Harder for hackers.
Simpler for you.

TREND MICRO™

BUILDING CYBER RESILIENCE FOR CENTRAL GOVERNMENT

Learn how Trend Micro Vision One™ can help mitigate risks and secure your complex, digital landscape

Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information.

Fueled by 35 years of security expertise, global threat research, and continuous innovation, Trend's AI-powered cybersecurity platform protects hundreds of thousands of organizations and millions of individuals across clouds, networks, devices, and endpoints.

With 7,000 employees across 70 countries and the world's most advanced global threat research and intelligence, Trend enables organizations to simplify and secure their connected world. TrendMicro.com

Harder for hackers.
Simpler for you.

CONTENTS

Section 1: Introduction 4
Section 2: Handling sensitive data 8
Section 3: Streamlining compliance and bridging skills gaps 12
Section 4: Overcoming budgetary challenges 16
Section 5: Addressing evolving threats 20
Section 6: Securing central government 24

SECTION 1: INTRODUCTION

Assessing the threat landscape

Central government plays a critical role in safeguarding national infrastructure and data sovereignty, both of which are vital to national security. As one of the most high-profile targets for threat actors, it is confronted by an increasingly complex and dangerous cyber threat landscape. So it should come as no surprise that administrations like yours are "routinely and relentlessly targeted" by a range of malicious actors, including hostile states, criminals, and hacktivists, according to the 2022-2030 Government Cyber Security Strategy.

The scale of the threat is significant. In the 2021-2022 period, the NCSC managed 63 nationally significant incidents. In 2024, the NCSC has already responded to 50% more nationally significant incidents compared to last year, alongside a threefold increase in severe incidents[1]. This underscores the critical role government departments play in maintaining national infrastructure and safeguarding sensitive data. As Dr. Richard Horne, CEO of the NCSC highlighted, the swift growth of cyber capabilities that was once limited to nation-states and well-funded groups, has significantly expanded the scope of potential threats.

The strategic importance of central government extends beyond the protection of data; it's about securing critical national infrastructure and ensuring the continuous operation of vital services. Infiltration into these systems could disrupt essential services and compromise public trust.

The challenge will always be finding a cost-effective way to mitigate this risk and fulfil your compliance obligations, without slowing down vital digital and cloud transformation projects. As departments continue to digitalise and adopt cloud technologies, the attack surface expands, creating more entry points for cybercriminals.

This is where Network Detection and Response (NDR) comes into play, offering early detection, rapid incident response, and proactive threat hunting to safeguard critical infrastructure.

For central government, effective cybersecurity is not only about protecting data; it's about maintaining national security, ensuring the continuity of critical services, and reinforcing public confidence.

1 https://www.ncsc.gov.uk/news/ncsc-warns-widening-gap-between-cyber-threats-and-defence-capabilities

Attacks and their implications

Malicious actors are increasingly targeting central government due to the critical data it manages. To maintain security, you must have systems and operations that are highly effective, intelligent and easy to manage.

WannaCry attack

In 2017, the WannaCry ransomware attack demonstrated the potential for cyber incidents to disrupt critical public services. Encryption malware was deployed 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[1], leading to thousands of cancelled appointments and operations. The attack impacted approximately 30% of NHS Trusts and lasted 4 days before the ransomware's 'kill switch' was identified, allowing the system to start coming back online. 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[2].

UK Electoral Commission incident

More recently, in a 2023 cyber incident that has since been attributed to a China state-affiliated actor, the UK Electoral Commission suffered a breach that exposed the personal information of 40 million voters. This highlighted the ongoing vulnerabilities in government systems, and resulted in a reprimand from the Information Commissioner's Office.

The attackers were able to access full copies of the electoral registers. These registers included the name and address of anyone in the UK who was registered to vote between 2014 and 2022. The commission's email system was also accessible during the attack.

The central government must prioritise advanced security protocols to safeguard national infrastructure, ensure citizen trust, and prevent further reputational and regulatory damage.

