Welcome to the NHS Cyber Security!

05th March 2025
15Hatfields Conference Centre,
Chadwick Court, London, SE1 8DJ

CONVENZIS TRAINING

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

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

Bharat Thakrar
CISO
CyberBTX

Panel Discussion

Lee Rickles
Director and Chief Information Officer
Yorkshire & Humber

Steven Furnell
Professor of Cyber Security
University of Nottingham

Patrick Maw
Consultant Clinical Scientist
University College London Hospital

Abhilash Marisela
Senior Cybersecurity Evangelist
ManageEngine

Garvin Taylor
Lead Client Service Manager
NHS Health Economics Unit

Slido

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

SCAN ME

Main Sponsor

CROWDSTRIKE

Main Sponsor

Kostandino Kustas
Sales Engineer
CrowdStrike

Know Your Adversary

The Value of Threat Intelligence and Posture Management in the NHS

Kostandino Kustas
Cyber Security Solutions Engineer

CrowdStrike

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 TRAINING

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

Chair Morning Reflection

Bharat Thakrar
CISO
CyberBTX

CONVENZIS

Case Study

boxxe
Tech Solutions

FORTINET

Case Study

Jason Cohen
Account Director
boxxe

Daniel Kendall
Principal System Engineer
Fortinet


The power of
boxxe
Tech Solutions

Our Journey

boxxe
Tech Solutions

NHS

1987

Company begins selling software to local MoD bases as SBL (Software Box Ltd)

1996

SBL secures new MoD security contract, saving them £40m

Becomes a Microsoft Large Account Reseller

2003

SBL creates Secure Content Delivery as a service platform

2008

SBL expands into hardware with new technology partners

2019

Entrepreneur Phil Doye acquires and invests in SBL

2020

SBL rebrands as boxxe, with the mission of making technology human

Over 2000 customers supported

2023

boxxe refreshes its brand identity, with new look and feel and go to market strategy

2024

boxxe acquires Total Computers into boxxe Group Ltd.

Making Tech Human™

Our Framework Access

RM6098	Technology Products & Associated Services 2	Lots 1, 2, 3, 4, 5, 6, 7 & 8
RM6100	Technology Services 3	Lots 1, 2, 3a, 3b, 3c & 3d
RM1043.8	Digital Outcomes and Specialists 6	
RM1557.13	G Cloud 13	Lots 1, 2, & 3
RM6147	Technology Online Purchasing Content	
RM3764III	Cyber Security Services 3	
RM6173	Automation Marketplace DPS	
RM6225	Audio Visual Technical Consultancy & Commissioning DPS	
Y20011	Software Products and Associated Services 2	
Y21028	Supply of IT Hardware	Lot 1
Y20023	Managed Services	
enFrame	Software	L6 – SL1, SL2 & SL3

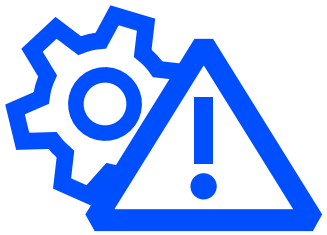
HTE	ICT Solutions (ComIT)	
NHS SBS	Digital Workplace Solutions	
NOE CPC	Provision of ICT Solutions Delivery: Professional Services & Consultancy Support	Lots 3, 4, 5 & 6
NEUPC	HE Networking Supply and Services (HENSS)	Lot 1
CPC	Software Licenses - Academies and Schools	Lot 1 & 2
PFS	PFS_EDTECH Framework for Education	Lot 1
JISC	Web Filtering Monitoring and Reporting	Lot 1
SUPC	Servers, Storage and Solutions National Agreement – Dell Technologies	Lots 1, 2, 3 &4

Making Tech Human™

COVERAGE

boxxe
Tech Solutions

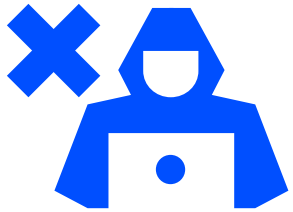
NHS



A1, A2, A3, A4

Objective A

Managing risk



B1, B2, B3, B4, B6

Objective B

Protecting against data breaches

C1, C2

Objective C

Detecting cybersecurity event

D1

Objective C

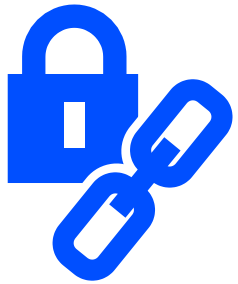
Minimising the impact of an incident

Making Tech Human™

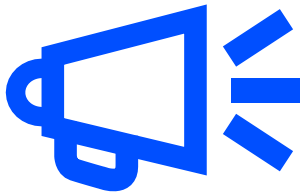
Approach

boxxe Tech Solutions

NHS



CONSOLIDATION



COMMUNICATION

GOVERNED

FINANCIAL

Making Tech Human™

CAF POINTS ON POINT

boxxe Tech Solutions

NHS

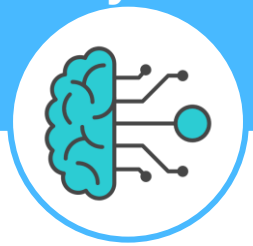
Objective A – Managing Security Risk

Appropriate organisational structures, policies, processes, and procedures are in place to understand, assess and systematically manage security risks.

Objective B - Protecting Against Cyber Attack

Proportionate security measures are in place to protect the networks and information systems.

Objective C - Detecting Cyber Security Events



Capabilities exist to ensure security defences remain effective and to detect cyber security events affecting, or with the potential to affect, essential functions.

Objective D - Minimising the Impact

Capabilities exist to minimise the adverse impact of a cyber security incident on the operation of essential function(s), including the restoration.

Making Tech Human™

Key Themes

boxxe Tech Solutions

NHS

Supply Chain

Cyber actors continuing to target the UK health and social care sector **supply chain**, in order to facilitate their cyber operations and access a large number of potential victims.

Ransomware

Ransomware remaining the largest and most likely disruptive threat to the UK health and social care sector.

Threat to CNI

Cyber threat to UK CNI has increased in the last year – due to geopolitics.

Data

UK health and social care sector considered an attractive target to a range of threat actors because of the quantity and sensitivity of **health data** available; including, intellectual property, big data and personal information held about UK citizens

Cyber

Due to **ambition to overtake Western countries in core technologies**, the UK health and social care sector, research and data are attractive targets

'Frail' system

The HSE estimates the cost of the cyberattack at **€102 million**. 14 May 2024

Law Society of Ireland
https://www.lawsociety.ie › gazette › top-stories › may

HSE facing 473 lawsuits after Russian cyber attack

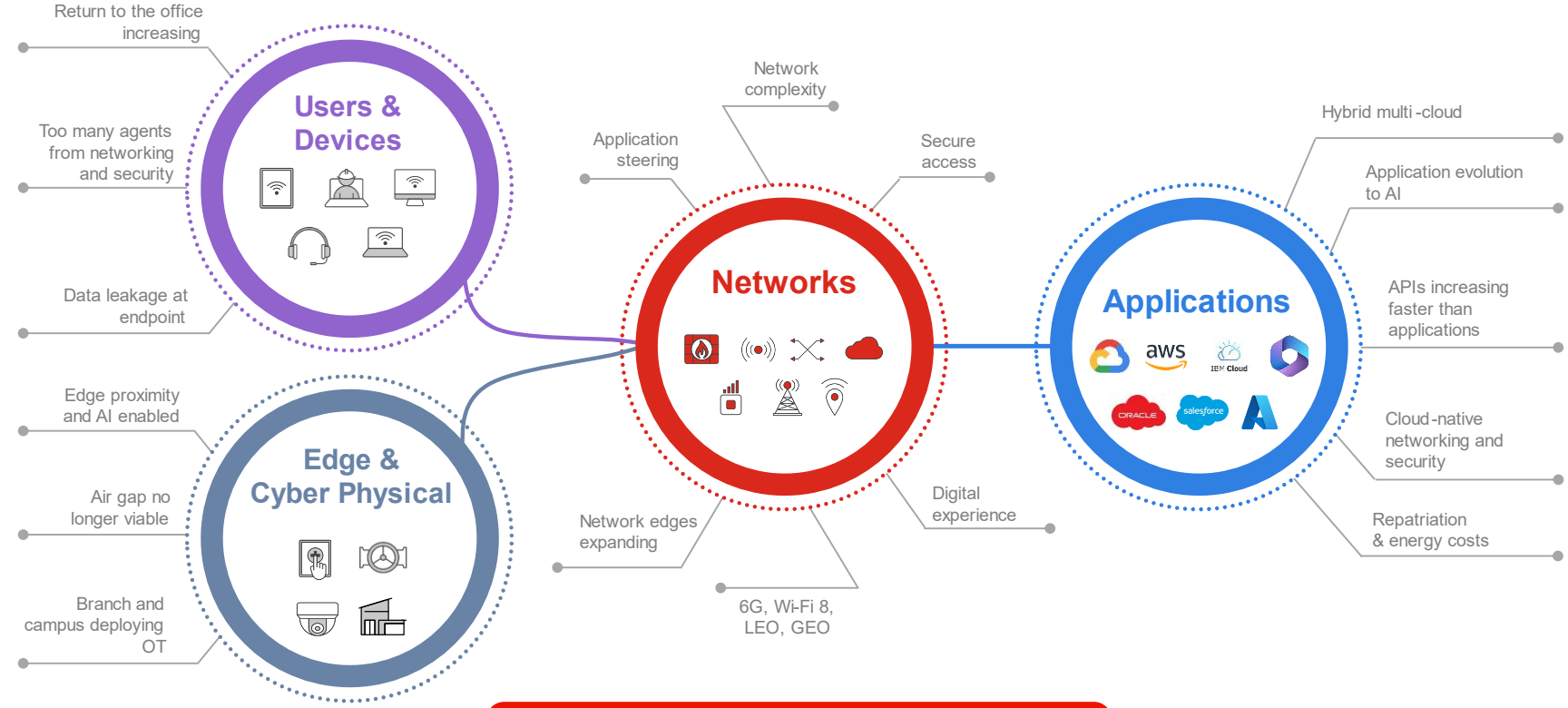
Cost to the NHS

The **£33m** cost to Synnovis revealed in its accounts today does not account for the whole of the financial cost of the attack, however. Documents seen by HSJ show a £35.7m hit to income and increase in costs to the south east London health system in the wake of the ransomware attack. 15 Jan 2025

Making Tech Human™

Objective A – Managing Security Risk

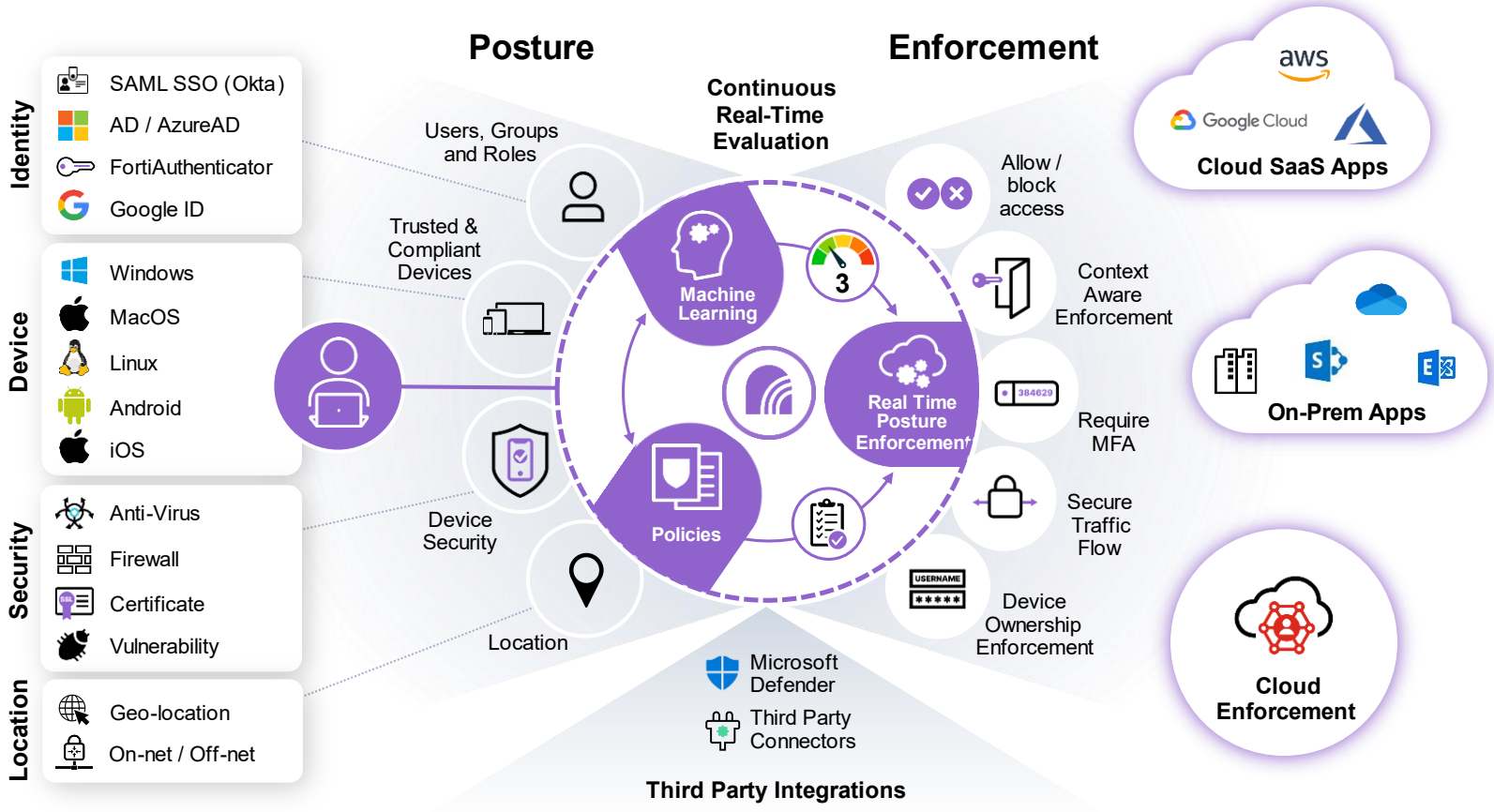
A1 - Governance
A2 - Risk Management
A3 - Asset Management
A4 - Supply Chain



Making Tech Human™

Objective B - Protecting Against Cyber Attack

B1 – Service Protection Policies, Processes and Procedures
B2 – Identity & Access Control
B3 – Data Security
B4 – Systems Security
B5 – Resilient Networks and Systems
B6 – Staff Training & Awareness



