Harder for hackers.
Simpler for you.

TREND MICRO™

TACKLING THE CHALLENGE OF NHS CYBERSECURITY

Discover how Trend Vision One ™ can secure your vast digital estate

CONTENTS

SECTION 1: INTRODUCTION

For NHS cybersecurity teams, the stakes are as high as they get, but operational skills deficits, tight budgets and supply chain risks persistently complicate their ability to defend critical infrastructure from cyber attacks.

- **NHS cybersecurity spending:** An NHS England programme aimed at expanding cybersecurity resilience faced budget cuts of 50% in 2024[1].
- **Impact of cyber incidents on patient care:** During the WannaCry ransomware attack, at least 34% of trusts in England were disrupted, leading to thousands of cancelled appointments and operations, with A&E patients having to travel further to be treated[2].
- **Cost of data breaches:** The average cost of a healthcare data breach from year 2023-2024 was £7.31 million, with costs related to breach management, legal fees, and regulatory fines[3].
- **Frequency of cyber attacks:** On average, NHS England's National Cyber Security Operations Centre (CSOC) blocks 21M malicious items every month. In 2024, the NHS saw a 300% increase in cyber incidents, compared to 2019[4].
- **Skills gap:** A 2024 survey on behalf of the UK's Department for Science, Innovation and Technology (DSIT) estimates that 24% of public sector organisations have a basic technical skills gap for cybersecurity[5]. This could be mediated by enhanced automation.

1 https://www.hsj.co.uk/technology-and-innovation/exclusive-cyber-security-budget-faces-50-cut/7036924.article

2 https://www.gov.uk/government/publications/cyber-security-strategy-for-health-and-social-care-2023-to-2030/a-cyber-resilient-health-and-adult-social-care-system-in-england-cyber-security-strategy-to-2030#current-and-emerging-threats

3 https://www.statista.com/statistics/387861/cost-data-breach-by-industry/

4 techUK briefing with Mike Fell, Director NHS National Cyber Operations (2024), https://www.youtube.com/watch?v=cTearlsIvxw

5 https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2024/cyber-security-skills-in-the-uk-labour-market-2024#fn:7

Assessing the threat landscape

The NHS is under unprecedented strain, and threat actors know it. In 2023, globally, healthcare was the second-most impacted sector through malware, according to Trend Micro data. And it recorded the second-highest number of risk events.

The NHS has complex technology environments with multi-platform IT systems and operational technology (OT), as well as plenty of legacy systems. This creates an expansive attack surface and the potential for multiple attack vectors. The complexity of securing this environment is exacerbated by a reliance on sharing data with vendors to deliver secure products. This can make effective security measures not only more challenging, but more costly – making it less likely that CISOs and Senior IT Leaders get the resources they need.

As events such as the Synnovis, Advanced and WannaCry attacks have shown, ransomware is arguably the biggest threat facing the NHS. It can cripple supply chains and critical services – putting lives at risk – leading to a cascade of cancelled operations, overworked staff, compromised data and unwanted regulatory scrutiny.

A strategy document for cyber resilience, published in March 2023 by the **Sunak Conservative government**, acknowledged that a perfect storm of budget and skills shortages, complex supply chains and legacy IT has been brewing – and protecting the large attack surface of a decentralised health service could be extremely challenging.

5 NHS Pillars

to minimise the risk of cyber-attack

1. **Focus on the greatest risks and threats**
2. **Defend as one**
3. **People and culture**
4. **Build securely for the future**
5. **Exemplary response and recovery**

What matters for NHS cybersecurity?

- **Dynamically understand evolving risks** and how they vary across the sector.
- **Increase visibility** of your large network attack surface.
- **Right-size cybersecurity** according to threat and potential harm.
- **Clarify regulations** and lawfully adhere to them.
- **Improve resilience** of the most critical NHS supply chains.

How does Trend meet those needs?

- **Enhanced threat intelligence:** Proactive defence and timely threat detection to prevent cyber incidents before they impact operations.
- **Real-time threat monitoring:** Advanced analytics provide deep visibility into network activities, enabling quicker identification and mitigation of potential threats.
- **Flexible, scalable security:** Adaptive security that evolves with the NHS's growing needs, ensuring defences scale in line with demand while efficiently managing a vast network of contracts and suppliers.
- **Compliance and regulatory support:** Ready to support compliance with regulations such as GDPR, the Data Security and Protection Toolkit (DSPY), the Cyber Assessment Framework (CAF) and the forthcoming Cyber Security & Resilience Bill 2024.
- **Integration and automation:** Automated threat detection and response streamlines security operations, integrating security tools and vendors to enable a unified strategy for managing supply chain risk.

Why Trend?

Trend has worked with the NHS and its suppliers for decades, including the South London and Maudsley NHS Foundation Trust (SLAM) and the Great Western Hospitals NHS Foundation Trust (GWH).