1 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

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

Central government's security goals

The Government Cyber Security Strategy sets an ambitious goal: to have all government organisations resilient to known vulnerabilities and attack methods by 2030[3]. To achieve this, the strategy emphasises the need for a holistic governmental approach, including:

- Adopting the NCSC's Cyber Assessment Framework (CAF) across all government organisations.
- Implementing a 'defend as one' approach to improve coordination and information sharing.
- Investing in skills and capabilities to address the cybersecurity skills gap in the public sector.

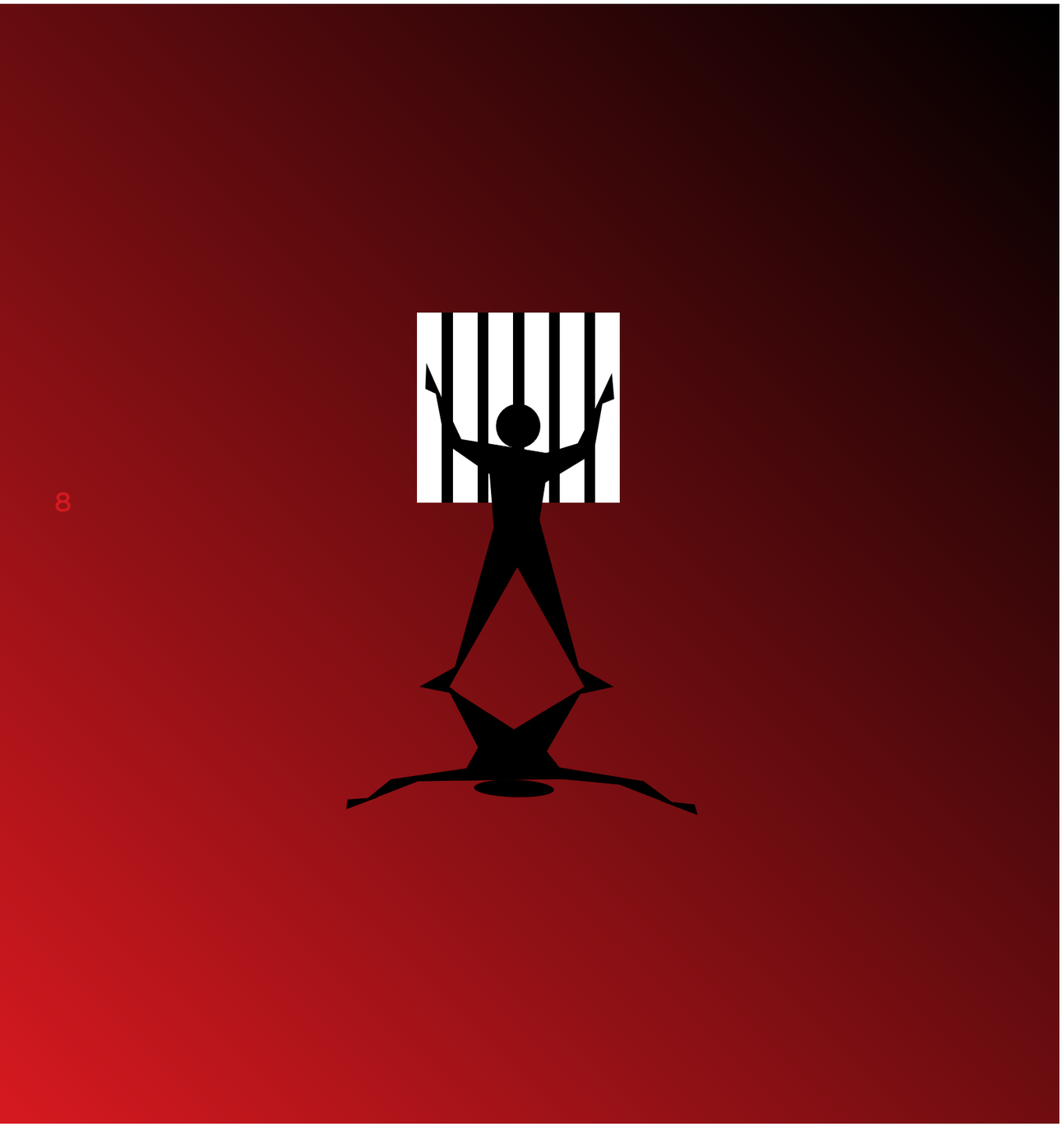
How does Trend Micro meet the needs of central government?