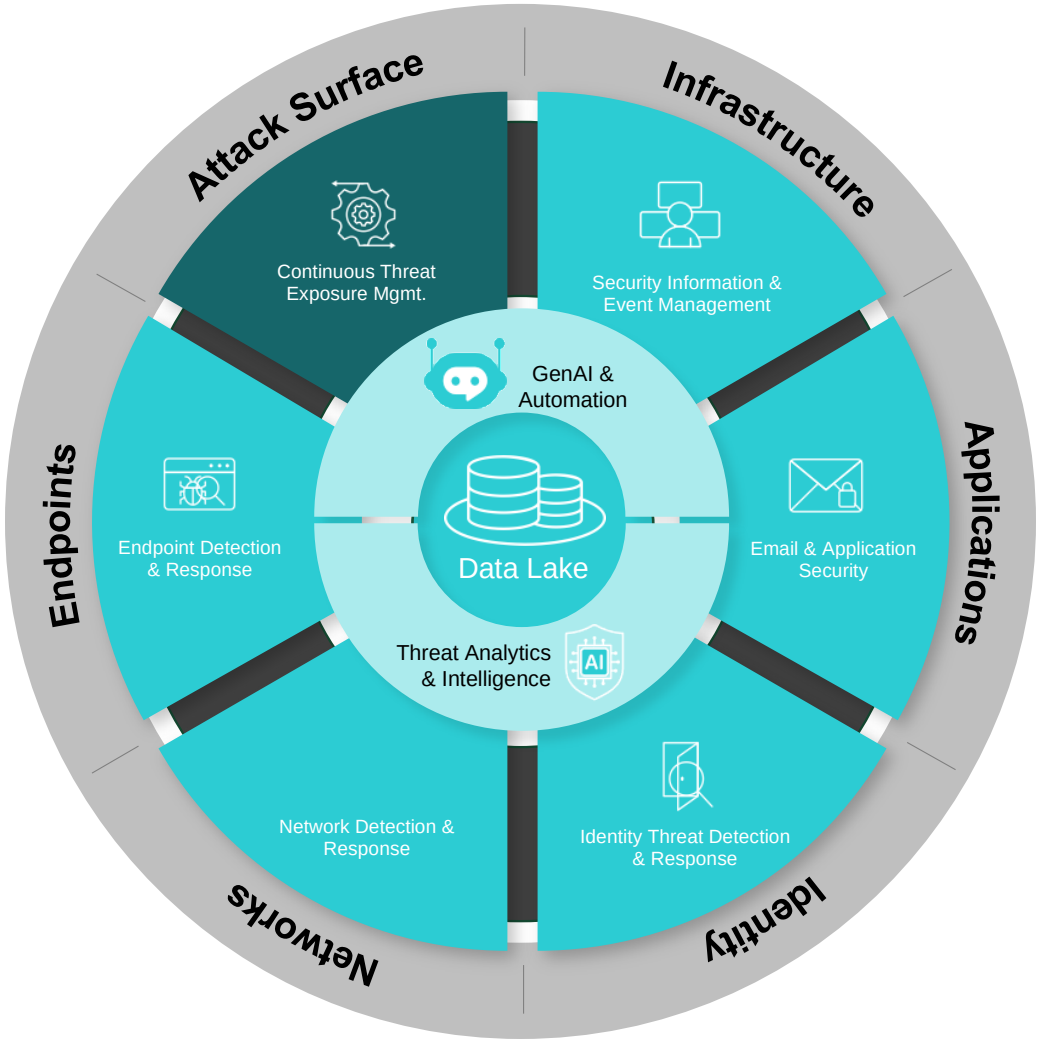
boxxe Tech Solutions

NHS

Making Tech Human™

Objective C - Detecting Cyber Security Events

C1 – Security Monitoring
C2 – Proactive Security Event Monitoring



NIST Cybersecurity Framework

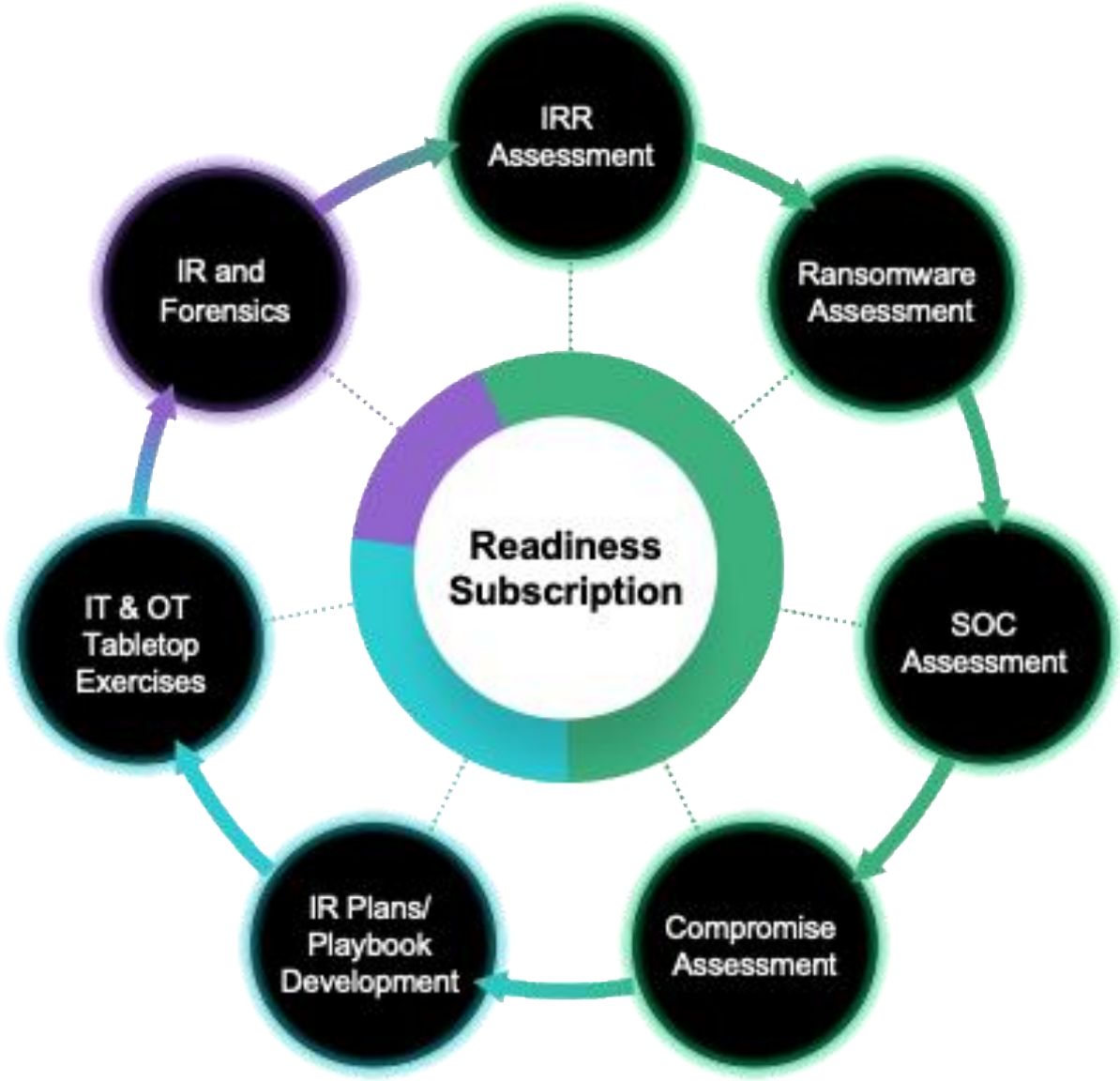
boxxe Tech Solutions

NHS

Making Tech Human™

Objective D - Minimising the Impact

D1 – Response & Recovery Planning
D2 – Lessons Learned



boxxe Tech Solutions

NHS

Making Tech Human™

Structured approach

To harness the full potential of a Cybersecurity Platform, an evolution of your team's organisation is possible:

Security Operations Team

- Layered Defense Strategy (SIEM/SOAR)
- Unified Security Policy Management
- Regulatory Compliance Assurance
- Advanced Threat Detection & Response
- Real-Time Traffic Analysis for Data Protection

Mesh Infrastructure Team

- Optimized Infrastructure Management
- 'Anywhere' Secure Connectivity
- MultiCloud Connectivity Strategy
- Proactive Issue Resolution
- Capacity Planning for Bandwidth & Circuits

boxxe Tech Solutions

NHS

Making Tech Human™


boxxe
Tech Solutions
NHS
Tech solutions
designed by people,
for people

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

stratodesk

Case Study

Paul Craddock
Global Solution Architect - Stratodesk

Stratodesk NoTouch: Secure, Sustainable OS & Management for VDI Endpoints for Healthcare

PRESENTER

Paul Craddock
Global Solutions Engineer
paul.craddock@stratodesk.com

stratodesk

Slido

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

SCAN ME

Fireside Interview

Azeem Bashir

Group Chief Information & Security Officer - CIO\CISO - President - Chair - Cyber Committee Member for EMEA & Asia-PAC - Hamilton Group

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

zscaler™

Case Study

Mike Culshaw
Security Specialist
Zscaler

Securing, Simplifying and Transforming The NHS

Mike Culshaw

Patient Safety Incidents Increase year on year

Synnovis attack highlights degraded, outdated state of NHS IT

More cyber attacks against the health service are likely, and will succeed if something isn't done to address the increasingly elderly NHS IT estate, experts are warning

By **Alex Scroxton,** Security Editor

Published: **08 Jul 2024 16:45**

Fix NHS gaps or face more attacks - ex cyber chief

Ciaran Martin, former head of the National Cyber Security Centre said hack was "one of the most serious cyber incidents British history"

Health board 'running as normal' after cyber attack

Two more Liverpool hospitals impacted by Alder Hey cyber attack

CYBER SECURITY, NEWS

5 December 2024

Ransomware group releases NHS Dumfries and Galloway patient data

CYBER SECURITY, NEWS

27 March 2024

Major London hospitals disrupted by cyber-attack

June 5, 2024

image: @georgeclerk | iStock

Major London hospitals, including Guy's, St Thomas', and King's College, have been severely disrupted by a cyber-attack that has forced the cancellation of operations and blood transfusions

NEWS

NCSC and partners issue warning over North Korean state-sponsored cyber campaign to steal military and nuclear secrets

Critical infrastructure organisations are strongly encouraged to stay vigilant to DPRK-sponsored cyber operations.

Advanced cyber-attack: NHS doctors' paperwork piles up

30 August 2022

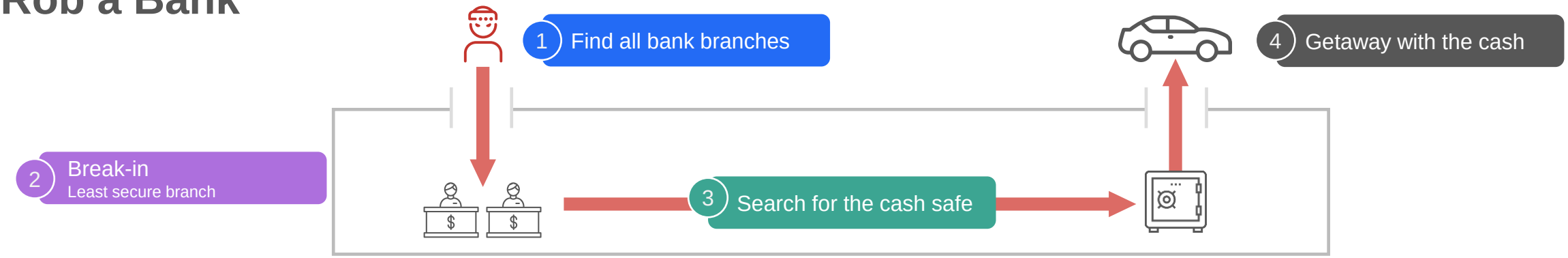
Staff are having to resort to writing care notes on pieces of paper after IT systems were targeted

Cybersecurity is a Patient Safety Risk not just an IT risk

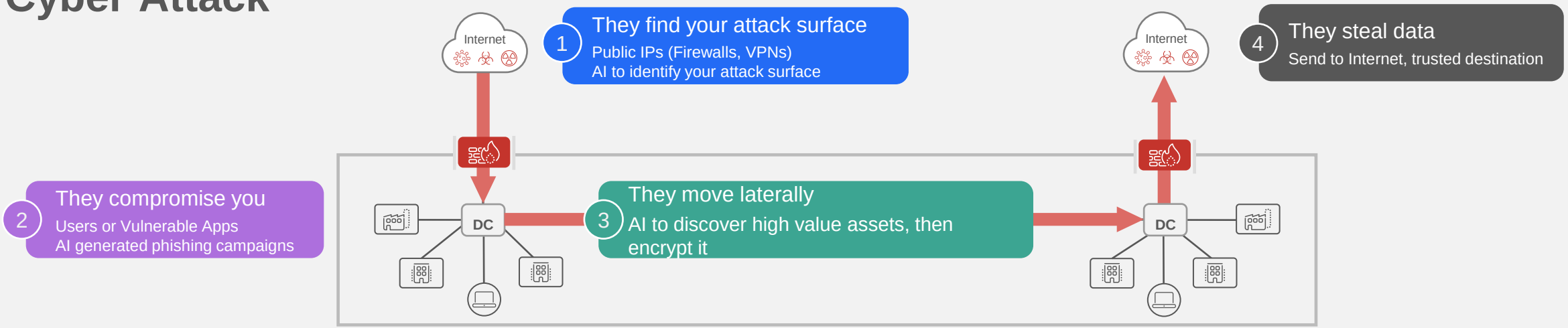
Productivity	Clinical	Reputation	Financial
IMPACT	IMPACT	IMPACT	IMPACT
• IT Teams workload • Clinical teams workload • Corporate Staff workload	• Operations cancelled • Appointments cancelled • No access to information	• Patient • Commissioners • Media	• Unplanned spend • Potential loss of contracted services • Average digital transaction cost 8p Average paper cost £12 *industry average • ICO Fines

The Anatomy of a Cyber Attack

4 Steps to Rob a Bank



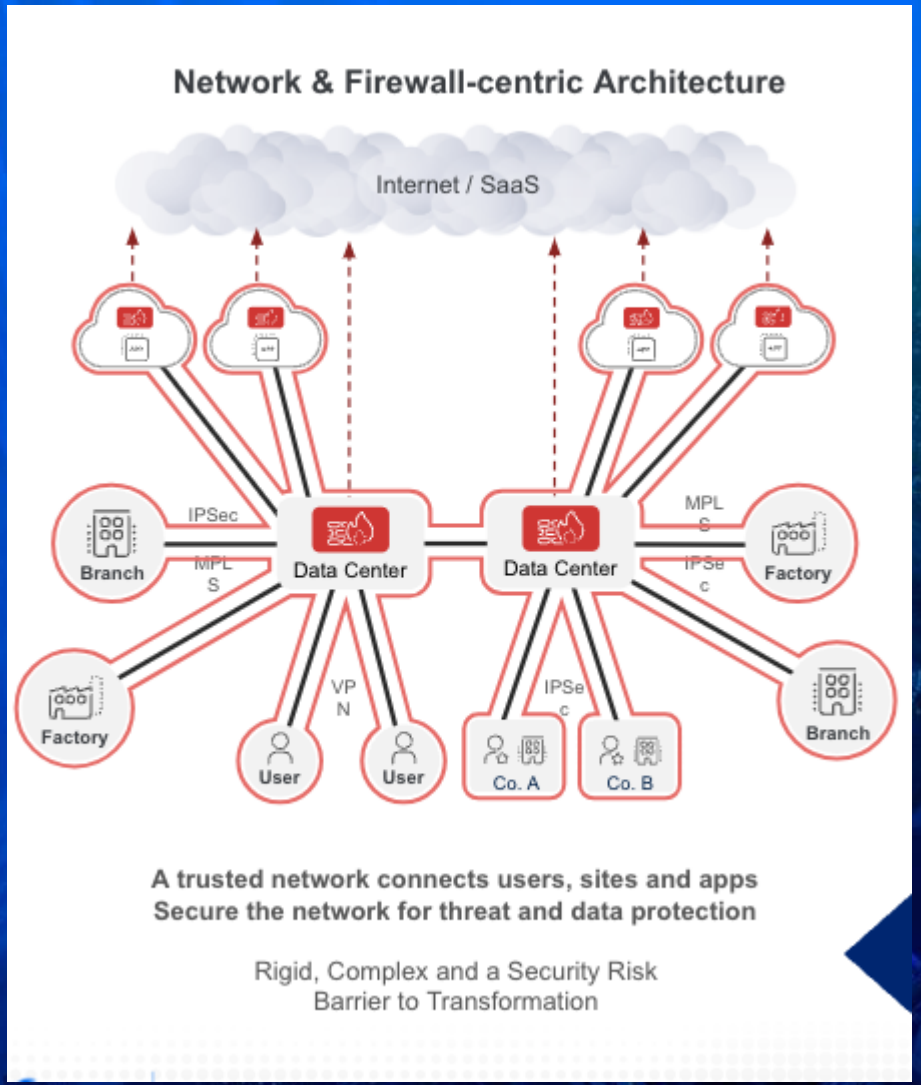
4 Steps for a Cyber Attack



Zero Trust In Action

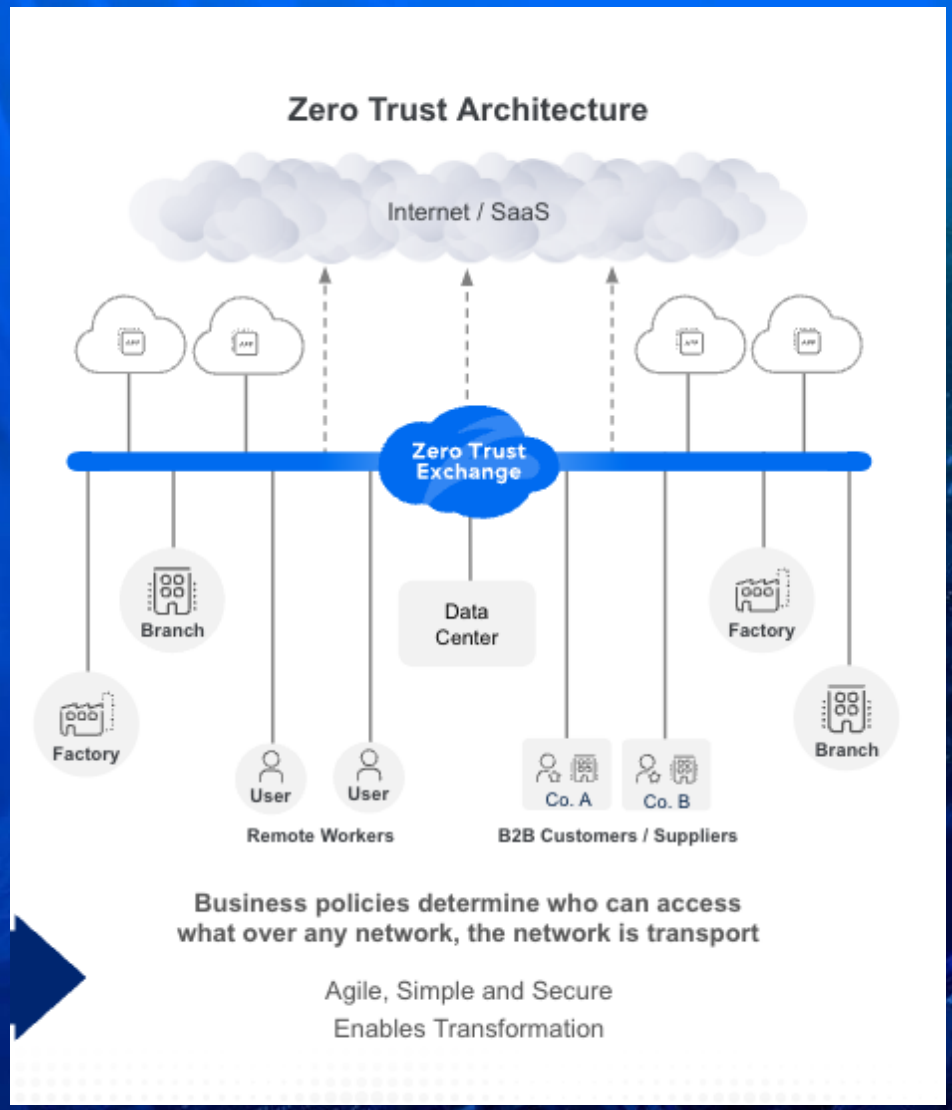
Scenario 1

- How to access via a traditional VPN
  - A RECEPTIONIST
  - AN ATTENDEE
  - A HOST
  - A Hacker