For the South London and Maudsley NHS Foundation Trust, we provide unified protection against zero-day and emerging threats across physical and hybrid cloud environments, including endpoint, cloud server and SaaS (software as a service) application security. This helps the small IT team at SLAM to hunt down network-layer threats more effectively, mitigate Microsoft 365 risks that slip through native security filters, and protect cloud and on-premises servers via a single pane of glass.

"Although we added more protection to our organisation through the various suites, the centralised pane of glass Trend Micro offers hasn't added any management overheads. It's more efficient than having four different vendors in place."

Stuart MacLellan, Head of Operations for Digital Service, SLAM

For the GWH Trust, Trend protects servers and endpoints for 6,000 users and more than 300 VMware servers. A virtual patching feature is particularly useful for the Trust as legacy servers can't always be simply upgraded due to their historic data. However, this feature protects even endpoints that are no longer supported by the vendor.

"If you have a critical vulnerability, Trend Micro is always ahead of the game. We've already mitigated risk even before Microsoft has given us a patch to deal with it."

Bev Sismey, IT Technical Operations Manager, GWH NHS Foundation Trust

SECTION 2: IMPROVING OPERATIONAL EFFICIENCY

Finding time for security isn't always easy

Nationally, the NHS protects over 1.9 million network devices and is targeted by roughly 21 million malicious emails every month[6].

It is safe to say that the NHS is a prime target for digital extortion, which limits the time available for patching and other vital security tasks. The challenge is compounded by the fact that not all the systems are the same, meaning a local, case-by-case approach is needed.

Operational impact of a cyber attack

Ransomware and data breaches can both lead to downtime which may impact services for days or weeks, worsening health outcomes, draining financial resources and damaging reputation. Distracted and overworked clinicians may then be more likely to fall for phishing attacks, creating a vicious circle.

90%

of healthcare institutions have had at least one security breach in the past few years[7]

4 DAYS

approximate time to recover from just one day of downtime

46%

of healthcare organisations experiencing data exfiltration see an increase in patient mortality

AND 38%

of those organisations see an increase in complications from medical procedures

6 techUK briefing with Mike Fell, Director NHS National Cyber Operations (2024), https://www.youtube.com/watch?v=cTearIsIvxw

7 81 Phishing Attack Statistics 2024: The Ultimate Insight - Nivedita James Palatty, Astra

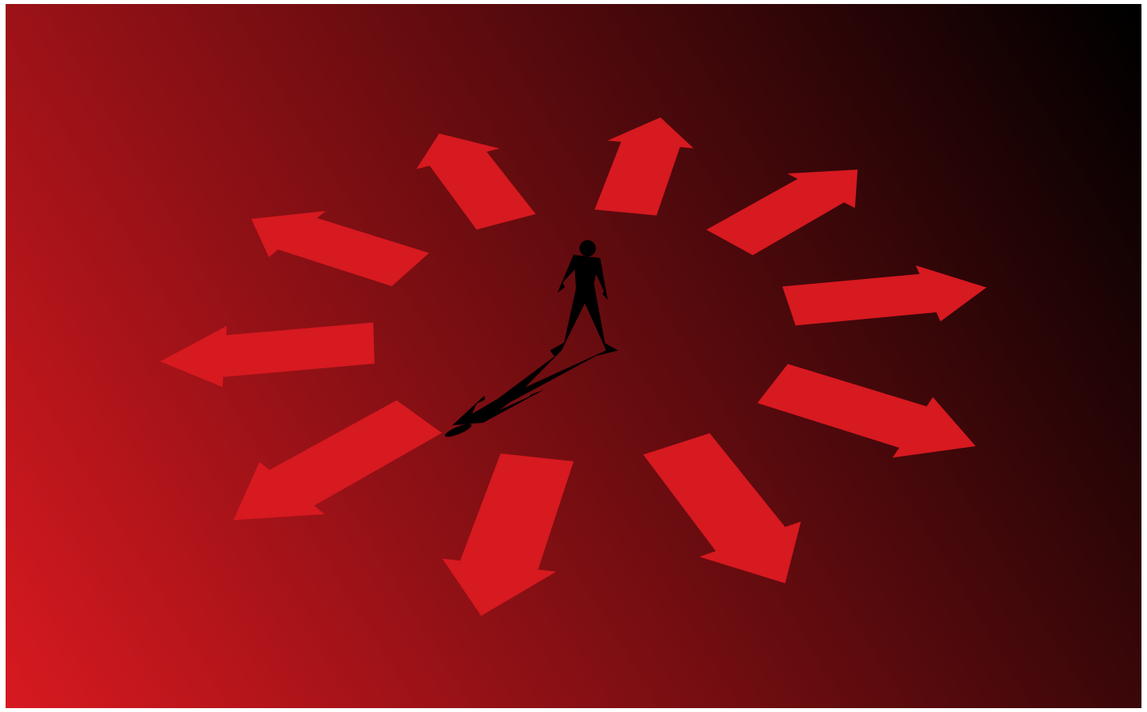
NHS operational goals and their security implications

Trend is experienced in working with the NHS' unique requirements and can offer the tools and expertise the NHS needs to ensure robust, cost-efficient network security as you work towards achieving key operational goals.