We meet organisations at the current stage of their cloud journey, whether they are fully in the cloud, operate in a hybrid environment, or remain on-premises to accommodate various infrastructure setups.

Discover how Trend's advanced cybersecurity solutions tackle the common challenges faced by your sector. This document outlines the key threats, their impact on your network, and how our integrated approach can cover a complex system environment, both on-prem and cloud infrastructure, ensuring sovereignty and compliance.

- **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:** Security that adapts to evolving needs across a vast array of contracts and suppliers, focused on scalability and managing numerous relationships efficiently.
- **Compliance and regulatory support:** Ready to support compliance with regulations such as GDPR, 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.

3 https://assets.publishing.service.gov.uk/media/61f0169de90e070375c230a8/government-cyber-security-strategy.pdf



SECTION 2: HANDLING SENSITIVE DATA

Navigating challenges in central government and national security

Central government must balance its cybersecurity imperatives against other priorities, including digital transformation, budget constraints and the need to deliver efficient public services. This balancing act represents one of the key challenges in government cybersecurity for the coming years.

As a long-time central government cybersecurity partner, Trend understands you may be struggling to manage risk across an attack surface that grows with each new cloud investment or remote-working endpoint. This attack surface also remains highly exposed due to elements of legacy IT.

We know that the point solutions you have bought over time often don't talk to each other and can leave dangerous visibility gaps, whilst also increasing the administrative workload for stretched teams. Finally, we know that efforts to improve threat detection and response are often stymied when analysts are overwhelmed with alerts.

For a government agency with 10,001+ employees, we provide comprehensive security solutions through Trend Vision One to help them identify and neutralise malicious activities on their network. This government agency, subject to state oversight, relies on Trend Vision One to provide critical insights that enable their SOC to swiftly detect and respond to potential threats. By surfacing key vulnerabilities and highlighting emerging risks, Trend Vision One enables the agency to take rapid action, preventing minor issues from escalating into more widespread problems.

"Trend Vision One has saved us ten percent of our time. It has helped us even more than that because the few times we have had a threat, it has stopped it in its tracks. This has prevented the threat from spreading and compromising multiple machines. Without Trend Vision One, we would have had to investigate the threat, which would have taken time and resources."

Matthew Guzzi, Information Systems Administrator at a government agency with 10,001 employees

Cloud migration and management

The UK government has set ambitious targets for cloud migration, and the transformation is happening at pace. Cloud adoption offers opportunities for improved efficiency, scalability, and cost-effectiveness. However, it also requires a shift in cybersecurity approach. Government departments must:

- Develop cloud-specific security strategies and policies
- Implement robust identity and access management systems
- Ensure proper data encryption and protection measures
- Continuously monitor and audit cloud environments for potential threats

One of the primary challenges is ensuring security during the migration process. According to the National Cyber Security Centre (NCSC), organisations often underestimate the complexity of cloud migrations, leading to potential vulnerabilities. Risk must be properly managed across both cloud and on-prem environments without added cost or security gaps. Departments need flexible and scalable security solutions to mitigate risks effectively while transitioning to cloud-based systems. You must also ensure you have adequate skills, processes, and controls available to manage cloud-related risk.

That's what Trend Vision One is designed to achieve. Our unified platform for attack surface risk management (ASRM) and extended detection and response (XDR) contains and mitigates the risks your administration faces every second of the day across its entire attack surface, while reducing costs, optimising productivity and preserving investment in digital transformation.