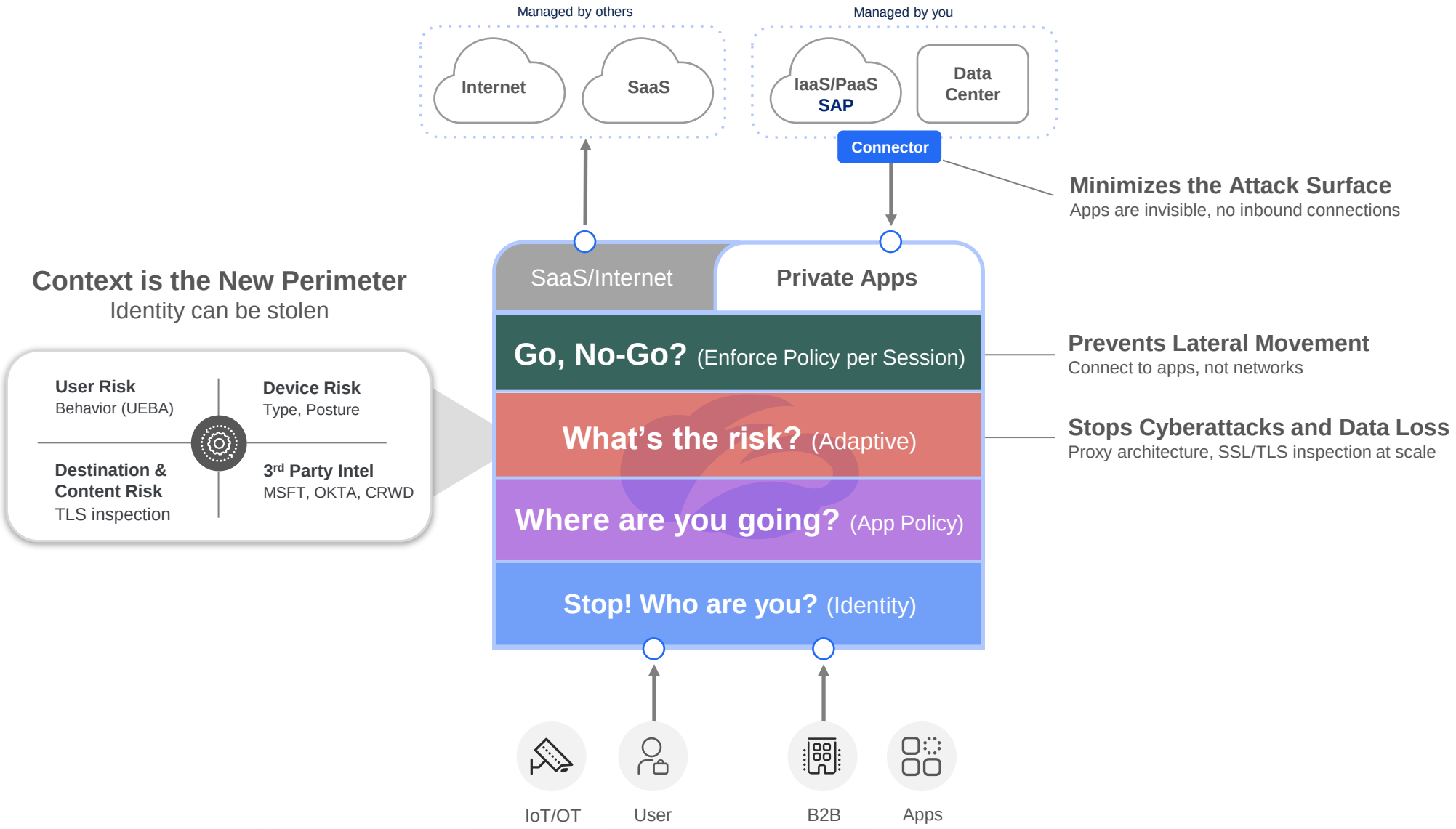


Scenario 2

- How to access via the ZERO TRUST EXCHANGE
  - A RECEPTIONIST
  - AN ATTENDEE
  - A HOST
  - A SECURITY GUARD



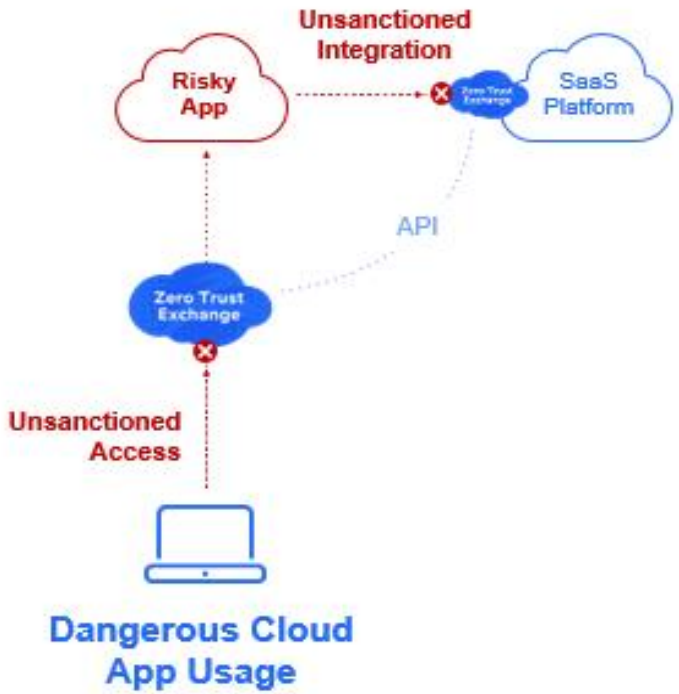
Zscaler Zero Trust Exchange Architecture



You can't do Zero Trust with Firewalls/VPN

Lets Talk about Shadow IT

Discover Shadow IT Apps and Third-party integrations



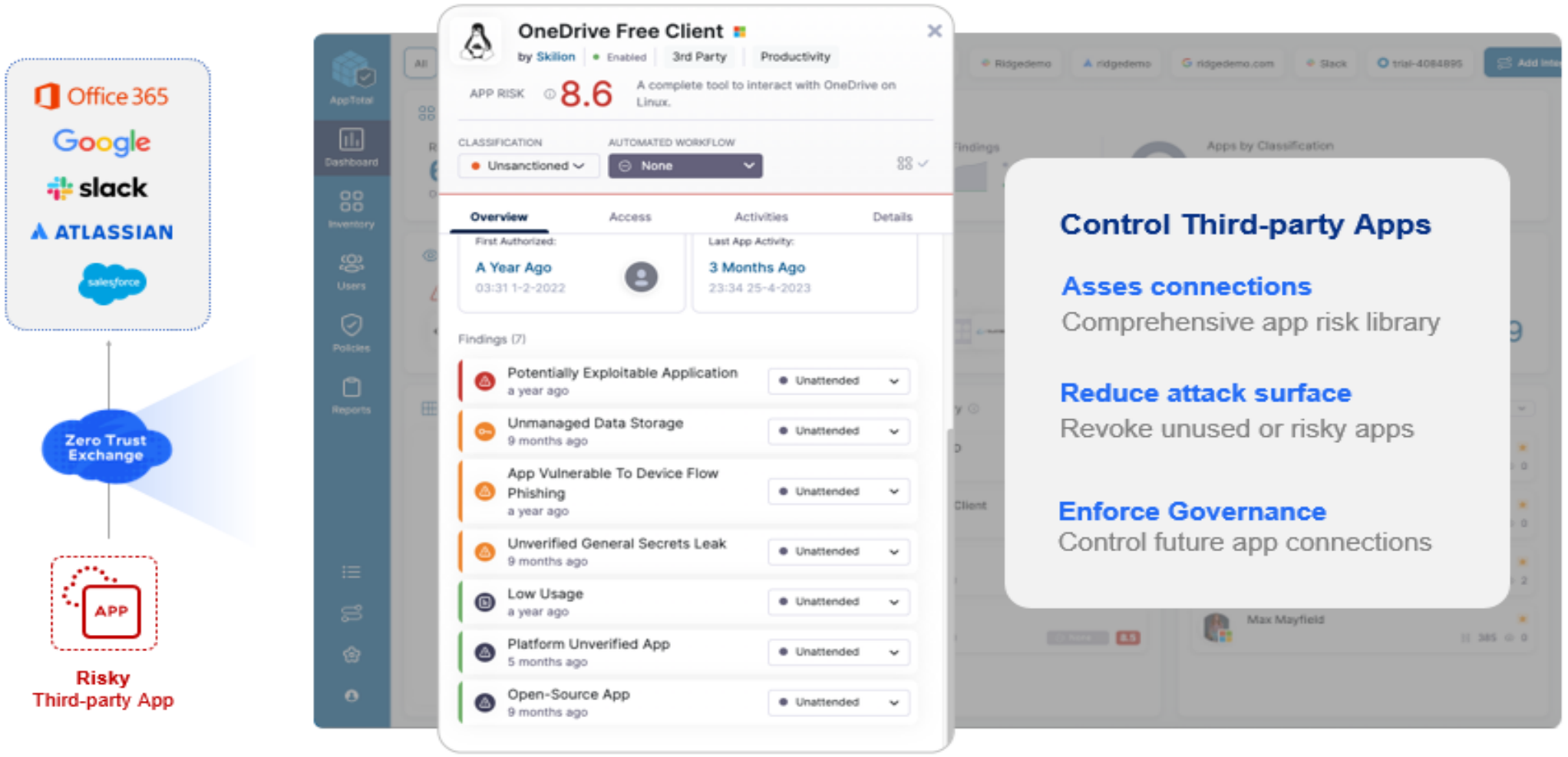
Advanced Shadow IT

- Discovery Risky Apps & SaaS Integrations
- Revoke access and stop data loss

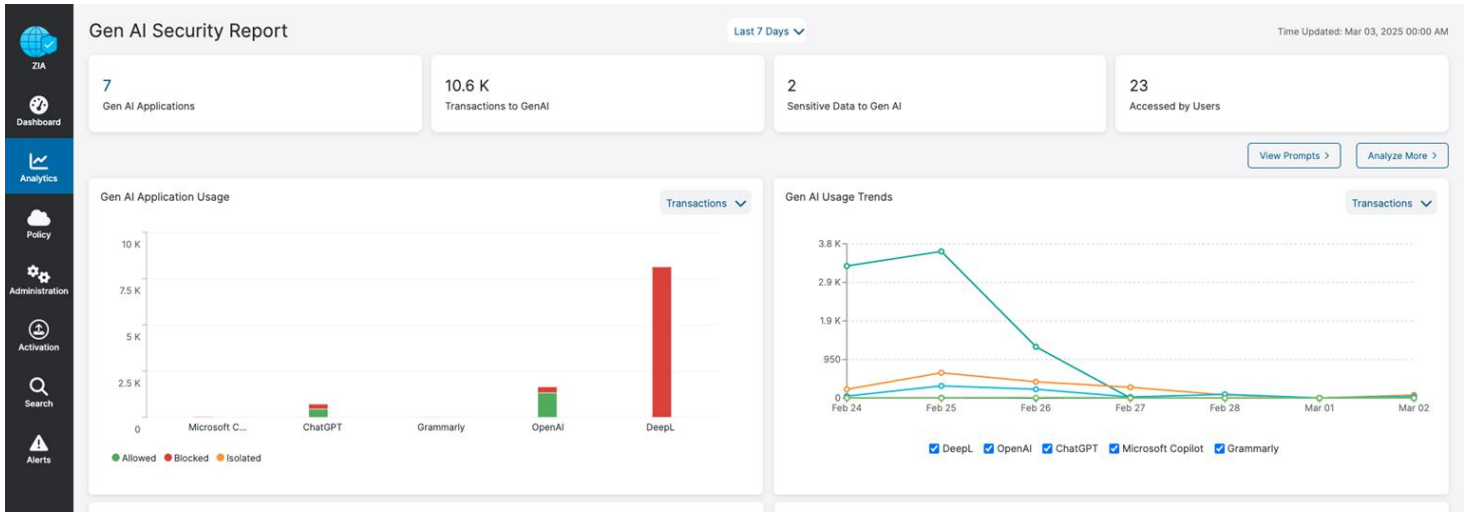
Comprehensive Catalog

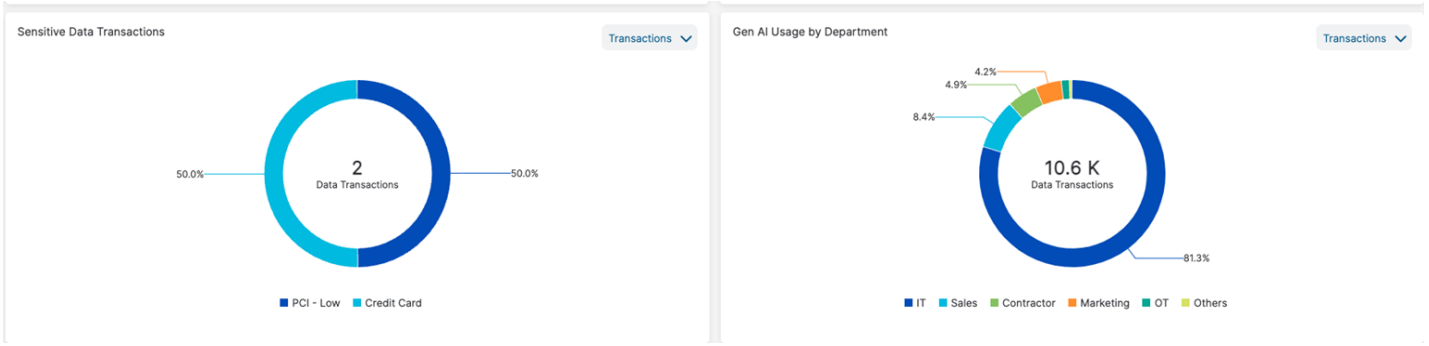
- 90k Apps and SaaS based services
- 130k browser extensions
- In-depth risk attributes from research and API sandboxing

SaaS Supply Chain: Secure SaaS from risky third-party apps



How Zscaler helps with the Gen AI - Headache





- **Secure Access Control:** Zscaler uses Zero Trust Network Access (ZTNA) to ensure only authorized users and devices can access generative AI platforms, reducing the risk of unauthorized access and breaches.
- **Data Loss Prevention (DLP)**: Sensitive data is monitored and protected to prevent accidental or intentional leaks into AI systems.
- **Threat Detection:** Zscaler inspects AI traffic to block malicious activities, such as data exfiltration, misuse of AI models, and AI-generated phishing content.
- **Governance and Compliance:** Detailed visibility and reporting help organizations monitor AI usage, enforce compliance, and align interactions with regulations.