Operational goal	Security implication
Reduce variation in clinical standards and outcomes, and support the adoption of validated, efficient, cost-effective services through the Getting It Right First Time (GIRFT) programme.	This means joining up all the NHS trusts, doing so creates many more points of failure, creating vulnerability to an array of cyber-attacks.
Drive improvements in patient outcomes and experiences and ensure the best value is achieved from the NHS's investment in medicines.	Cybersecurity is crucial for patients to trust digitalised healthcare. Patient outcomes are reliant on continuous system availability and minimal downtime.
Generate more value for each pound (£) spent on corporate services and reduce unwarranted variation.	Centralised cybersecurity management reduces the workload, costs and turnover of security staff, while improving operational efficiency and value for patients.
Reduce addressable spend by leveraging collective buying power, delivering consistency, compliance and more effective contracting.	Supply chain cybersecurity raises questions for NHS trusts. For example, does the supplier prioritise cybersecurity and are their cybersecurity professionals suitably skilled?

Trend Vision One helps to minimise system downtime, for maximum operational efficiency:

- **Attack Surface Risk Management (ASRM)** continuously assesses risk, suggests recommendations and automates remediation to build resilience
- **Extended Detection and Response (XDR)** with AI empowers analysts to prioritise alerts more effectively, ensuring emerging threats are contained early
- **Generative AI** helps to upskill Security Operation Centre (SOC) analysts as they tackle fast-moving threats



SECTION 3: SUPPLY CHAIN INTEGRATION

Supply chains, extending across continents and made up of numerous partners and suppliers, are crucial to the NHS. These far-reaching supply chains present an increased risk. And any security system cuts two ways; of course you want to keep the bad things out, but you still want your service-users, partners and suppliers to be able connect.

A secure environment for sharing critical data and security protocols should already be in place, which should be able to deliver flexibility and scale to accommodate evolving needs. It's imperative this is protected by a solution that enables collaboration and information sharing among different NHS trusts and partners to enhance collective security measures.

Having a secure, pre-provisioned connectivity solution eliminates the need for the NHS to develop new B2B connections whenever a supplier is onboarded. Such an environment must deliver no-compromise protection against cyber attacks, insider threats and accidental exposure, with consistent policy enforcement at every supplier location.

Given the enormity of the task and the lack of resources available to most security teams, it is essential to have automated protection that stops known and unknown malware, exploits, credential theft, command-and-control traffic (C2) and many other attack vectors across all ports and protocols.

Previous approaches to creating B2B connections have included company-owned, managed VPNs or carrier-operated multiprotocol label switching wide area networks (MPLS WANs). These are often expensive, slow to deploy, high-latency and difficult to manage in any combination. Whereas a scalable, always-on, secure WAN that is accessible over the public internet can help to onboard global suppliers in minutes, rather than months.

Why should this secure environment be built in the cloud?

- Support global suppliers without having to set up points of presence in data centres.
- Scale automatically to cover all the right places, even during organisational changes, mergers or acquisitions.
- New sites and suppliers can be onboarded under common security policy in a fraction of the time previously possible.
- Policy changes are implemented in the cloud, providing rapid protection that fits tight timelines for risk exposure, meets management goals, and is compliant.
- Security and traffic logs processed and stored in the cloud can be scanned by machine learning algorithms to spot anomalies indicating credential theft, compromised devices or accounts.
- Cloud services enable overextended security teams to focus on security, rather than focusing on operating equipment, data centres, power, HVAC systems, etc.
- A security platform maintained and operated in the cloud reduces a significant amount of resource overhead.

Problem: You need to provision remote network access for supply chain partners who monitor and manage equipment and sales. Your acceptable use policies and trust-based access protocols are not enough to keep you secure, because 'trusted' vectors – that is, users, applications and content – can still be compromised.

Solution: Trend can provide secure, remote access to managed entities that is locked down to specific users, applications, devices and data. Plus, every file, document, script, portable executable file and process can be scanned for known and unknown malware, attempted exploits and usage anomalies.