Trend Vision One helps to protect sensitive data, simply and reliably:

- 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: STREAMLINING COMPLIANCE AND BRIDGING SKILLS GAPS

Streamlining compliance and bridging skills gaps are two interconnected challenges facing the UK central government in its cybersecurity efforts. The complex regulatory landscape, coupled with a persistent shortage of cybersecurity professionals, presents significant hurdles for government departments.

Ensuring regulatory compliance

One thing all central government departments have in common is a patchwork of regulations, standards and codes of practice governing how they operate. Your challenge is to find a trusted partner that understands these exacting requirements, and delivers solutions designed to take the pain out of compliance.

Compliance with various cybersecurity regulations and standards is a major challenge. Government departments must adhere to a range of requirements, including the Minimum Cyber Security Standard, the NCSC's Cyber Assessment Framework (CAF), and data protection regulations like GDPR.

Navigating this complex regulatory landscape without guidance can be time-consuming and resource-intensive. It can also delay security responses and impact overall organisational agility and strategic objectives.

Mitigating the skills gap

The skills gap in cybersecurity further complicates compliance efforts. The UK, like most countries around the world, is suffering from a major shortage in skilled cybersecurity professionals.

According to the UK Government's Cyber Security Skills in the UK Labour Market 2023 report, 50% of all UK businesses have a basic cybersecurity skills gap, with little improvement from the previous year. In the public sector, this skills shortage is often more acute due to competition from the private sector for talent.

The report also found that 33% of organisations have an advanced cybersecurity skills gap, and there's an estimated shortfall of 11,200 people to meet the demand of the cyber workforce. This acute cybersecurity skills shortage not only makes it difficult for government departments to implement and maintain robust cybersecurity measures but also exacerbates the challenge of securing sensitive data and navigating complex compliance requirements. It further impacts the ability to manage both legacy systems and modern cloud infrastructures effectively.

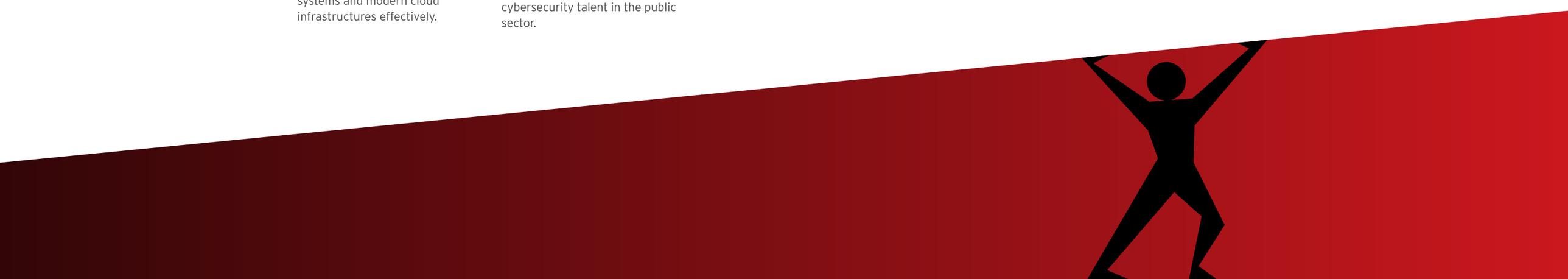
For central government, these challenges have several implications –