Next Steps

1. Pay us a visit upstairs on the Zscaler stand

Thank you!

Zero Trust for CXOs

Zero Trust for Boards

Zero Trust for Architects

Download your complimentary copy

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

CONVENZIS TRAINING

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

Chair Afternoon Reflection

Bharat Thakrar
CISO
CyberBTX

CONVENZIS

Case Study

BlueFort Security

Case Study

Josh Neame
Chief Technology Officer
BlueFort Security Ltd

Peter Batchelor
Regional Sales Director
Silverfort

SILVERFORT

BlueFort Security

NHS

King's College Hospital

NHS Foundation Trust

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

Slido

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

SCAN ME

Keynote Presentation

Lee Rickles
Director and Chief Information Officer
Yorkshire & Humber

Ian Clucas
Deputy CIO
Interweave

INTERWEAVE
CONNECTING CARE

Securing Internet-facing Shared Care Records

5th March 2025

With the increasing adoption of cloud-based shared care records, ensuring the security of internet-facing systems handling sensitive patient data is paramount.

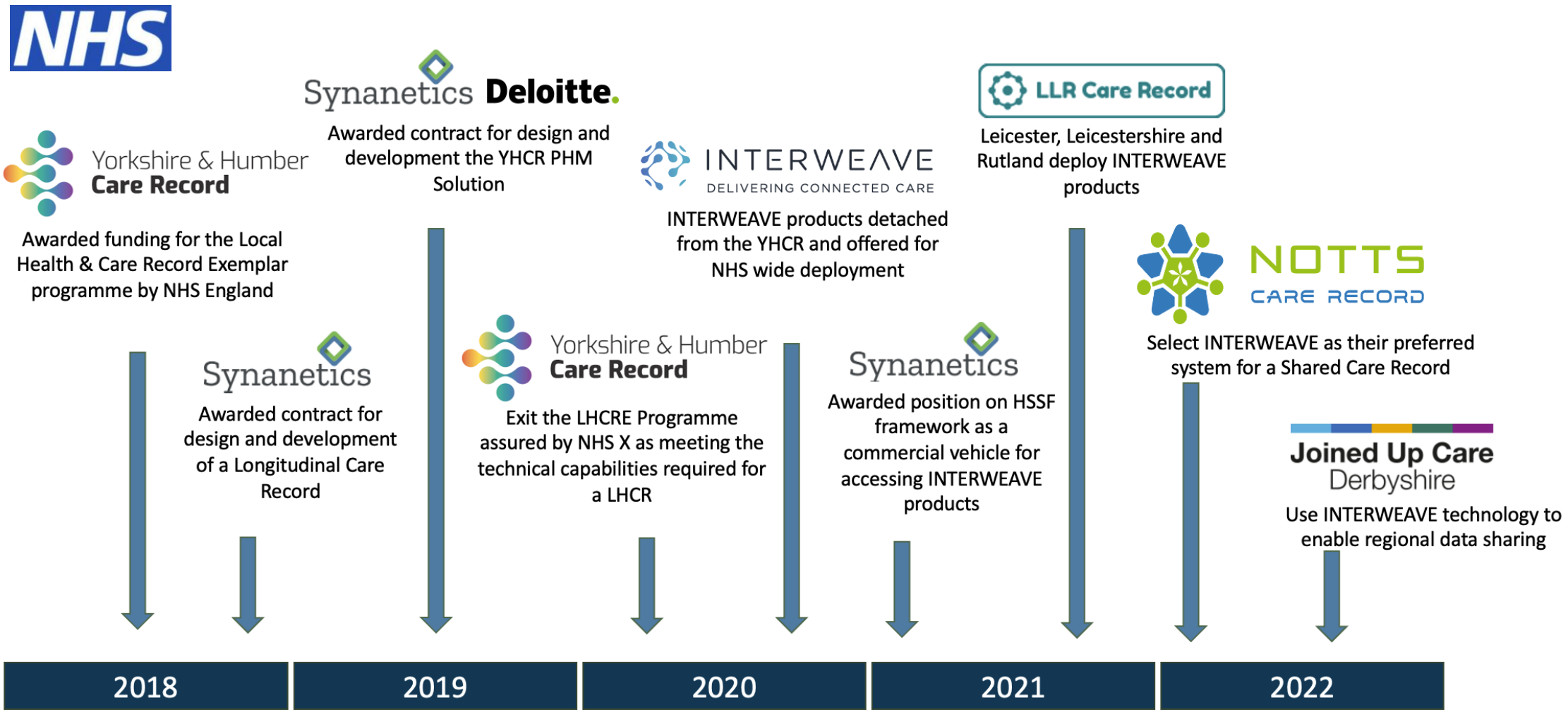
This briefing outlines key security considerations and best practices for protecting a system that provides access to over 8 million health and care records.

Lee Rickles
CIO Humber Teaching NHS Trust
Programme Director for YHCR

Ian Clucas
Deputy CIO Interweave

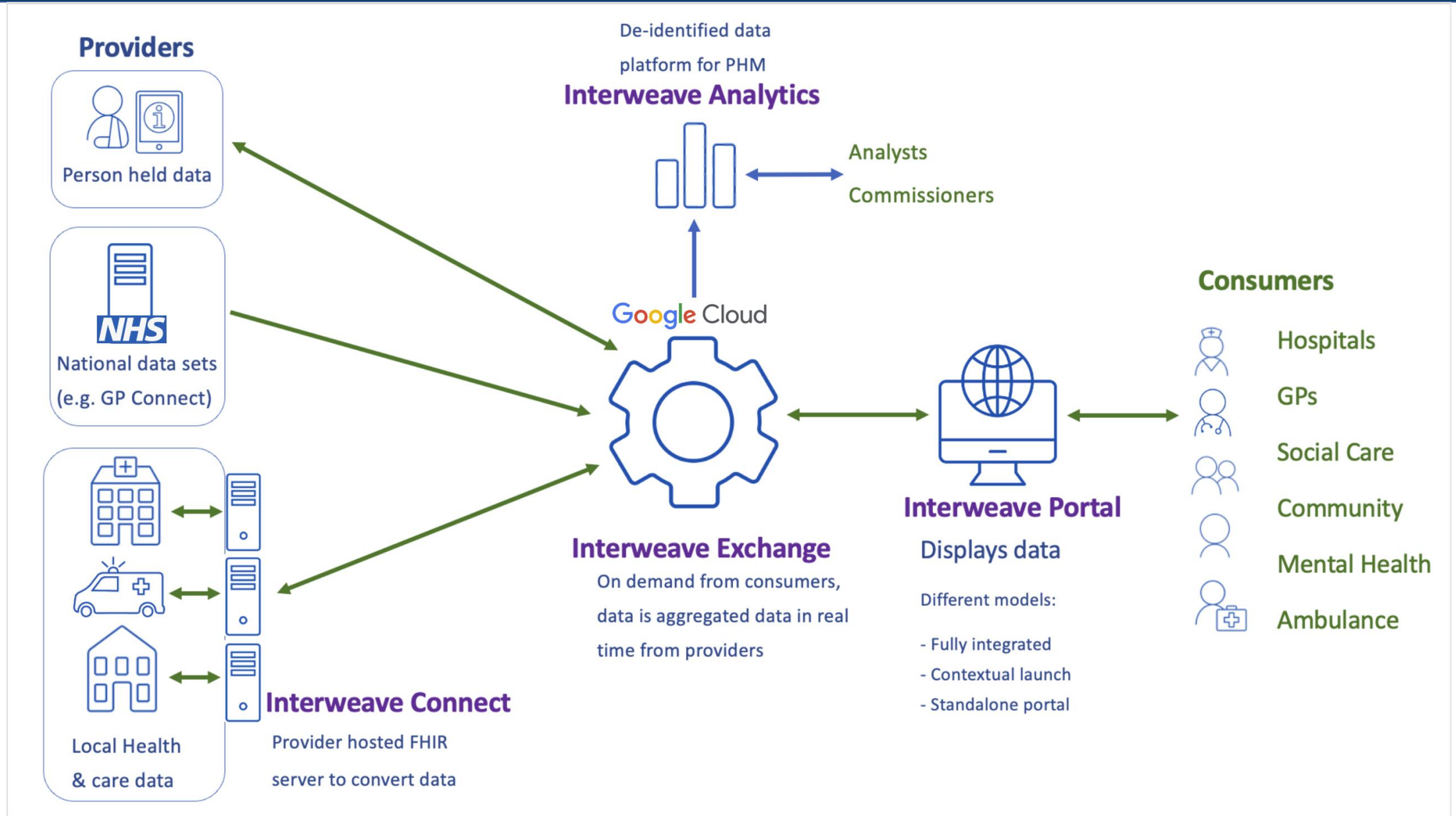
INTERWEAVE
CONNECTING CARE

Interweave journey



INTERWEAVE CONNECTING CARE

High level overview



Key Security Challenges

Protecting patient data is crucial to maintain trust and comply with GDPR regulations and NHS Digital Security Standards.

A multi-layered approach is essential to address the key challenges of:

- Increasing cyber threats (ransomware, phishing, insider threats)
- Compliance with UK GDPR, Data Protection Act 2018 & NHS security standards
- Ensuring secure interoperability and data exchange across multiple health & care organisations
- Assuring cyber compliance of providers and consumers connecting to the platform
- Preventing unauthorised access while enabling real-time data sharing

Security Framework

National Cyber Security Centre
a part of GCHQ

10 Steps to Cyber Security

This collection is designed for security professionals and technical staff as a summary of NCSC advice for medium to large organisations. We recommend you start by reviewing your approach to risk management, along with the other nine areas of cyber security below, to ensure that technology, systems and information in your organisation are protected appropriately against the majority of cyber attacks and enable your organisation to best deliver its business objectives.

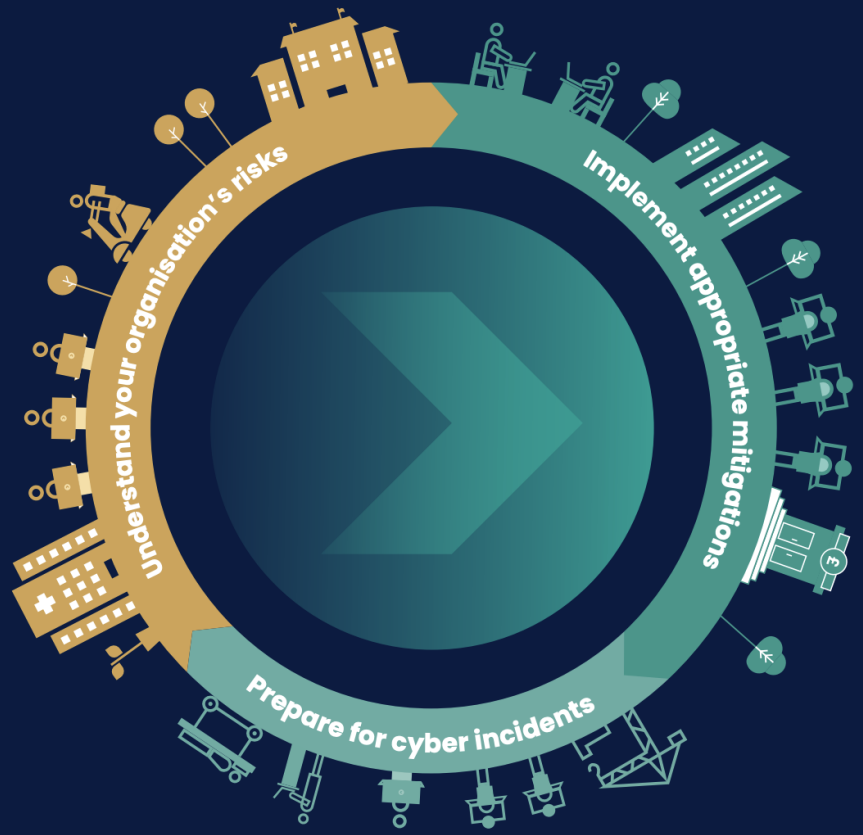
Risk management
Take a risk-based approach to securing your data and systems.

Engagement and training
Collaboratively build security that works for people in your organisation.

Asset management
Know what data and systems you have and what business need they support.

Architecture and configuration
Design, build, maintain and manage systems securely.

Vulnerability management
Keep your systems protected throughout their lifecycle.



Identity and access management
Control who and what can access your systems and data.

Data security
Protect data where it is vulnerable.

Logging and monitoring
Design your systems to be able to detect and investigate incidents.

Incident management
Plan your response to cyber incidents in advance.

Supply chain security
Collaborate with your suppliers and partners.

INTERWEAVE
CONNECTING CARE

Security Framework

1. Governance & Compliance
1. Data Security & Encryption
2. Cyber Security solutions & Threat Detection
3. Resilience and Recovery
4. Identity & Access Management (IAM)
5. Third-party & Supply chain
6. Staff training and awareness

INTERWEAVE
CONNECTING CARE

Governance and Compliance

- GDPR compliance
- Alignment with standards (including NHS mandated)
    - Data Security and Protection Toolkit (DSPT)
    - Digital Technology Assessment Criteria (DTAC)
    - Cyber Essential Plus (CE+)
    - Cyber Assessment Framework (CAF)
    - Centre for Internet Security controls framework (CIS)

- Security Strategy and Policies
    - Regular Audits
    - Security Posture Assessments
    - Pen testing schedule
    - Usage audits - who accessed who – federated trust-based policy

INTERWEAVE
CONNECTING CARE

CAF

- https://www.ncsc.gov.uk/collection/cyber-assessment-framework
- 4 Principles with 14 Regulations
- Focused on governance, risk management, and compliance
- Purpose: assess cyber security maturity
- Aim: robust Cyber resilience
- Required for regulated sectors in the UK (health, energy, transport etc)

Centre for Internet Security

- https://www.cisecurity.org/controls/v8
- 18 Controls
- More technical step-by-step guide to implement security measures
- Purpose: provide cyber security best practices
- Aim: improve cyber security and risk reduction

Governance and Compliance cont…

- Which framework to use?
  - Both ☺
  - CAF compliance mandatory
  - Independent CIS assessment to identify areas for improvement in our security posture

INTERWEAVE
CONNECTING CARE

Data Security & Encryption

- Zero Trust architecture (ZTA)
  - Least privilege access
  - Role Based Access Control (RBAC)
  - Continuous authentication – “never trust, always verify”
  - Network segmentation - isolate different environments

- End-to-End Encryption (E2EE)
  - Encrypted data at rest and in transit
  - Use industry-standard protocols for secure data exchange
    - AES-256
    - TLS 1.2 or higher
    - OAuth 2.0

INTERWEAVE
CONNECTING CARE

Cyber Security solutions

- SIEM functionality (Security Information and Event Management) within Google Cloud Security
- Google Security Centre - centralised platform to enhance security and privacy
  - Google workspace monitoring (Real time Monitoring, Alert Centre, Security Dashboard, Investigation tools)
  - Threat detection and alerts (machine learning-based detection to spot unusual behaviours and potential data breaches)
  - Privacy Controls, DLP, Endpoint Security etc
- Other options:
  - Google Chronicle - enterprise solution
  - Splunk, Microsoft Sentinel
  - Elastic Security - free-tier open source
- Risk vs Budget

INTERWEAVE
CONNECTING CARE

Resilience and Recovery

- Data Backup & Disaster Recovery
  - Backups (geographically separated)
  - Business Continuity Plans
  - DR plans and testing
  - Penetration testing cycle of business
- Incident Response
  - Incident Response Plan (IRP) for rapid breach management (all detailed in BCP)
  - Post Incident Review procedures (PIR)

Identity and Access Management (IAM)

Consumer access to the Shared Care Record

In order of best user experience:

- Authentication from trusted Consumer systems for context launch (OAuth 2.0)
- Single Sign On from trusted organisations via AD
- Multi-factor authentication – One Time Token for standalone Portal

INTERWEAVE
CONNECTING CARE

Third-party and Supply chain

- Supplier security accreditations
  - Technical: CE+ or higher, e.g. Service Organisation Control Type 2 (SOC 2)
  - Process assurance: IASME or higher, e.g. ISO27001
  - Pen testing: NCSC Approved CHECK certified
- Rigorous Data Provider Cyber Assurance
  - DMZ, firewalls, patch management, device management, AV, malware, password and leavers policies
- Independent assessments of supply chain
  - Third-party risk assessments, benchmarking against best practices
- Monthly Security Review meetings (review actions, vulnerabilities, SCC, threat notifications)
- Data Protection Agreements (DPA) underpin operational arrangements for data sharing

INTERWEAVE
CONNECTING CARE

Staff training and awareness

- Mandatory training course - Information Governance and Data Security
  - Assessments needed to pass
  - Annual renewal schedule
- Phishing and social engineering awareness – regular simulated tests and follow up courses
- Policies
  - Data Quality
  - Data Protection
  - Data handling
  - DPIA
  - Information security & risk
  - Information Governance
  - Cloud Security
  - Record Retention
  - Starters and Leavers
  - Subject Access Requests

INTERWEAVE
CONNECTING CARE

In Summary

- Implement best practice measures and controls
- Continuous monitoring
- Regular training and supply chain audits
- Update to handle evolving threats
- Compliance with standards and regulations
- Be able to recover!