Confidentiality, integrity and availability in the supply chain

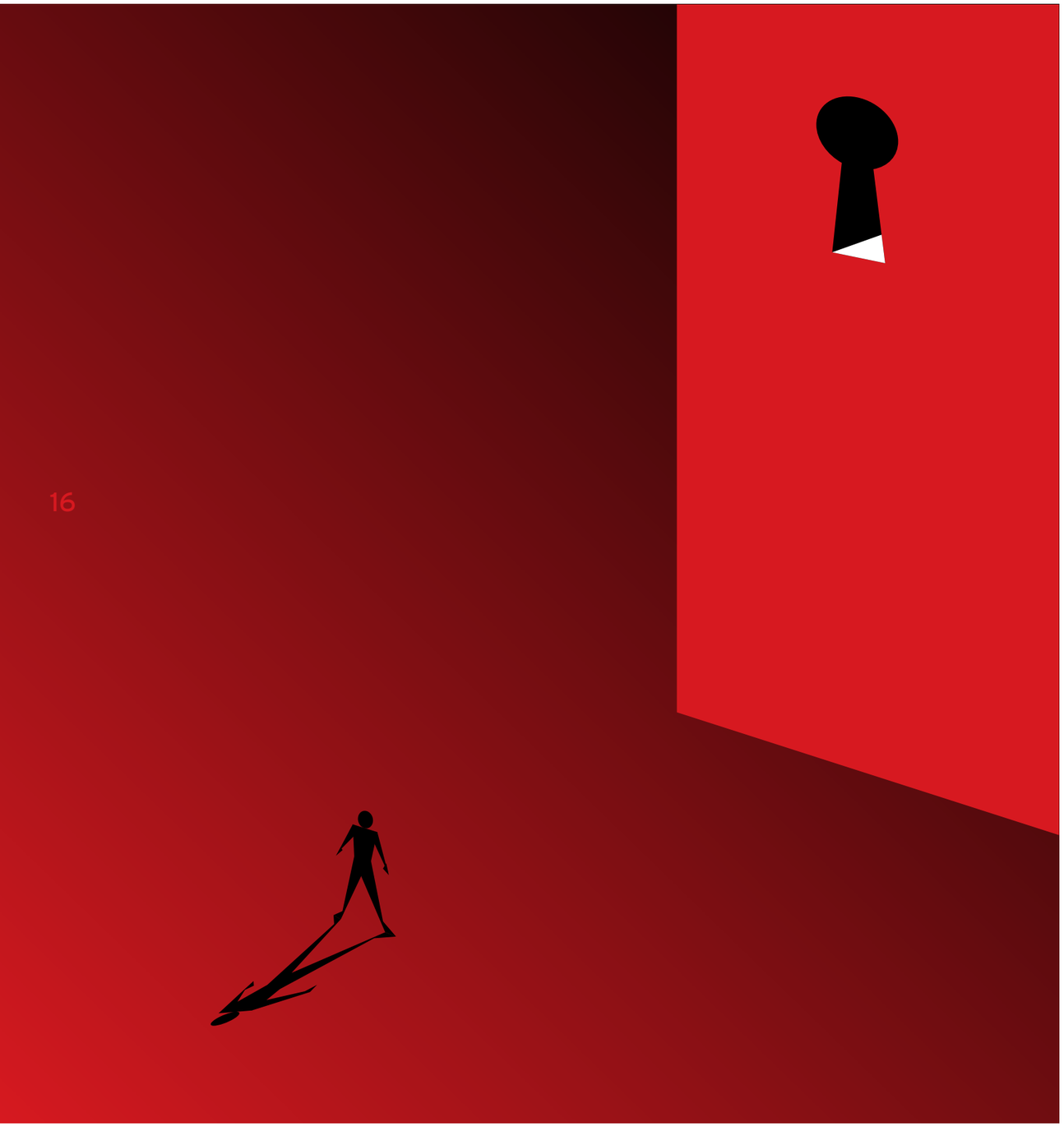
It may not surprise those familiar with the history of supply chain security to learn that the NHS usually considers information risk only for a limited number of suppliers, often based on contract size. This approach presents three problems –

1. **Other contractors that pose risks, such as legal firms, are often overlooked**
2. **It is not scalable for the NHS, which has too many contracts to consider them individually**
3. **Suppliers often share information with their own suppliers, who in turn share it with theirs and so on, increasing risk as visibility and control decrease**

The sector must work harder to get safety assurances in case risks to the confidentiality, integrity and availability of overarching systems are identified. Security challenges like these must be resolved for the NHS to safely operate – both individually and co-operatively with other NHS trusts – in networked, multi-vendor, cloud-based environments.

Trend Vision One can help the NHS manage risk across a vast supply chain:

- Provide a holistic view for risk management of suppliers and their respective networks, and align with regulatory and compliance requirements for supply chain security.
- Supporting zero-trust initiatives to minimise supply chain and identity-based risk such as credential phishing.
- Attack Surface Mapping and Cyber Asset Attack Surface Mapping enable scanning and mitigation of current, potential, and near-miss supply chain attacks, reducing the risk of cascading failures.



SECTION 4: SECURING COMPLEX ECOSYSTEMS

From pathology service providers to pharmacies and HVAC companies, the NHS manages a complex ecosystem of suppliers and partners. This makes it an attractive target for threat actors, constantly scanning for any security gaps they can exploit.

The complexity of these relationships can also be an enemy of effective security, as is the wide variety of maturity in cybersecurity posture across the supply chain. NHS CISO, Phil Huggins has described the state of security as **"15 to 20 years behind other sectors"**.

Challenges for NHS cyber teams:

- A large number of tools and disintegrated capabilities
- Limited expertise and experience
- Inability to determine what was detected or stopped
- Inability to use or access local and global intelligence
- Decreasing effectiveness and increasing costs of securing the environment
- Large volumes of low-fidelity alerts

Is your team operating on these *flawed* assumptions?