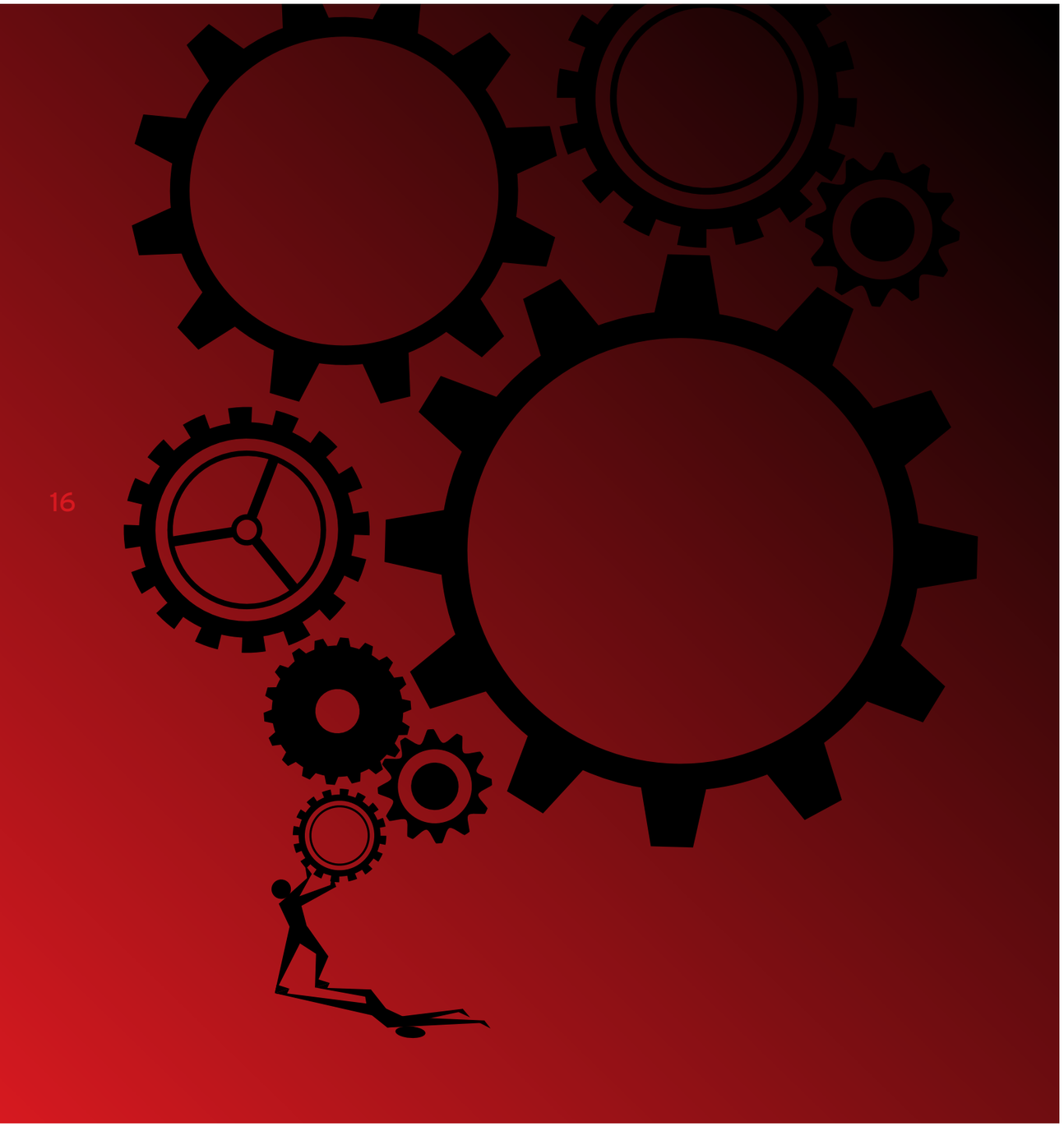
- **Increased vulnerability:** The skills gap can lead to security vulnerabilities if departments lack the expertise to implement and manage complex security systems.
- **Compliance risks:** Without adequate skills and resources, departments may struggle to meet regulatory requirements, potentially leading to non-compliance and associated risks.
- **Inefficient resource allocation:** The complexity of compliance and the skills shortage can lead to inefficient use of limited resources, as departments struggle to balance security needs with other priorities.

Looking ahead, streamlining compliance processes and addressing the skills gap will be crucial for improving the overall cybersecurity posture of central government. This may involve leveraging technologies like automation and AI to enhance compliance processes, as well as developing innovative approaches to attract and retain cybersecurity talent in the public sector.