Thank you!

INTERWEAVE
CONNECTING CARE

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

Morten Kjaersgaard
Chairman and Founder
Heimdal®

Heimdal®

Building Cyber Resilience in the NHS: Compliance, Risk, and Security.

05 March | 3rd NHS Cyber Security Conference | Convenzis

www.heimdalsecurity.com

Morten Kjaersgaard

Chairman & Founder, Heimdal

With over **16,000 organizations** globally relying on Heimdal, we are committed to **securing healthcare data, reducing attack surfaces, and mitigating risks**—all while enabling IT teams to focus on patient care rather than firefighting threats.

Let's Connect

Securing Healthcare: Cybersecurity Challenges in the NHS

Heimdal®

81%

Rising Cyber Threats

81% of UK healthcare providers experienced **ransomware attacks**, highlighting significant vulnerabilities.

Gov News 2024

20+

Complex Software Ecosystem

Healthcare institutions manage over 20 critical IT systems, including EMRs, IoT devices, and third-party applications, creating **multiple entry point**s for cyber threats.

Global Lockton 2025

55%

Monitoring & Detection Gap

55% of healthcare organizations lack **real-time threat detection** capabilities, leaving them vulnerable to undetected breaches.

Proofpoint 2024

Strict Compliance Frameworks

CYBER ESSENTIALS

CAF

National Cyber Security Centre

GDPR

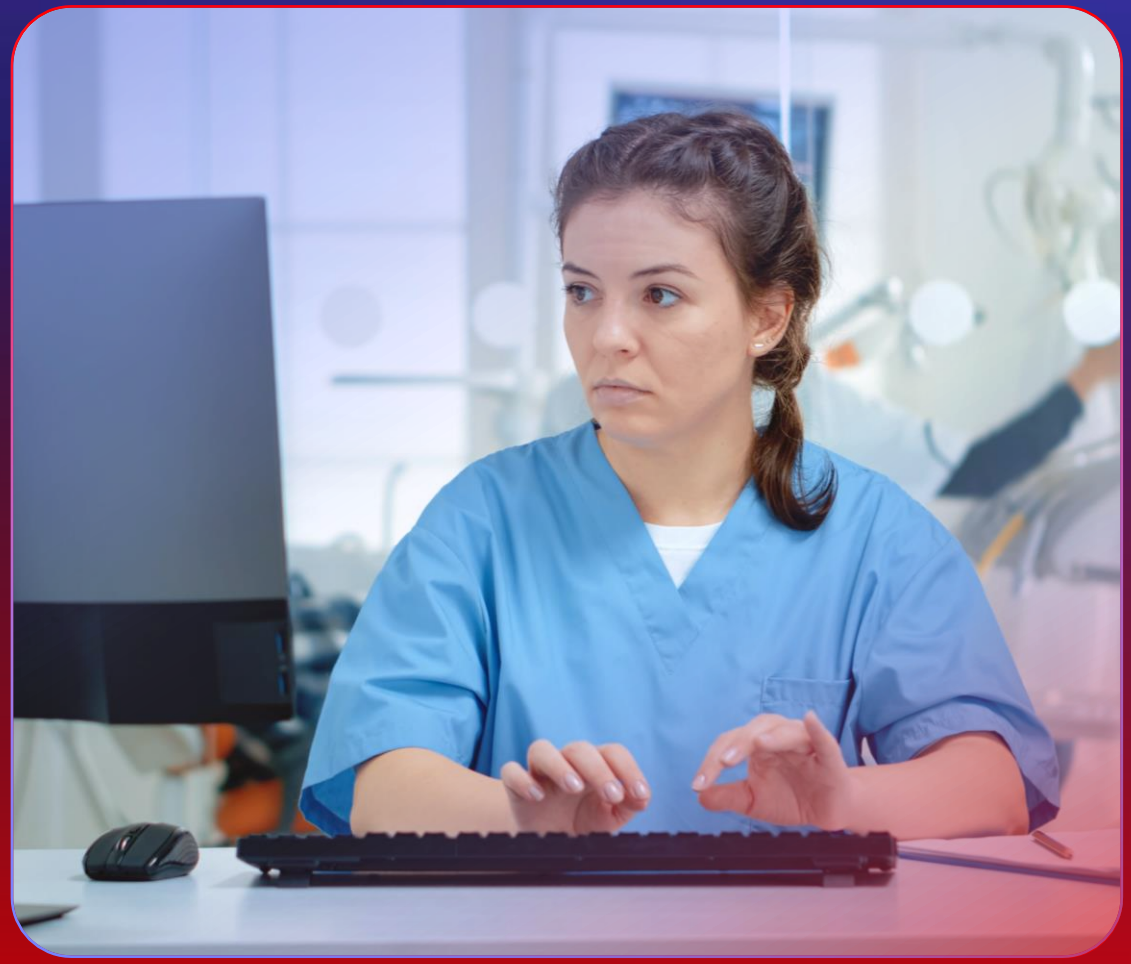
NIS2 Directive

ISO 27001

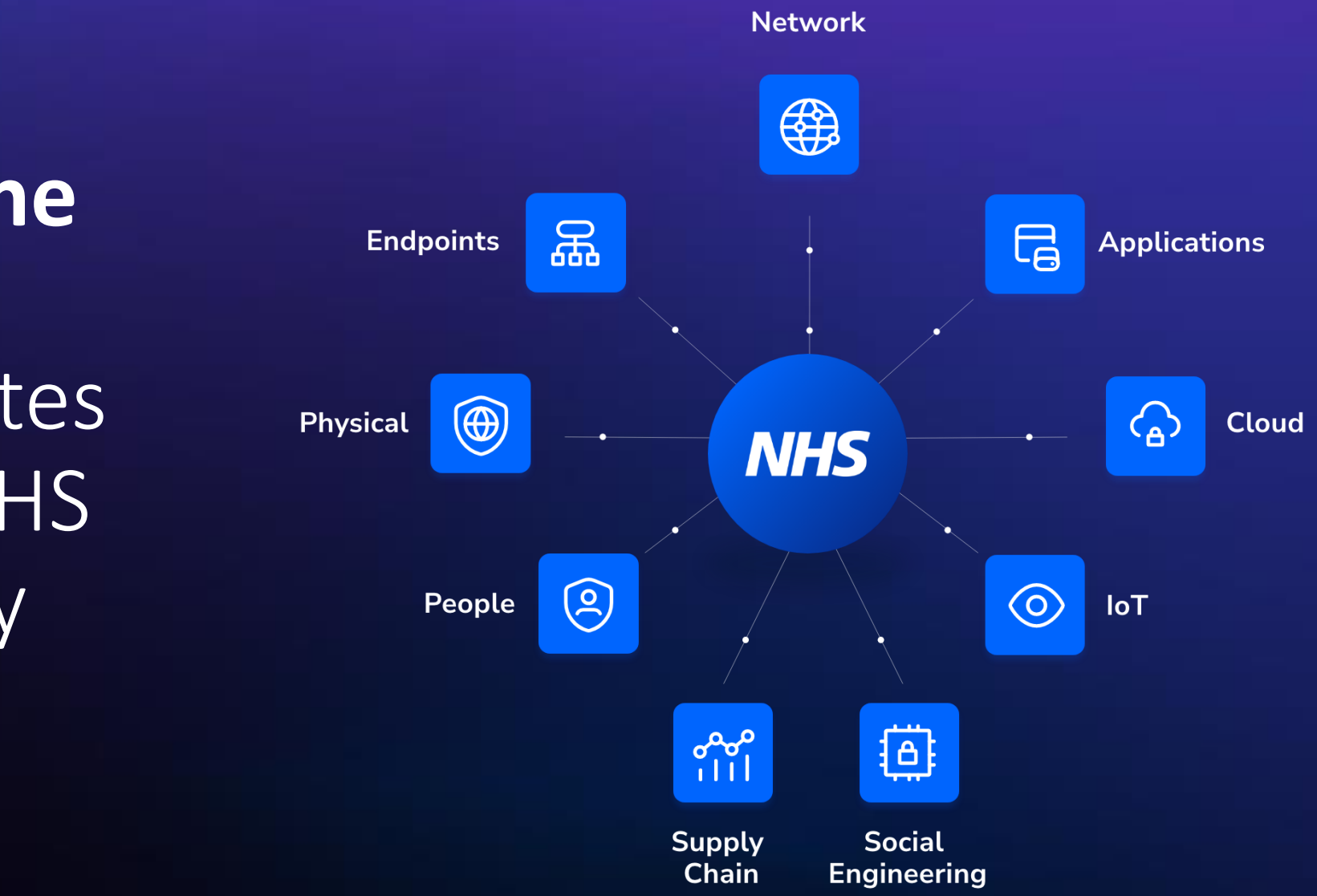
Heimdal®

What Customers Tell Us:

- Extensive Digital Infrastructure
- Valuable Data
- Operational Continuity is Critical
- Growing Threat of Ransomware
- Security is Not the Primary Focus



Navigating the Vast Attack Surface: Routes & Risks for NHS Cybersecurity



Heimdal®

The Heimdal Way

One Platform. Total Security.

Heimdal®

Heimdal®

Advanced Protection for the Healthcare Sector

- Unified Security with Full Local Visibility
- Vulnerability mgmt. w. IPXE & License mgmt.
- Rights Mgmt. (PEDM), App Control w. , AppFencing
- Heimdal NGAV with USB mgmt. that supports NHS CSOC
- Compliance, Governance & Audit Reporting
- 24x7 Security Operations Centre

Cybersecurity Manager

Greater Manchester Hospital

“After a POC, we quickly decided to go with Heimdal Patch & Asset Management. The product practically sold itself: it works seamlessly with no disruptions or headaches, and you can see the results right away. It saves us a lot of time, effort, and money.”

Head of IT Infrastructure

Mid Cheshire Hospital

“Heimdal Application Control ticks all our needs: a perfect cost-effective solution for our environment, a knowledgeable and supportive team, and high coverage to protect major attack surfaces.”

Navigating the Maze: The Complexity of Multivendor Cybersecurity Landscapes

Heimdal for Healthcare – Modular Extended Coverage

Heimdal®

Cloud Security

- M365 Email Security
- M365 User Security
- CASB
- Cloud Workspace Ransomware Protection (MS One Drive)

Network Security

- DNS Security - Network

Endpoint Security

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

Vulnerability Management

- Patch & Asset Management
- Infinity Management

Privileged Access Management

- Privilege Elevation & Delegation Management
- 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)

Unified Endpoint Management

- Remote Desktop
- BitLocker Management
- Scripting
- USB Control

XDR MXDR Platform & SOC Services

- Extended Detection & Response (XDR)
- Managed Extended Detection & Response (MXDR)

Heimdal®

Compliance

Made Easy

Heimdal®

CAF Standards

Establishes structured security measures across healthcare, ensuring **risk assessments, privileged access management, and threat monitoring** to protect critical NHS infrastructure.

Cyber Essentials & NIS2

Requires healthcare organizations to achieve Cyber Essentials certification and align with NIS2 regulations, ensuring **baseline security** protections against common cyber threats

Ransomware Payment Bans

UK policy discussions are shifting towards **prohibiting ransomware payments**, urging NHS organizations to focus on **prevention, resilience, and incident response** rather than paying attackers.

Cyber Essentials: Controls & Solutions

Heimdal®

1. Firewall
2. Malware Protection
3. Patch Management
4. Secure Configuration
5. User Access Control

Recommended Modules

- Next-Gen Antivirus & XTP
- DNS Security
- Patch & Asset Management (PAM)
- Privilege Elevation & Delegation Management (PEDM)

Cyber Assessment Framework (CAF): Controls & Solutions

Heimdal®

A

A1 Governance
A2: Risk Management
A3: Asset Management
A4: Supply Chain

B

B1: Policies, Processes, and Procedures
B2: Identity and Access Control
B3: Data Security
B4: System Security
B5: Resilient Networks and Systems
B6: Awareness and Training

C

C1: Monitoring Coverage
C2: Proactive Security Event Discovery

D

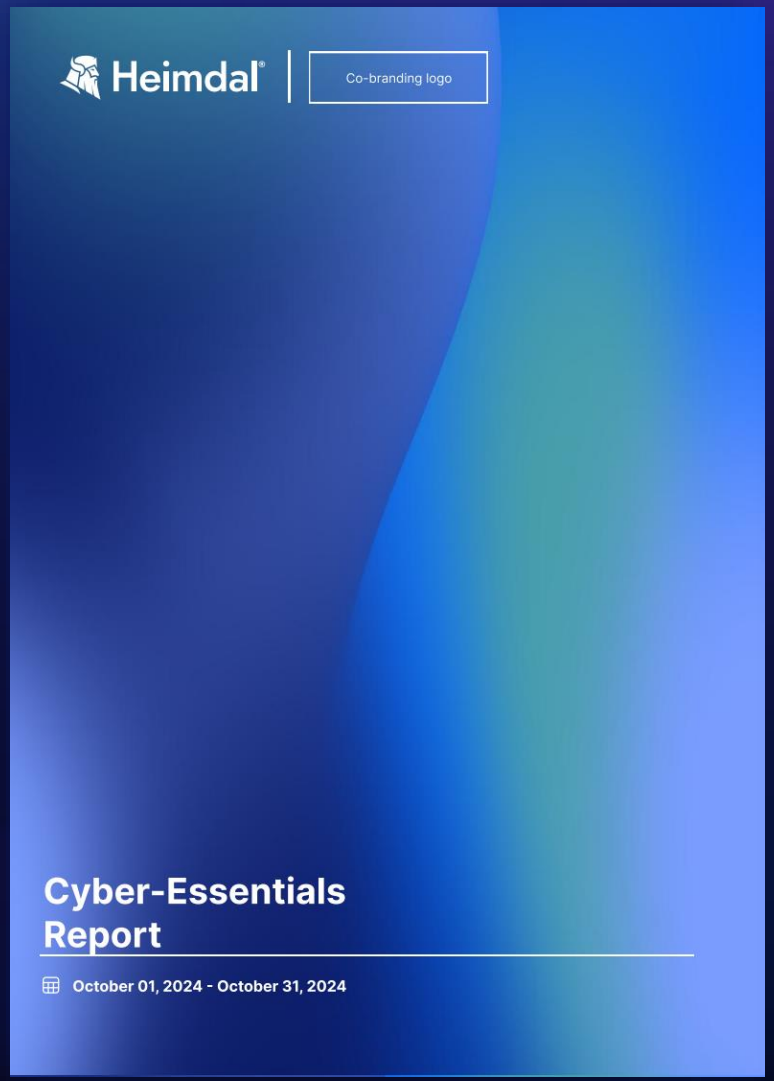
D1: Incident Response
D2: Lessons Learned

Recommended Modules

- Threat Hunting & Action Center (TAC)
- Privilege Elevation & Delegation Management (PEDM)
- Patch & Asset Management (PAM)
- Ransomware Encryption Protection (REP)

Compliance View: Single Pane of Glass View Across Your Estate

Automated Compliance Reports



Automated Compliance Reports

Heimdal | Co-branding logo

Cyber-Essentials Report

October 01, 2024 - October 31, 2024

1. Device compliance

Device name	Group Policy	Operating System	NGAV	Firewall	Brute Force	Isolation	Admin Rights	XTP	Patching Status	Compliant
Ioana's PC	Group Policy 1	Windows	!	✓	!	✓	✓	✓	✓	!
Work Laptop 1	Group Policy 2	Windows	✓	✓	✓	✓	✓	✓	✓	✓
Desktop 1	Group Policy 1	Windows	!	✓	!	✓	✓	✓	✓	!
Stefan's Workstation	Group Policy 2	Windows	✓	✓	✓	✓	✓	✓	✓	✓
Cosmin VM	Group Policy 2	Windows	✓	✓	✓	✓	✓	✓	✓	✓
Support Workstation	macOS GP	macOS	✓	NA	NA	NA	NA	NA	✓	NA
Pre-Sales VM	Linux GP	Linux	NA	!	NA	NA	NA	NA	✓	NA
Ioana's Galaxy S21	Android GP	Android	✓	NA	NA	NA	NA	NA	NA	NA

✓ **Compliant** - module/option is enabled or status for the specific category is OK

! **Not Compliant** - module/option is not enabled or status for the specific category is not OK

NA **Does not apply** - Heimdal cannot establish the compliance status due to lack of data

Heimdal | Co-branding logo

Cyber-Essentials Report

October 01, 2024 - October 31, 2024

2. Secure configurations

Active Directory	Password Length status (min. 12 characters)	2FA Status
DevelopmentTeam	✓	!
Pre-SalesTeam	✓	✓
SupportTeam1	!	!
SupportTeam2	✓	✓
FinanceTeam	✓	✓
ITAdmins	✓	!
ManagementTeam	✓	!
ComplianceTeam	!	✓

✓ **Compliant** - module/option is enabled or status for the specific category is OK

! **Not Compliant** - module/option is not enabled or status for the specific category is not OK

ⓘ Data extracted from Azure AD settings

Strategy for ICBs

Multi-tenancy Architecture & Approach

NHS ICBs: Security at Scale, with Local Autonomy

Heimdal®

NHS

Integrated Care Board

Central Funding, Management & Local Procurement

Adopt only what you need

Economy at scale

Individual needs with no co-dependency

Integrates with NHS Eng

Regional cyber maturity

Heimdal®

Exclusive Offer

Heimdal Essentials for the NHS

Exclusive Convenzis NHS Offer: Heimdal Essentials for Healthcare

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

Q&A

See it in Action:
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

Keynote Presentation

Garvin Taylor
Lead Client Service Manager,
Health Economic Unit

Health Economics Unit

ML
A care system support organisation

“We are not in Kansas anymore”

Garvin Taylor
NHS Lead Client Service Manager
Health Economics Unit

What do you remember about 2011?