- All the security technology is behaving exactly how it's supposed to
- Vendors are making honest claims about software behaviour and capabilities
- Your security solution has been configured correctly
- The process works and nothing will break when it comes to IT change management
- Breaches and threats are not so serious and can be easily contained

Attacks and their implications

Although supply chain attacks account for a very small proportion of overall global attacks, they are often the most destructive. Supply chain incidents can have a critical knock-on impact on NHS services: cancelled appointments and life-saving operations, overworked staff and financial and reputational damage.

Synnovis attack

In July 2024, pathology services provider Synnovis was forced offline by a ransomware attack from the Qilin group, causing server issues for Guy's and St Thomas' and King's College Hospital NHS Foundation Trusts, and primary care services in South East London.

At least 1,608 elective procedures and 8,349 acute outpatient appointments were postponed across the two trusts, and an urgent appeal for blood donors was issued by the NHS. The group also leaked an estimated 400GB of sensitive internal information including patient names, dates of birth, NHS numbers and blood test results.

Advanced attack

In 2022, software supplier, Advanced was hit by the prolific LockBit group. Threat actors accessed a Citrix server by using legitimate third-party credentials to establish a remote desktop (RDP) session. Data from Staffplan and Caresys customers were exfiltrated, impacting care homes and services.

In the aftermath, seven of Advanced's health systems, including software used for patient check-ins, medical notes and the NHS 111 service, were taken offline. It took weeks for the services to get fully back online, with out-of-hours GP practices and others forced to revert to pen and paper.

WannaCry attack

In 2017, the WannaCry ransomware attack deployed encryption malware to over 200,000 computers in over 100 countries. Many NHS devices running a supported, but unpatched, operating system were vulnerable.

At least 34% of trusts in England were disrupted[8], leading to thousands of cancelled appointments and operations. WannaCry was the largest attack to affect the NHS, with an estimated cost of £20 million during the outbreak and an additional £72 million to restore data and systems[9].

8 https://www.gov.uk/government/publications/cyber-security-strategy-for-health-and-social-care-2023-to-2030/a-cyber-resilient-health-and-adult-social-care-system-in-england-cyber-security-strategy-to-2030

9 https://www.gov.uk/government/publications/cyber-security-strategy-for-health-and-social-care-2023-to-2030

The advantage of detecting anomalous behaviour

The NHS is rightly concerned about data being exposed due to preventable errors like misconfigured firewalls and databases. These types of attacks are as audacious as ever and, with the proliferation of endpoints due to complex supply chains, cloud technologies (SaaS), more remote workers and customers: the dangers are constantly increasing.

Aside from identifying, classifying, and controlling access to sensitive data in the cloud, the NHS also needs to find a means of detecting anomalies in the diverse way users work with data. To defend against insider threats, the NHS must continuously profile user and device behaviour to detect anomalous activity that could indicate stealthy attacks, compromised devices or user accounts.

Mitigating methods that use rich data from endpoints, networks and clouds combined with analytics allow the detection of attacks such as credential theft and tunnelled DNS, which are nearly impossible to identify, from standard threat logs or high-level network flow data.

Trend Zero Trust Secure Access (ZTSA) follows the principles of zero-trust networking. It can strengthen the overall security posture by enforcing strong access control permissions from multiple identity services across your NHS Trust.

Rather than granting access to the entire network, as a VPN does, ZTSA provides a gateway to specific applications and resources, restricting access to everything within the network that is not being employed. If valid user credentials are stolen, the level of access they will grant can be contained, effectively reducing the blast area of any attack.

Trend Vision One can help the NHS manage risk across its attack surface:

- Supporting zero-trust initiatives to minimise supply chain and identity-based risk such as credential phishing.
- Understanding user behaviour and enforcing authentication policies to reduce third-party risk.
- Correlating security events across identities, email, endpoints, files, commands, processes and other assets to stop identity and supply chain attacks in their tracks.

SECTION 5: SUPPORTING LEGACY IT

The landscape of the NHS is rapidly evolving, with technology playing an increasingly vital role in driving efficiency, improving patient outcomes, and enhancing connectivity across the system. However, navigating the complex terrain of healthcare technology adoption, integration, and scalability presents significant challenges for NHS Trusts.

Outdated IT is a clear and present danger to any organisation, but NHS Trusts can be left with no choice but to run legacy software due to compatibility issues and long operational technology lifespans on equipment like MRI scanners. It's not always possible to install security products on this type of equipment, due to supplier or manufacturer stipulations, so security teams must rely on network and endpoint security in the hope that they can prevent legacy systems from cyber infection.

50%

of NHS Trusts say that the complexity of legacy systems and lack of technical expertise are preventing them from making further digital improvements[10].

88%

of companies continue to be held back by legacy technologies, which is not only risky, but also expensive.

15%

annual budget increase can be attributed to the need to maintain outdated software.

Threat actors are deploying automated scanning tools to find weaknesses in legacy kit like MRI scanners. If the sector can't update the software, vulnerability exploitation could enable sabotage or data theft.