Trend Vision One provides comprehensive security for new regulatory requirements and skills shortages:

- **Attack Surface Risk Management (ASRM)** provides a library of ready-made workflows to improve security teams' productivity and speed when completing critical tasks related to security and compliance – this is especially useful considering the cybersecurity skills shortage
- **Vision One's Generative AI cybersecurity assistant (Vision One Companion)** provides enhanced capabilities, accessibility and efficiency. It helps cybersecurity professionals respond to complex scenarios more swiftly, mitigating the skills shortage and improving outcomes
- **Zero Trust** principles are embedded in Vision One, which provides confidence when centralising policy decisions from a single console





SECTION 4: OVERCOMING BUDGETARY CHALLENGES

Central government faces significant challenges due to tight budgets, which can lead to difficult choices and risky compromises. Investment in technology is of paramount importance to remain effective, efficient and secure. However, with constrained financial resources, identifying the areas that require the most urgent allocation of limited public funds will always be a process that is fraught with complexity. The struggle to balance securing critical services while achieving cloud migration goals intensifies under these budgetary constraints.

The Government Cyber Security Strategy 2022-2030 has outlined ambitious goals for improving cybersecurity across government, but it also acknowledges the need for substantial investment to achieve these objectives[4].

The Cyber Security and Resilience Bill, announced in the July 2024 King's Speech, aims to strengthen the UK's cyber defences and protect essential public services. It responds to the growing threat of cyber-attacks on critical infrastructure, with recent incidents affecting the NHS and Ministry of Defence highlighting vulnerabilities. The bill will apply UK-wide and is scheduled for introduction to Parliament in 2025.

For the central government sector, these budgetary challenges have several implications:

- **Prioritisation dilemmas:** Departments must make difficult decisions about where to allocate limited cybersecurity budgets, potentially leaving some areas vulnerable.
- **Delayed modernisation:** Budget constraints can slow down the adoption of new, more secure technologies, leaving departments reliant on outdated and potentially vulnerable systems.
- **Skills retention challenges:** Limited budgets can make it difficult for government departments to compete with the private sector for top cybersecurity talent.

4 https://assets.publishing.service.gov.uk/media/61f0169de90e070375c230a8/government-cyber-security-strategy.pdf

To address these challenges, the Government Cyber Security Strategy emphasises several tactics:

- **Risk-based approach:** Encouraging departments to prioritise cybersecurity investments based on a thorough assessment of risks and potential impacts.
- **Shared services:** Promoting the use of shared cybersecurity services across government to achieve economies of scale and maximise the impact of limited resources.
- **Public-private partnerships:** Exploring opportunities to collaborate with the private sector to access additional resources and expertise.

The strategy also highlights the need for a whole-of-government approach to cybersecurity investment, recognising that the interconnected nature of government systems means that vulnerabilities in one department can potentially impact others.

Looking ahead, overcoming budgetary challenges will require innovative approaches to resource allocation and a clear articulation of the return on investment for cybersecurity spending. This may involve developing more sophisticated models for quantifying cyber risk and the potential impacts of cyber incidents, helping to justify necessary investments.

There is also a growing recognition that cybersecurity investment should be viewed not just as a cost, but as an enabler of digital transformation and improved public services. By framing cybersecurity in this way, government departments may be better positioned to secure the necessary resources to build robust cyber defences.

- Strengthening national security with Trend Vision One, The Enterprise Strategy Group's economic validation of Trend Vision One demonstrated a **70% reduction in cybersecurity cost**, combined with a **17%** r**eduction in data breach risk** and **20% reduction in employee turnover**[5].
- It further demonstrated a reduction of alerts per day from **1,000 to 4** and reduced the **average cost of a data breach by £1.3m** while resulting in **$2.43m average cost savings** from improvement in customer churn.

There are further uncalculated benefits that will have accrued from reducing the training and management workload for stretched in-house IT teams.