- Government launch Policy Paper “Cyber Security Strategy”
  - No GDRP until May 2015
  - No Data Protection act 2018

MyHIVforum was launched

Unlocking insights

The myHIVForum: A vibrant space capturing life-defining reflections of its members

Topic Modelling: Harnessing the power of Natural Language Processing (NLP) to explore the abstract 'topics' within the forum posts

Our Objective:

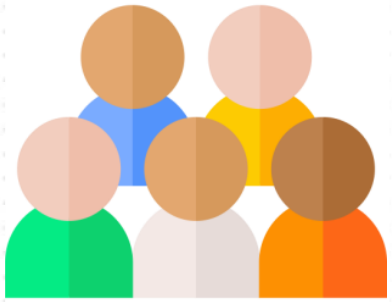
- To gain a deeper understanding of the issues and themes that matter most to the members of the myHIVforum
- Understand the impart of HIV, on the lives of people living with HIV in areas ranging from relationships and sexuality to housing ,work and mental health
- Understand changes in HIV care and treatment and health workers attitudes towards people living with HIV

The myHIVForum: Data

51,000 Forum Posts

Only platform for people living with HIV
- Mainly anonymous posts
- Confidentiality was not protected legally
- Stigma attached to a persons' HIV status

5000 members



Remove personal data

3 stakeholder meetings
- Current forum members
- THT
- THT volunteers
- HEU team

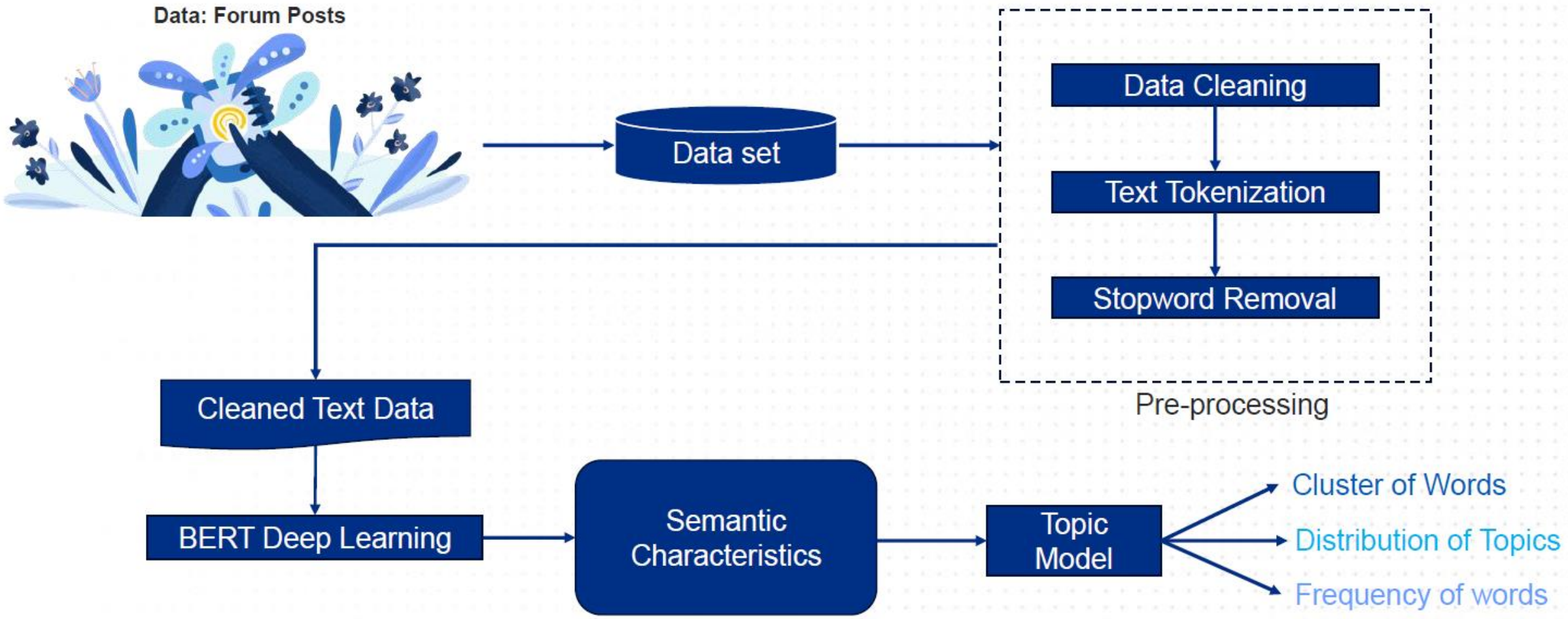
7000 Topics

Raw Text

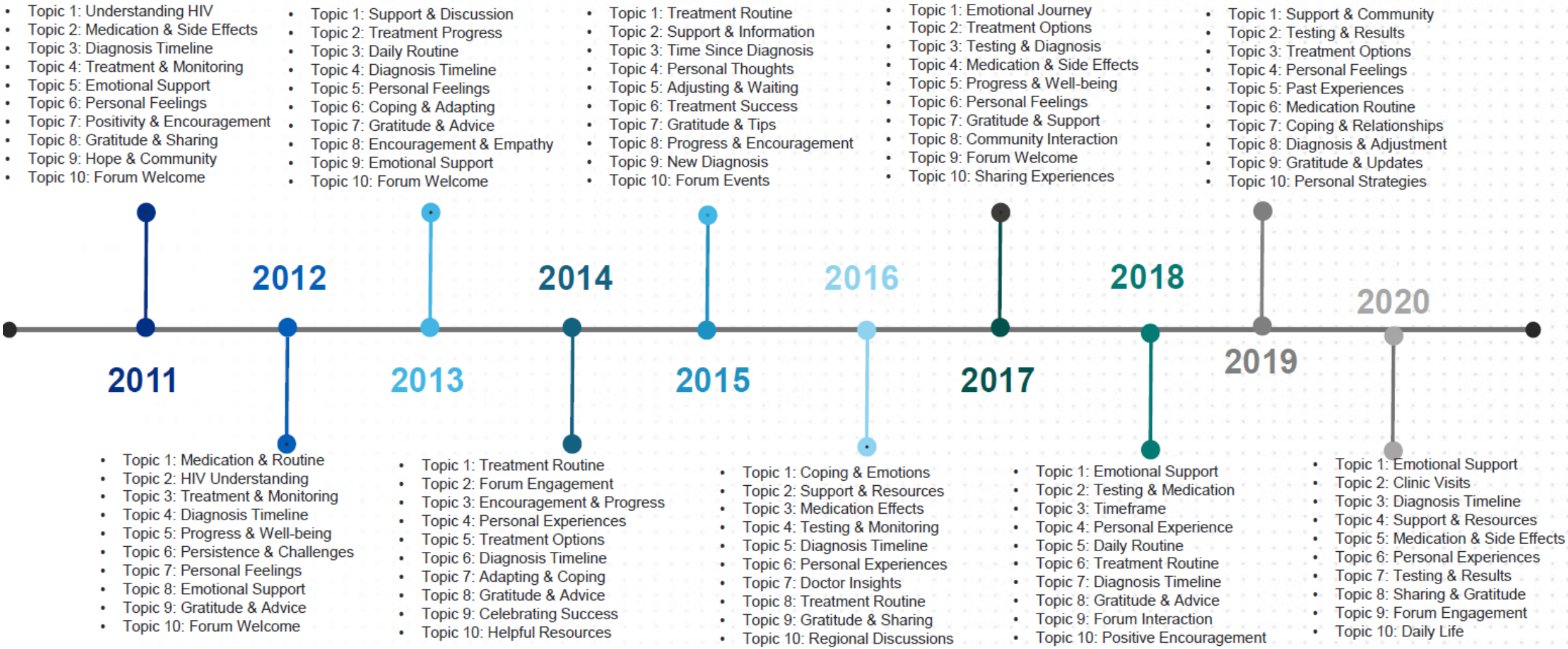
Post Date

Post Country

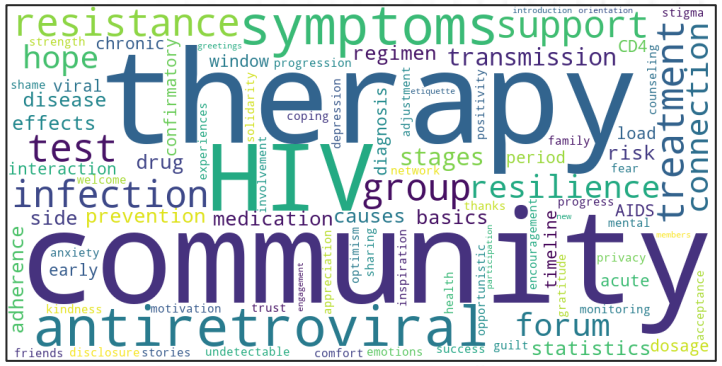
Process


Data: Forum Posts
Data set
Data Cleaning
Text Tokenization
Stopword Removal
Pre-processing
Cleaned Text Data
BERT Deep Learning
Semantic Characteristics
Topic Model
Cluster of Words
Distribution of Topics
Frequency of words

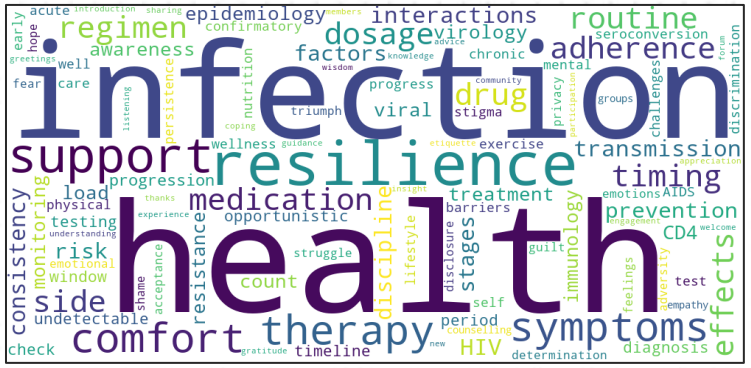
Results: Dynamic Topic Modelling across UK 2011 2020



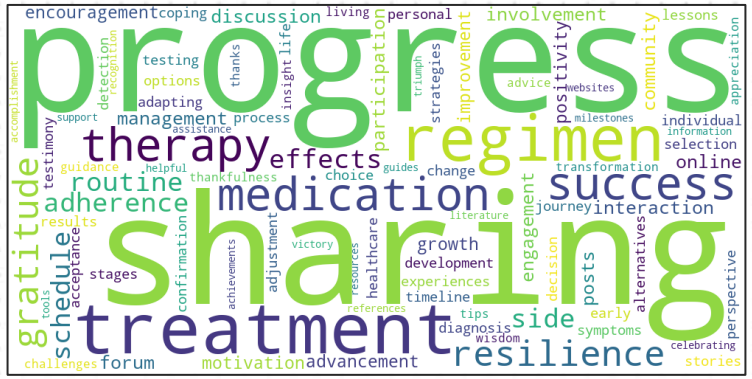
How did the conversation evolve over time?



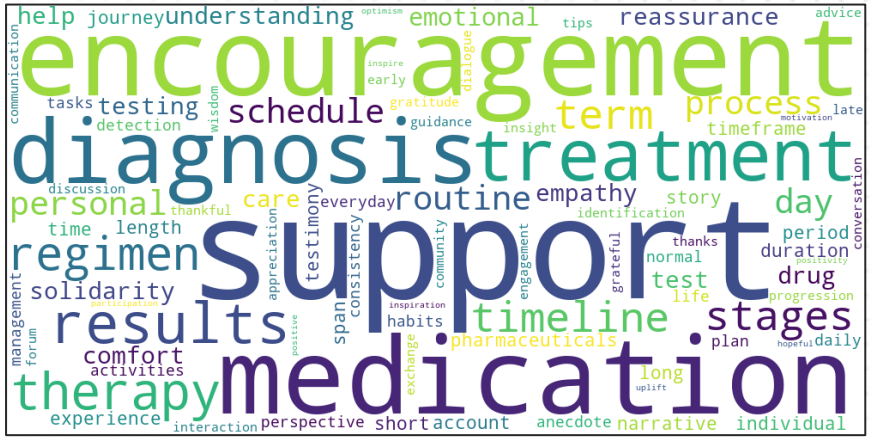
2011



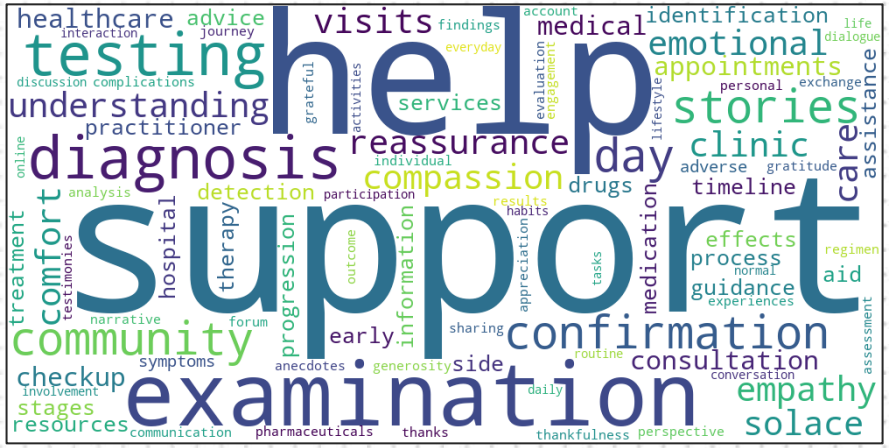
2013



2015



2018



2020

Conclusion

- A decade long collection of personal and diverse patients' narratives were saved
  - Better understanding of the impact of digital health communities on patient centred care
  - The concerns and challenges of people living with HIV was mapped out over time
  - Better understanding of the evolution of NHS medical pathways
  - Peer to Peer support was critical in the early days where limited information was available

