.
- Yes to AI, but a balanced approach to its adoption and other emerging technologies is crucial, considering both the benefits and risks involved.
- Only through collaborative efforts and a comprehensive cybersecurity strategy can the health and social care sector navigate the constant challenges posed by the cyber pandemic and protect the well-being of our patients and public.

THANK YOU

AHLC Solutions

Andy.Williams@ahlcsolutions.com

Securing the Future of Healthcare

Navigating the Cybersecurity Landscape in the NHS

CONVENZIS

Thank you for attending the Securing the Future of Healthcare Conference!

CONVENZIS

Securing the Future of Healthcare

Navigating the Cybersecurity Landscape in the NHS

Register for the next Cyber Conference in April 2024….