Trend Vision One can help you extract greater functional value and cost-efficiency from your cybersecurity:

70%

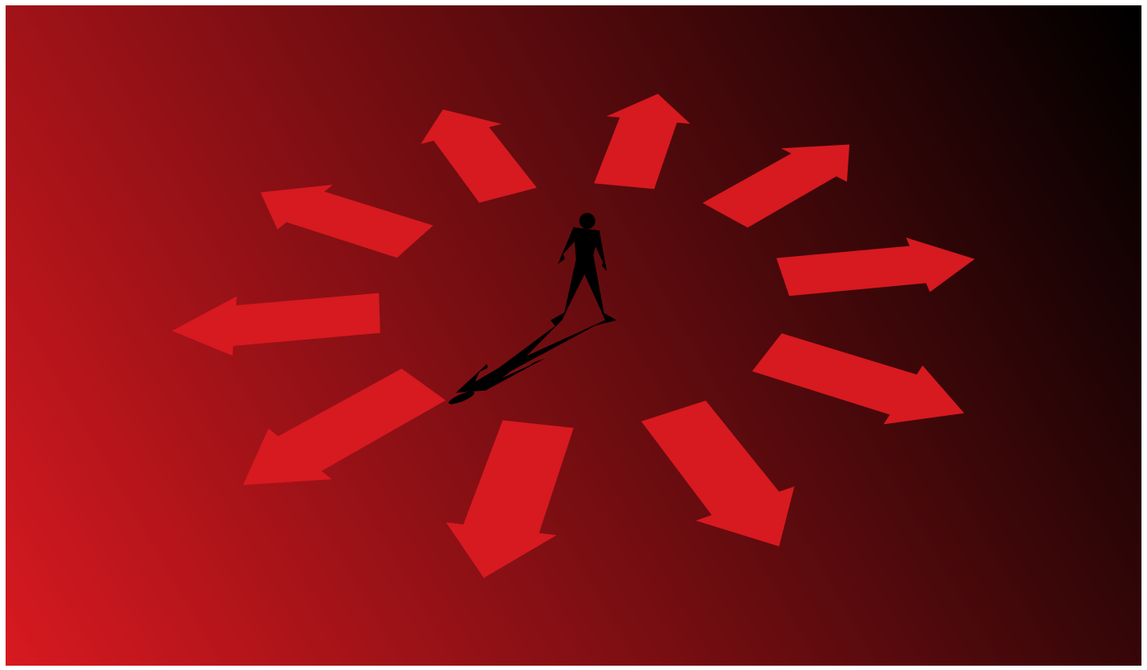
Reduction in cyber security costs

£1.3m

Average cost reduction of data breach

79%

Decrease security spend



5 https://www.trendmicro.com/explore/centgov/2523-v1-en-3pa

SECTION 5: ADDRESSING EVOLVING THREATS

Evolving your defences

The threat landscape is constantly changing, with new attack vectors, techniques, and actors emerging regularly. This dynamic environment requires government departments to be agile, proactive and constantly vigilant.

As referenced in the Government Cyber Security Strategy, government organisations are "routinely and relentlessly targeted" by a range of malicious actors, including hostile states, criminals and hacktivists. The strategy notes that the frequency and sophistication of these attacks are increasing, with cyber criminals continually adapting their methods to exploit new vulnerabilities.

For central government, meeting evolving threats has several implications:

- **Continuous adaptation:** Departments must constantly update their cybersecurity strategies and technologies to keep pace with new threats.
- **Enhanced threat intelligence:** There's a growing need for real-time threat intelligence and information sharing across government departments.
- **Advanced defence capabilities:** As threats become more sophisticated, government departments need to develop more advanced defence capabilities, including the use of AI and machine learning for threat detection and response.

The Government Cyber Security Strategy has outlined several approaches to address these challenges:

- **Adopting a 'defend as one' approach:** This involves improving coordination and information sharing across government departments to create a more unified defence against cyber threats.
- **Implementing the NCSC's Active Cyber Defence program:** This program aims to tackle a significant proportion of the cyber attacks that hit the UK.
- **Developing advanced incident response capabilities:** This includes establishing the Government Cyber Coordination Centre (GCCC) to coordinate operational responses to significant incidents.