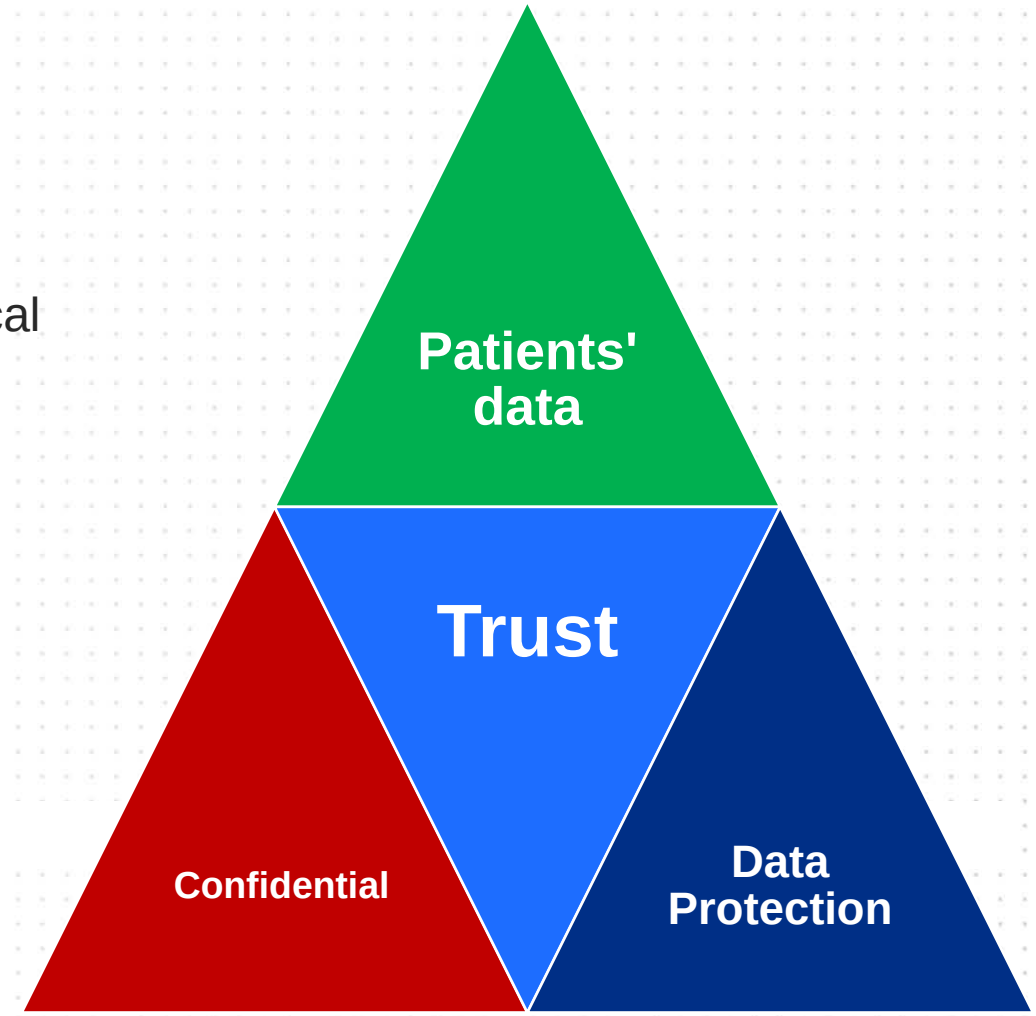
We’re not in Kansas anymore

We’re not in Kansas anymore

The importance of Trust to reduce Health inequalities

- People with protected characteristics must trust that their medical data is secure and will not be “weaponised” against them at a future date
- Health inequalities will increase, if we do not protect their data
- Ensuring confidentiality of the patient's information is critical

Build trust with data collection to continue to improve and reduce health inequalities with potentially vulnerable minority groups



Health Economics Unit

ML
A care system support organisation

Thank you


garvin.taylor@nhs.net


https://healtheconomicsunit.nhs.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

Keynote Presentation

Patrick Maw
Consultant Clinical Scientist
University College London Hospital

Connected Medical Devices

Patrick Maw - Consultant Clinical Scientist
Medical Physics and Biomedical Eng
University College London Hospital

March 2025

What is a Medical Device?

- Medical Device Directives 93/42/EEC
- Any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, together with any accessories, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application, intended by the manufacturer to be used for human beings for the purpose of:
- Diagnosis, prevention, monitoring, treatment, or alleviation of disease
- Diagnosis, monitoring, treatment, alleviation of, or compensation for an injury or handicap
- Investigation, replacement, or modification of the anatomy or of a physiological process
- Control of conception
- This includes devices that do not achieve their principal intended action in or on the human body by pharmacological, immunological, or metabolic means—but may be assisted in their function by such means.

Regulations

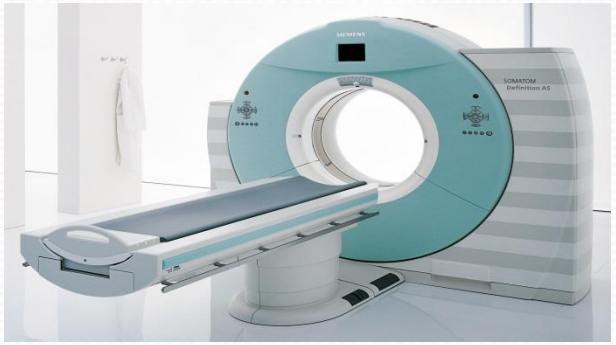
- Essential Requirements for Performance and Safety (GSPR)
- Classification of Medical Device by risk – Class I (Low), IIA, IIB (Medium) and III (High)
- Medicines and Healthcare products Regulatory Agency (MHRA) – Competent Authority for UK – Previously the MDA
- Application through law of the MDD
- Later revisions to the MDD 1993 and the new MDR recognise software as a Medical Device.

Classification of Medical Devices by Risk

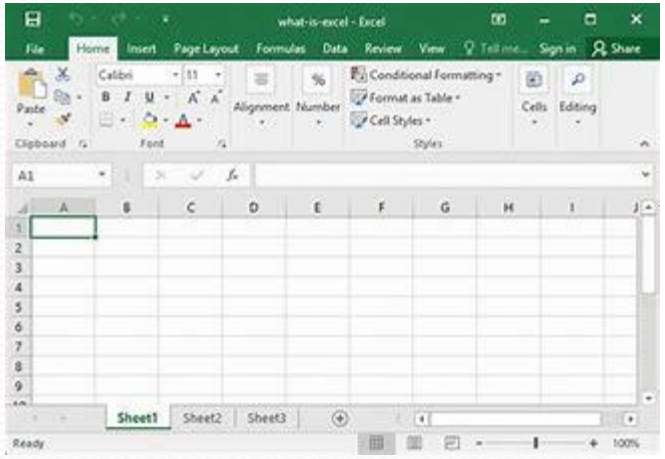
- Class I
- e.g. Surgical Gauze, Wheelchairs
- Class IIA
- e.g. Hearing Aids, Ultrasound Equipment, Patient Monitors
- Class IIB
- e.g. Infusion Devices, Surgical Lasers
- Class III
- E.g. Prosthetic Joints, Stent Graphs
- Changes to the medical device requires the CE marking process to be carried out for re validation.

What do Networked Medical Device look like?

Traditional Medical Devices

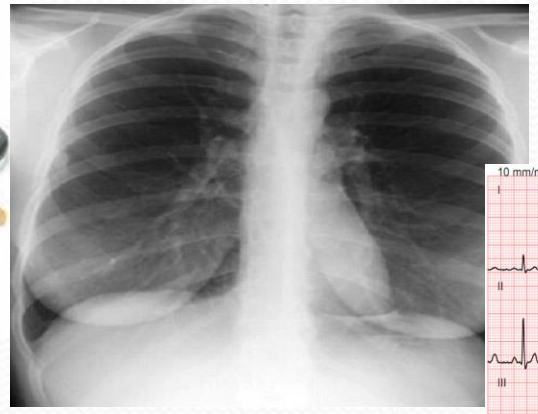


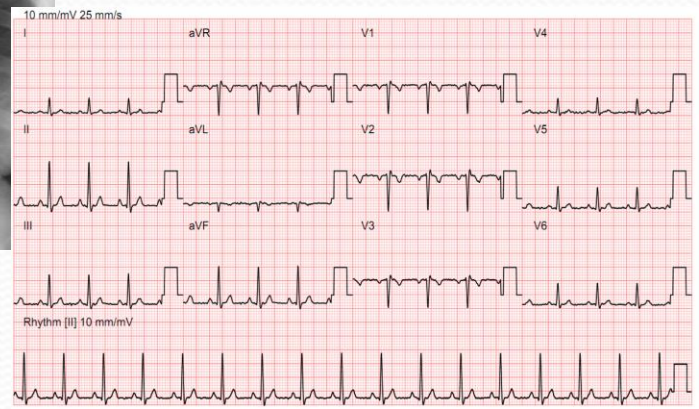
Software medical devices



Why Network Medical Devices?

- Requirement for an Electronic Patient Record (EPR).
- What we have\had:





What we have\had.

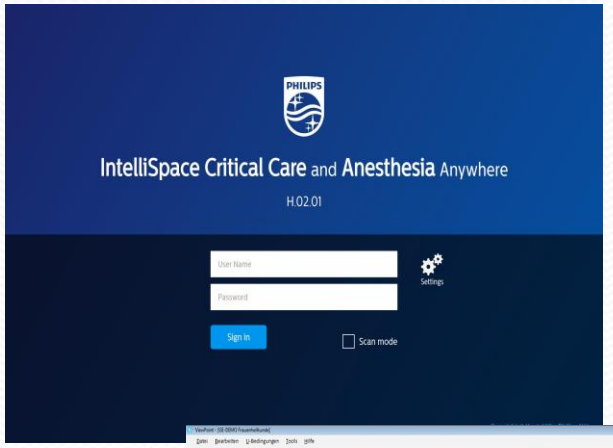
DAILY REPORT SCHEDULE

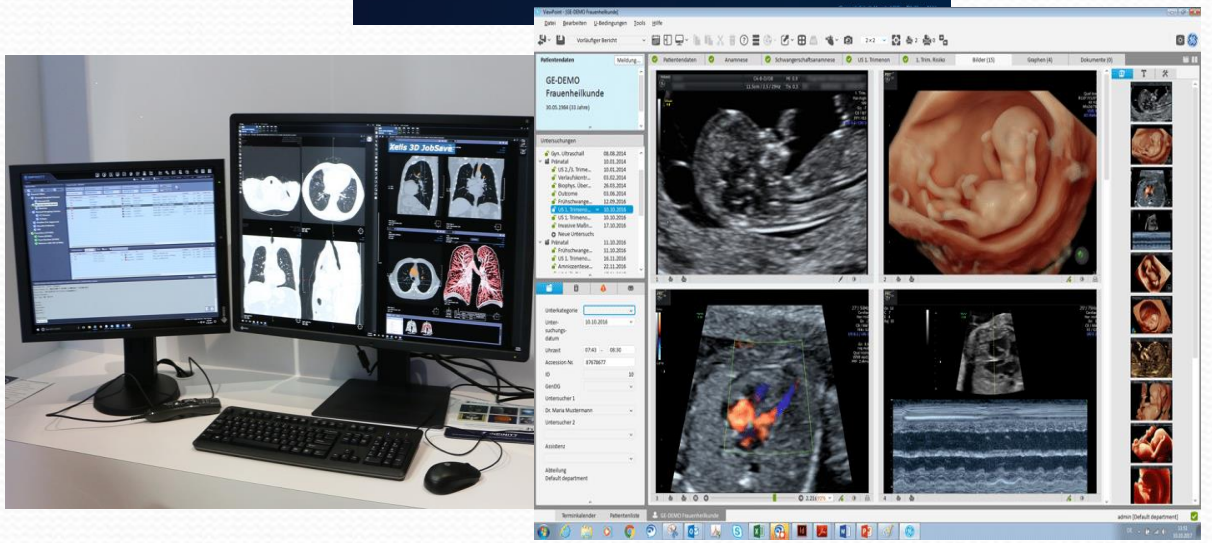
PATIENT NAME																
TIME	7AM	11AM	3PM	7PM							3PM	7PM	7AM	11AM	3PM	7PM
B/P																
HR																
RR																
O2 SAT																
TEMP																
GLU																
PAIN																
PAIN IV MEDS CHECKS	@ □ 15 □ 15 □ 30	@ □ 15 □ 15 □ 30	@ □ 15 □ 15 □ 30	@ □ 15 □ 15 □ 30							@ □ 15 □ 15 □ 30	@ □ 15 □ 15 □ 30	@ □ 15 □ 15 □ 30	@ □ 15 □ 15 □ 30	@ □ 15 □ 15 □ 30	@ □ 15 □ 15 □ 30
MISC CHECKS	□ □	□ □	□ □	□ □							□ □	□ □	□ □	□ □	□ □	□ □

PAT

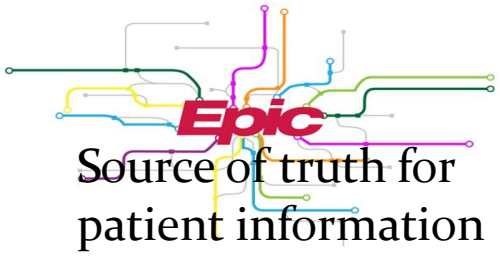
PATIENT	0700	0800	0900	1000					1500	1600	1700	1800

Medical IT Systems

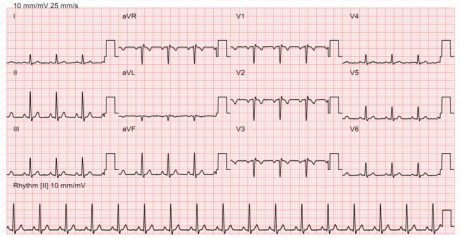


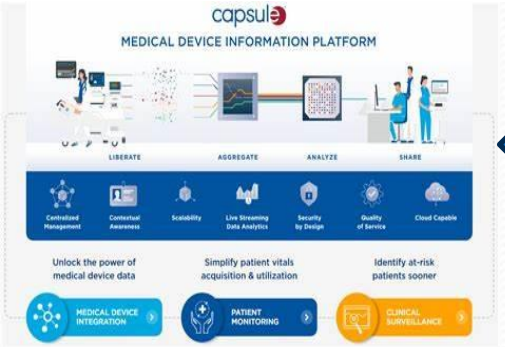


Transition to a new EHRS

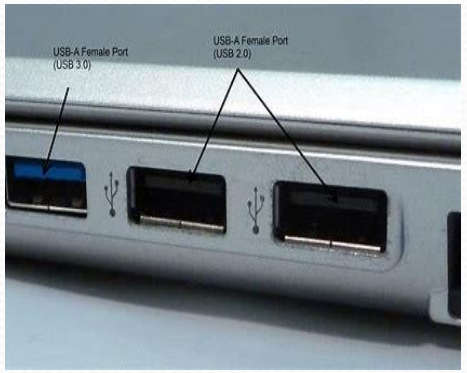


Source of truth for patient information





Device Connections




Wanna Decryptor 1.0
Ooops, your files have been encrypted!
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. (But you have not so enough time.)
You can try to decrypt some of your files for free. Try now by clicking <Decrypt>.
If you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
How Do I Pay?
Payment will be raised on
5/15/2017 16:25:02
Time Left
02:23:58:28
Your files will be lost on
5/19/2017 16:25:02
Time Left
06:23:58:28
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
QR Code
15zGqZCTcys6eCjDkE3DypCjXi6QWRV6V1
Copy
Check Payment
Decrypt

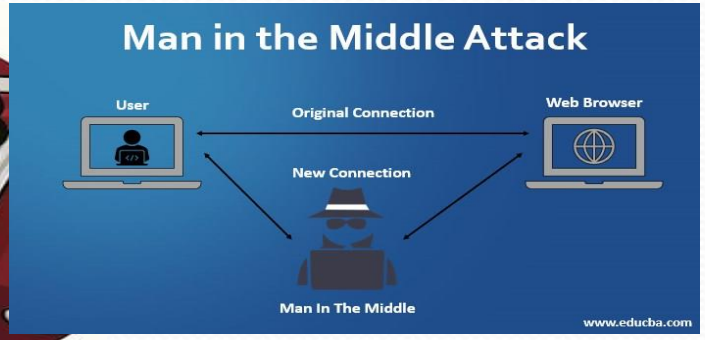
What are the problems?