10 https://www.healthtechdigital.com/legacy-systems-and-lack-of-tech-expertise-and-leadership-pose-major-barriers-to-nhs-transformation/

The NHS is renowned for complex, legacy IT

Legacy systems are considerably more susceptible to security vulnerabilities and attacks because they are simply not designed to combat modern security threats. Threat actors are constantly evolving and developing new tactics, and legacy systems lack the required security features and updates to effectively protect an organisation.

The NHS utilises large quantities of legacy systems and a huge majority of the staff are overworked and suffering work fatigue, making them more susceptible to human error. In short, cyber adversaries aim for low-hanging fruit.

The NHS faces a relatively unusual situation of having many of its staff members working in multiple locations, but far too often the staff are not adequately trained across all the relevant locations. They have a lack of a complete view of their cybersecurity posture. Insufficient reviews of security, especially in the maintenance of legacy systems, give an incomplete understanding of who accesses systems and how they are secured.

The ultimate goal is holistic visibility

With this, the NHS can gain a full understanding of risk, the expected "normal" behaviour, and identify critical areas throughout its extended supply chain. The transformation of legacy technology means there needs to be a comprehensive shift in the NHS's approach to address elements like cybersecurity, communication and data collection.

A comprehensive cybersecurity solution provides protection against known and unknown attacks by combining host intrusion prevention, desktop firewall and peripheral device control. That's essential for eliminating exposures from home computers, kiosks and guest laptops. Such a solution creates a virtual desktop environment offering a protected network session that includes the ability to detect and kill malicious code such as keystroke loggers from capturing username and password information and screen scrapers from spying on user activity.

Trend Vision One is specifically tailored to secure legacy NHS systems:

- Continually assesses security posture, including vulnerabilities and misconfigurations, suggesting remedial measures and automating key steps.
- Works across OT, IT and mobile devices to lock down security risk, wherever legacy technology exists.
- Empowers security analysts with AI capabilities to stop and contain threats exploiting legacy technology even faster.

SECTION 6: RESOURCE OPTIMISATION

Don't settle for 'good enough' security

Continued cost pressures mean security investments rely on being able to create an outstanding business case. The NHS is also short of IT skills and security professionals, competing against deeper-pocketed rivals for an increasingly limited talent pool. Security tools can only go so far to mitigate the shortfall and point solutions can compound the challenge by creating more management overheads and security alerts that overwhelm SOC analysts.

Cybersecurity staff shortage

The scarcity of cyber resources exacerbates the industry's recruitment crisis. Cybersecurity necessitates advanced tools, training modules and cutting-edge technologies to combat evolving threats effectively.

The difficulty of point products

While it is possible to right-size network-based protection according to its throughput, the amount of decryption required, and so on; this is not possible for endpoint protection. The traditional approach of deploying multiple single-purpose point products from different vendors was always destined to fail.

The lack of effective security and significant waste of endpoint resources due to software bloat has opened the door to a new generation of endpoint security solutions.

With endpoint security, the NHS needs to be confident in the mitigation capabilities of their chosen technologies. Selecting the right solution for network and endpoint security should not be taken lightly as endpoint infections can have a direct, detrimental impact on operational uptime.

Trend Vision One Economic Overview – the Enterprise Strategy Group (ESG)[11]

ESG focused on the quantitative and qualitative benefits organisations can expect by using Trend Vision One when compared to fragmented cybersecurity strategies to improve security posture and protect, detect and respond to security threats and events.

Economic analysis revealed that Trend Vision One provides its customers with significant savings and benefits in categories including the following:

- **Reduced risk**
  ESG found that Trend Vision One customers had a lower likelihood of ransomware and breach events as well as reduced impact of actual events.
- **Improved detection and response**
  Customers reported a significant improvement in the ability to detect issues that create the highest level of risk and remediate those issues in less time with Trend Vision One.
- **Improved operational efficiency**
  Trend Vision One customers found that their overall security and incident response spend was lower when compared with their previous solutions.

With Trend Vision One, customers are able to proactively secure entire classes of digital assets – including devices, servers, domain and IP addresses, cloud assets and APIs – that have been left under-protected, or even unprotected, in the past.

11 ESG report on the NHS: https://www.trendmicro.com/explore/en_gb_esg_report/2523-v1-en-3pa?xs=570470#page=1

Trend Vision One can help to optimise your security resources:

Make use of AI to upskill analysts, automate tasks and prioritise alerts, and unlock financial advantages, such as:

70%
Reduction in cybersecurity costs

£1.3m
Average cost reduction of data breach

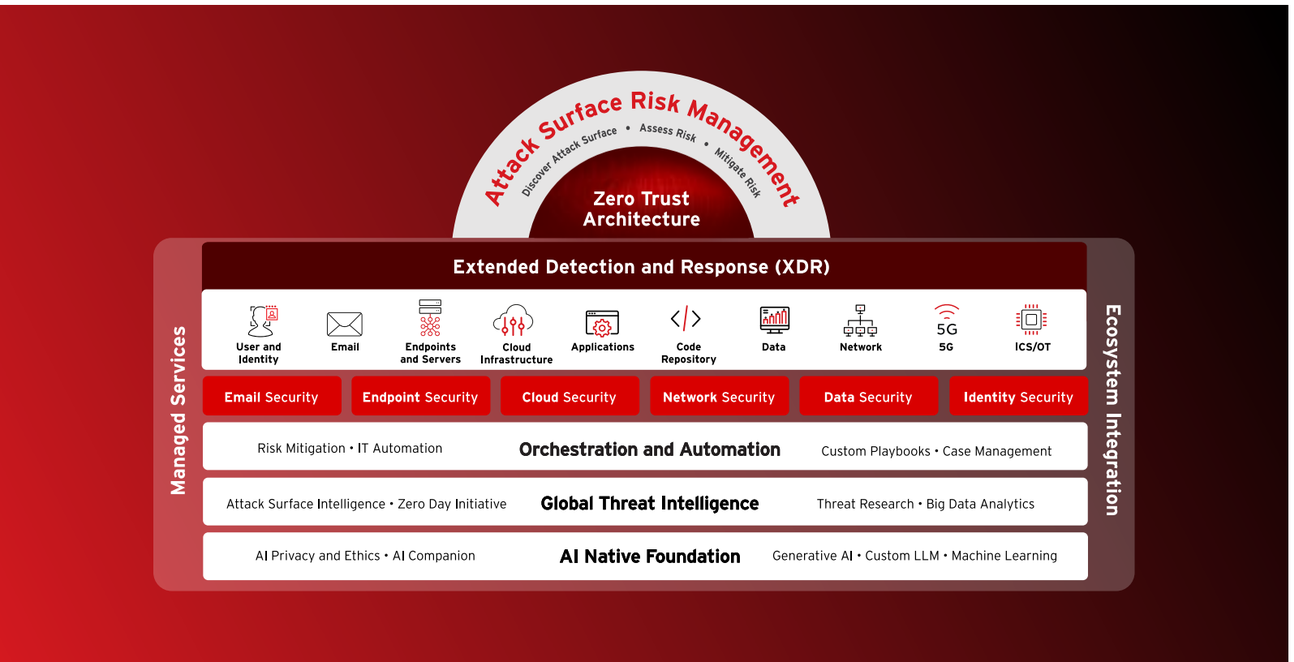
79%
Decrease security spend

SECTION 7: SECURING THE NHS – WHY TREND IS A TRUSTED CYBERSECURITY PARTNER

Get the most complete attack surface coverage

Trend Vision One provides comprehensive visibility and proactive risk management, simplifying compliance and reducing the need for multiple tools. This consolidation not only cuts costs but also streamlines workflows, allowing for faster threat detection and response.

The platform's virtual patching capability ensures protection of critical assets from both known and unknown threats, supporting business continuity and safeguarding patient data. It can help you transform cybersecurity from a cost centre into a strategic enabler, ensuring robust protection while enhancing operational efficiency.



Advantages of Trend Vision One

Integrates Attack Surface Risk Management (ASRM) and extended detection and response (XDR) into a unified cloud-native platform

While serving cloud, hybrid and on-premises environments, Vision One combines ASRM and XDR in a single console to effectively manage cyber risk across your NHS Trust. It provides NHS Trust cyber teams with powerful risk insights, earlier threat detection and automated risk and threat response options. Cyber teams can utilise the platform's predictive machine learning and advanced security analytics for a broader perspective and advanced context.

Combines an expansive protection portfolio, industry-leading global threat intelligence, and a broad ecosystem of API-driven, third-party features

Security and SOC analysts, threat hunters, and senior security leaders across an NHS Trust are given the tools to contextualise risk and reduce the likelihood of attacks, while reducing false positives and noise within the environment continuously and proactively. This integrated solution provides improved visibility that leads to quicker detection, fewer blind spots, and greater potential for total remediation.

Delivers the broadest native XDR sensor coverage in the cybersecurity market

The platform's native-first, hybrid approach to XDR and ASRM benefits NHS security teams by delivering richer activity telemetry – not just detection data – across security layers with full context and understanding. This results in earlier, more precise risk and threat detection and more efficient investigation.

Improves visibility, insight, and total security posture

In the 'Trend Vision One Economic Overview Report'[12] by ESG, one of the top benefits customers mentioned was the improved visibility of their entire security posture and their new-found ability to proactively manage risk. Customer interviews included a consistent sentiment: **"Before Trend Vision One, we just didn't know"**.

Provides a consolidated list of opportunities to improve your security posture from a operations dashboard

In the same report, another capability that was specifically called out as a game-changer was the operations dashboard. This feature provides a comprehensive view of the security status and risks in an organisation's devices and accounts, with the ability to dig into each area to examine more specific details.