The strategy also emphasises the importance of partnerships with the private sector and international allies in addressing evolving threats. This collaborative approach recognises that many cyber threats are global in nature and require coordinated global responses.

Meeting evolving threats will require a combination of technological innovation, strategic planning and workforce development. Government departments will need to invest in advanced technologies like AI-powered threat detection systems, while also developing the skills and capabilities of their cybersecurity workforce to effectively use these tools.

For some, it is tempting to turn to pre-bundled and generic solutions, which are seen as providing security that is "good enough". However, this can prove to be a costly and risky mentality, especially for networks so sensitive as those belonging to central government – it's an inadvisable gamble to take, knowing how much of a prized target your data represents, and it's a false economy, as a breach of sensitive data resulting from inadequate cybersecurity can have far greater reputational and financial costs, along with significant impacts on citizens.

Trend Vision One can help you stay ahead of the always evolving threat landscape:

- Tailored for your specific on-prem and hybrid cloud environments, ensuring **optimised protection, detection and response** with no visibility gaps, whatever your IT set-up.
- **Risk Insights** provide real-time understanding of your security posture. Remediation suggestions and automations fix vulnerabilities, misconfigurations and other issues.
- **Predictive machine learning and advanced security analytics** reduce false positives and empower security and SOC analysts to prioritise XDR alerts and quickly respond to risk.

SECTION 6: SECURING CENTRAL GOVERNMENT

Why Trend Micro is a trusted cybersecurity partner

Evolving threats require an evolving cybersecurity solution

The cybersecurity landscape for the UK's central government is complex and challenging, but there are clear paths forward for improvement and resilience.

Challenges facing central government

- **A constantly evolving threat landscape**: Government organisations face relentless attacks from diverse malicious actors, requiring continuous adaption and vigilance.
- **Complexities of cloud migration and management:** Balancing the benefits of cloud adoption with the imperative for robust security measures can pose a significant challenge[6].
- **Addressing the cybersecurity skills gap**: With half of UK businesses experiencing a basic cybersecurity skills shortage, bridging this gap is a critical priority.
- **Navigating budgetary constraints:** Resource allocation for cybersecurity initiatives demands careful prioritisation amidst tight financial limitations.
- **Streamlining compliance in a complex regulatory environment:** Simplifying compliance processes while adhering to stringent regulations is a pressing need for organisations.

Despite these challenges, central government has made notable progress. The establishment of the National Cyber Security Centre (NCSC), the creation of the Government Security Group, and the introduction of the Minimum Cyber Security Standards (MCSS) have all contributed to improving the government's cybersecurity posture.

6 https://www.infosecurity-magazine.com/news/cybersecurity-skills-gap-stagnant/

The Government Cyber Security Strategy's key initiatives for improving cybersecurity

- Adopt the NCSC's Cyber Assessment Framework (CAF) across all government organisations, providing a common language and approach to cybersecurity.
- Implement a 'defend as one' approach to improve coordination and information sharing across departments.
- Invest in skills development to address the cybersecurity talent shortage in the public sector.
- Leverage advanced technologies, including AI and machine learning, for threat detection and response.
- Develop stronger partnerships with the private sector and international allies to address global cyber threats.

Invest in 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.

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

Industry accolades for Trend Micro

"Trend Micro is a good fit for customers who want a consistently strong endpoint protection platform that can support evolving to XDR"[7]

- Trend Micro a Leader The Forrester Wave™:

Attack Surface Management Solutions, Q3 2024

Trend Micro a Leader The Forrester Wave™:
Attack Surface Management Solutions, Q3 2024

FORRESTER®

"Ranked #1 in IDC's Worldwide Hybrid Cloud Workload Security Market Shares report"[8]

- IDC Worldwide Security Market Shares

IDC

"Trend Micro ranked #1 in the production category for ensuring early attack prevention"[9]

- 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"[10]

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

Gartner

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

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

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

10 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 Central Government cyber security advisors

Speak with us >

Start your complimentary 30-day trial

Activate here >