- A lot of current Medical Devices are based on Windows Operating Systems.
- More importantly older Windows OS's -

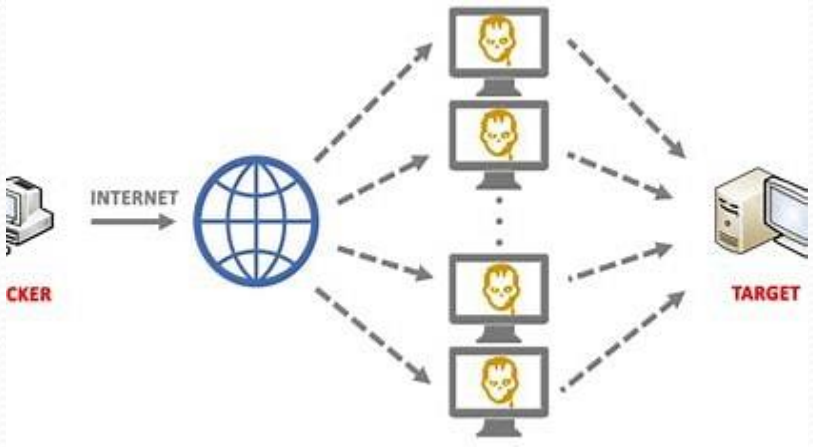
What are the problems?

- Operating systems such as:

What are the threats?



138 known hacking groups

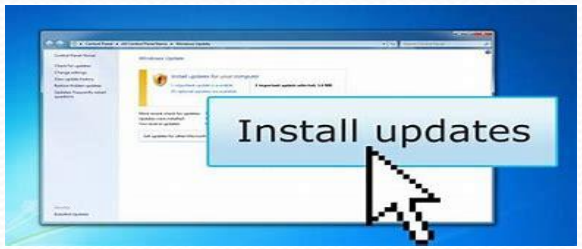


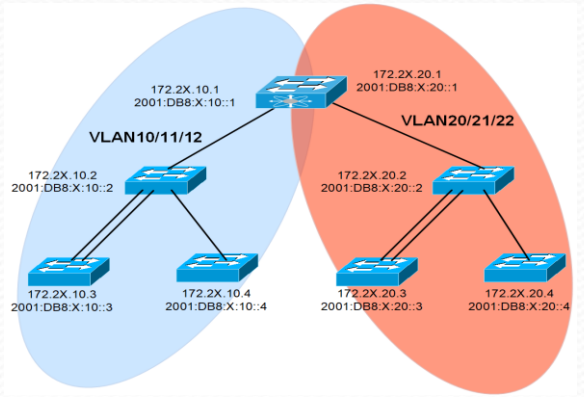
Networked Medical Devices

- How do we deal with this???

- NO – We implement measures to mitigate the risk.

How are IT networks protected?





Why is this a problem?

- Traditional medical device patches can arrive months after any known exploits.
- Also unlikely to be able to run any AV
- Monitoring Agents cannot be installed.

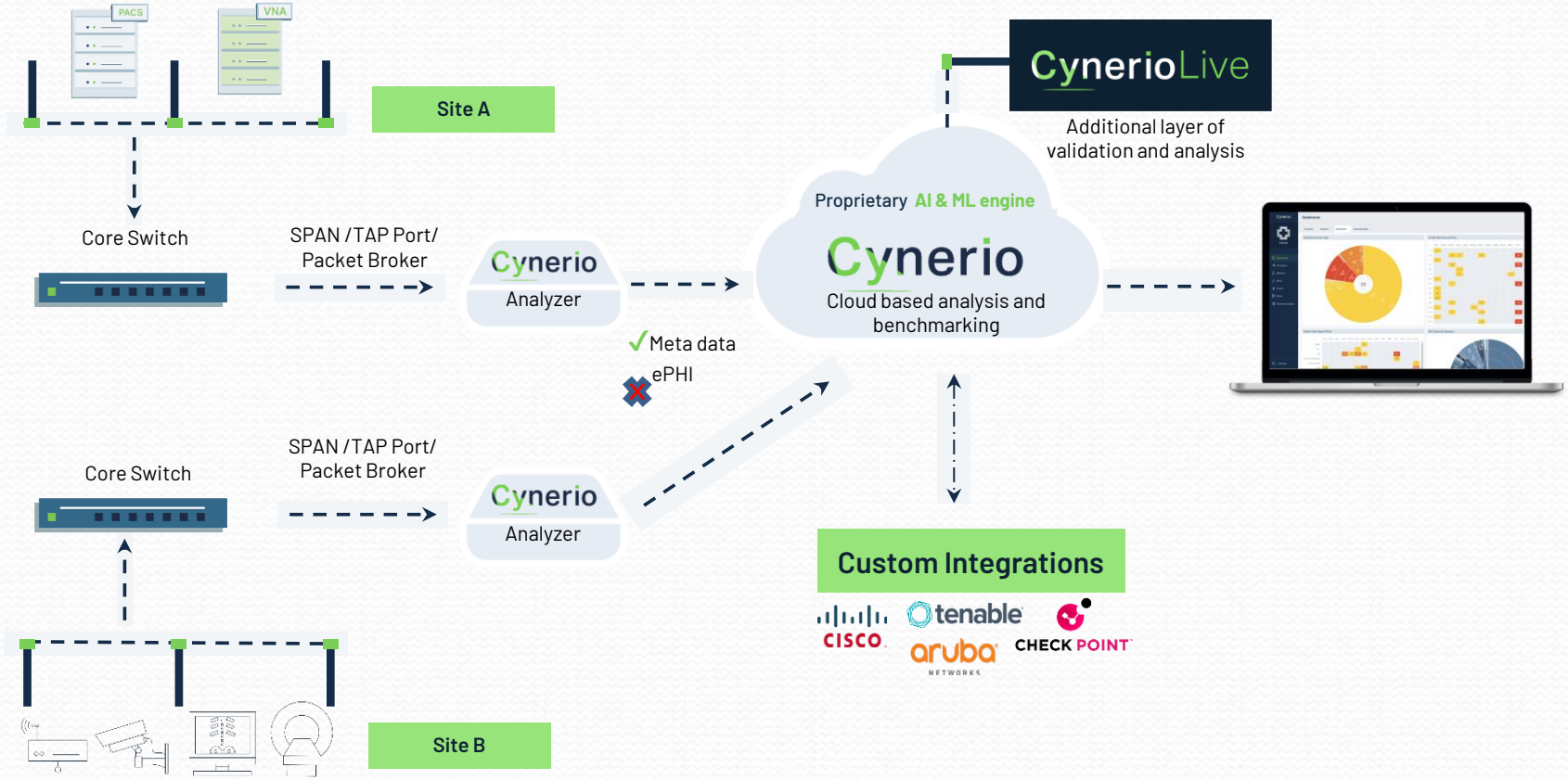
- Software medical devices that run on standard PC hardware may not be allowed to install patches or AV if the manufacturer doesn't allow.
- This would invalidate the CE\UKCA marking.

Why is this a problem?

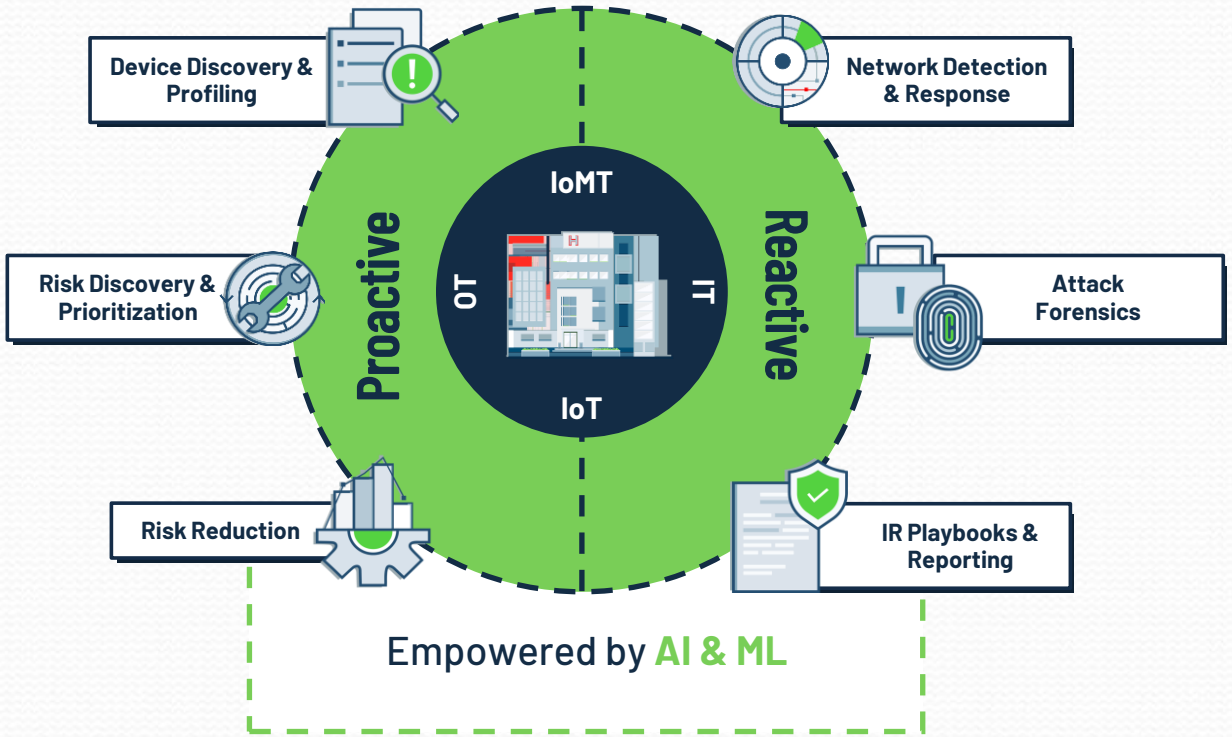
- No Visibility of traditional medical devices
- No Real Time information on cyber issues
- No idea what devices are communicating with

AI Based Intrusion Detection

How Does It Work?



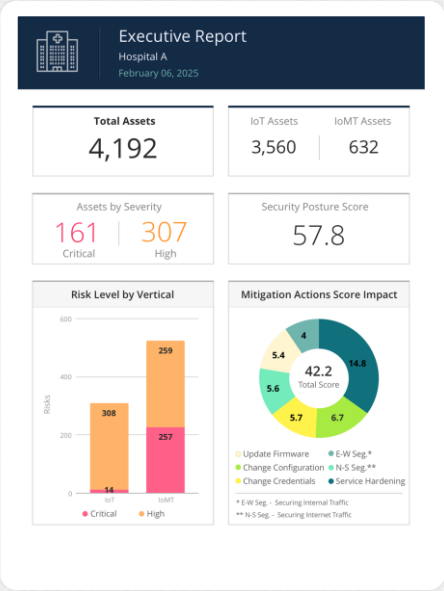
Cynerio Platform: Security First Approach

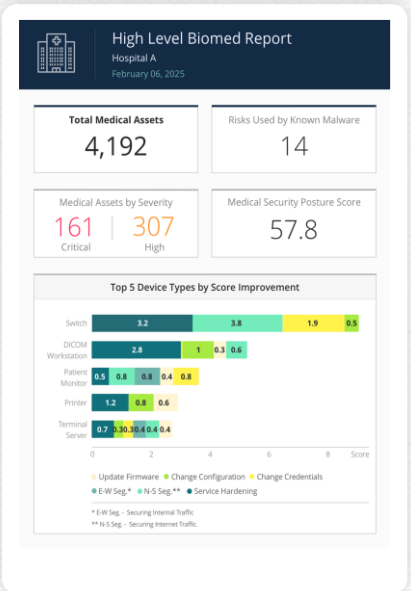


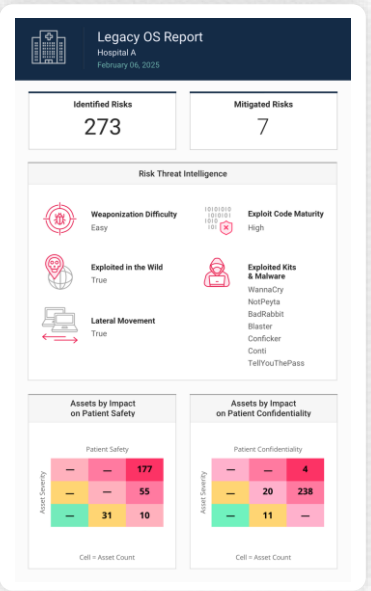
Complete Asset Visibility - Medical / IoT / IT / OT

- Automated Discovery and Analysis
- Over 150 Attributes per device
- Single Pane of Glass
- Location Information with integrations to Wireless systems
- Device/Fleet Utilization (Daily and last 30 days)
- Digitized MDS2 forms for ease of search/ FDA recalls

Reporting Center





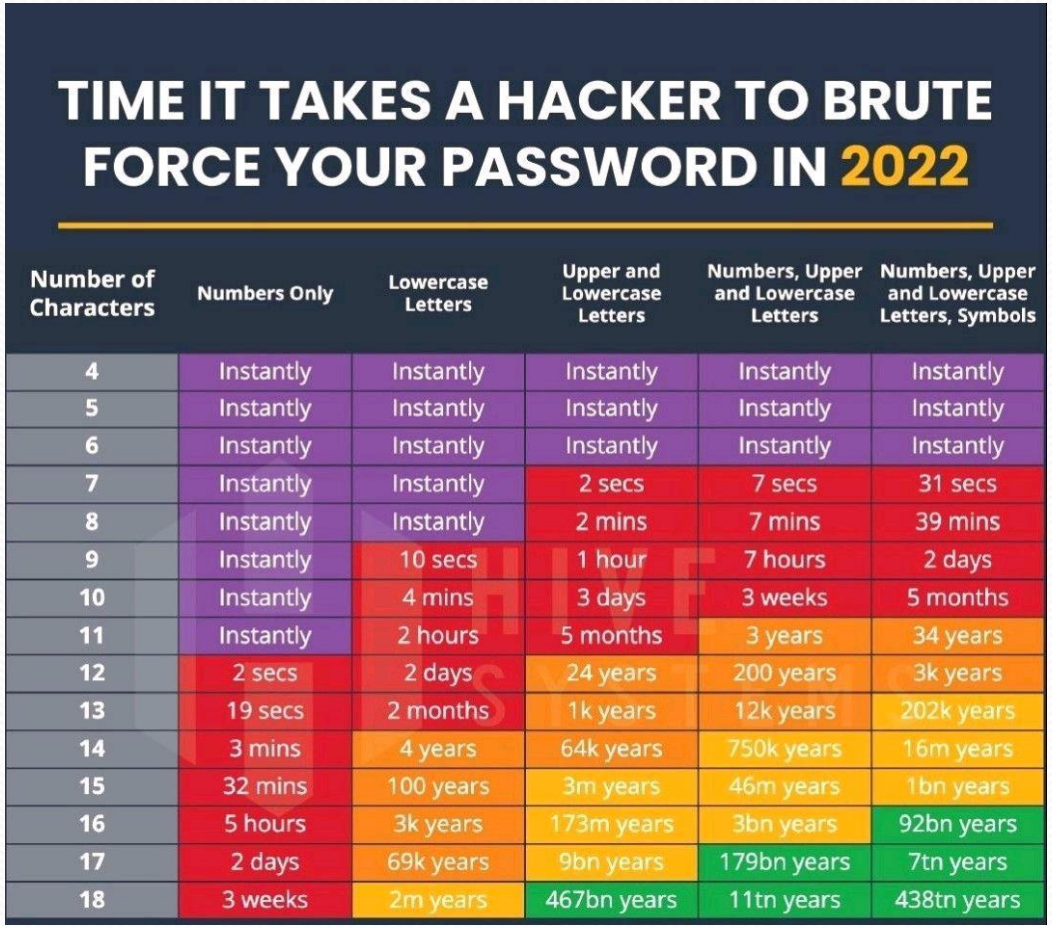


- **Role based access & customization**
- **Simplified internal & external audits**
- **Automated compliance reporting**
- **Time-saving automation & reduction of manual work**

Things to remember

- Medical Devices share the same vulnerabilities as PC's when networked.
- However the differences due to regulation must not be forgotten.
- If handled correctly there is a great benefit to the care path of a patient.
- Most of the standard protective measures apply.
- Anti-virus, Patching and Password complexity.

Password Security



TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

Questions??????

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

Steven Furnell
Professor of Cyber Security
University of Nottingham

Patrick Maw
Consultant Clinical Scientist
University College London Hospital

Andrew Wright CISSP CISM
Joint Head of Cyber Security and information Assurance
NHS – Hillingdon and LNWH Hospital Trusts

Slido

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

SCAN ME

Keynote Presentation

Gavin Stone

Intelligence Officer. Mentor & Trainer. Body Language Expert. Media Talent & Public Speaker. Best Selling Author. Guest Host NBC Radio