12 ESG report on the NHS: https://www.trendmicro.com/explore/en_gb_esg_report/2523-v1-en-3pa?xs=570470#page=1

Why Trend as Partner for the NHS

"Trend Micro is a good fit for customers who want a consistently strong endpoint protection platform that can support evolving to XDR" [13]

- Trend Micro a Leader The Forrester Wave™

FORRESTER®

"Ranked #1 in IDC's Worldwide Hybrid Cloud Workload Security Market Shares report" [14]

- IDC Worldwide Security Market Shares

IDC

"Trend Micro ranked #1 in the production category for ensuring early attack prevention" [15]

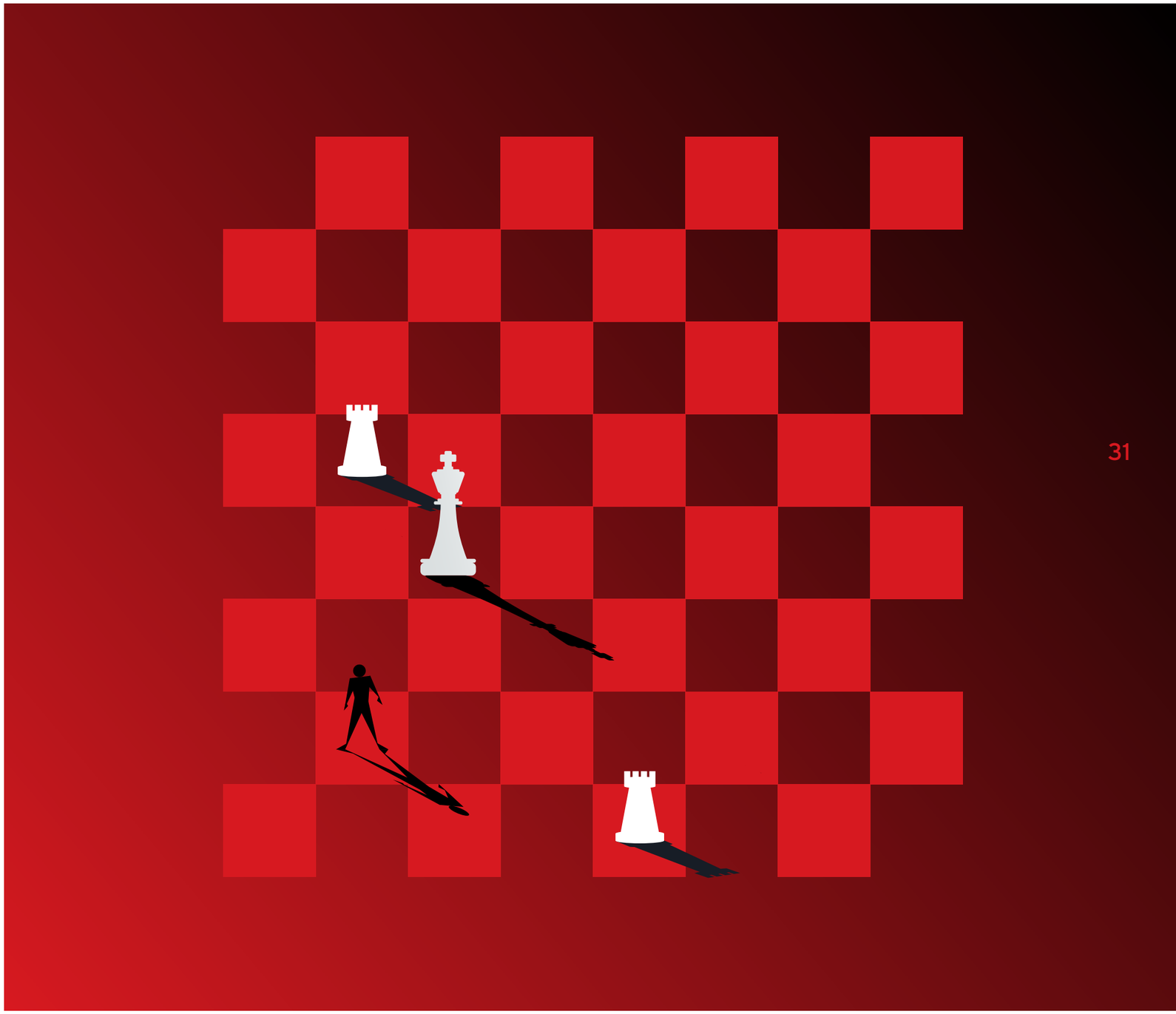
- MITRE Engenuity Att&CK Evaluations: Quick Guide Guide

MITRE

"Trend has been named and recognized by Gartner in both Endpoint (EPP/EDR) and Network (NDR) security" [16]

- Gartner: Trend Micro a Leader in the Endpoint Protection Platform Magic Quadrant

Gartner



13 https://www.trendmicro.com/explore/forrester-wave-asm

14 https://statics.teams.cdn.office.net/evergreen-assets/safelinks/1/atp-safelinks.html

15 https://www.trendmicro.com/explore/industry-recognition-eu/01436-v1-en-rpt?xs=391652

16 https://resources.trendmicro.com/Gartner-MQ-EPP-2024.html

TREND MICRO™

Harder for hackers.
Simpler for you.

STAY AHEAD OF YOUR CYBER RISK SPEAK WITH US TODAY:

Book a 15-minute discovery call with one of our trusted NHS cybersecurity advisors

Speak with us >

Start your complimentary 30-day trial

Activate here >