Harder for hackers.
Simpler for you.

# BUILDING CYBER RESILIENCE FOR LOCAL GOVERNMENT

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

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

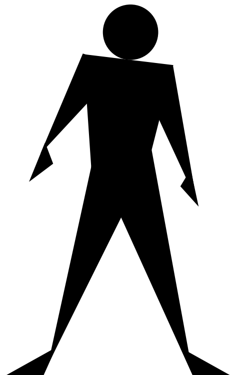
Fueled by 35 years of security expertise, global threat research, and continuous innovation, Trend's AI-powered cybersecurity platform protects hundreds of thousands of organizations and millions of individuals across clouds, networks, devices, and endpoints.

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 | 9 |
| Section 3: | Regulatory compliance | 12 |
| Section 4: | Overcoming political and financial blockers | 17 |
| Section 5: | Resource optimisation | 20 |
| Section 6: | Securing Local Government | 25 |



# SECTION 1: INTRODUCTION

For local government in the UK, cybersecurity matters more than ever.  The sector is responsible for handling vast amounts of sensitive data, including personal information about residents, financial records, and details related to public services, yet cybersecurity resources are often limited.

Protecting these networks from cyber-attacks is critical not only to prevent significant financial and reputational costs but also to safeguard the personal data of citizens. Cybersecurity breaches can compromise this sensitive information, leading to identity theft, fraud, and loss of public trust. Additionally, breaches can cause network downtime and cascading operational disruptions, directly affecting public services that citizens rely on.

For local authorities, the challenge of cybersecurity is compounded by constrained budgets, legacy systems and a shortage of cybersecurity skills, making it difficult to stay ahead of the constantly evolving threat landscape.  Many authorities find themselves wrestling with the need to modernise their digital infrastructure while simultaneously guarding against these threats, all while managing highly sensitive personal data and preserving public trust.

To address these challenges, local government must prioritise cybersecurity, invest in modern technologies, and implement comprehensive strategies to protect their digital assets and maintain public trust.

- **The public sector is a prime target**
  - Councils in the UK are dealing with thousands of attempted cyber-attacks every day, with 2.3 million attacks being detected so far this year.[1]
- **The number of cyber attacks is growing**
  - In 2022, UK councils faced over 10,000 cyber attacks daily, with phishing being the most common attack vector.[2]
  - Cyber attacks on local authorities increased by 24% between 2022 and 2023, with personal data breaches skyrocketing by 58% in the same period.[3]
- **Data breaches are often costly**
  - A ransomware attack on Hackney Council in 2020 resulted in £12 million worth of damages being paid.[4]
  - Over a period of 3 years, Kent City Council was targeted by cyber attacks 13 times, resulting in 2,452 personal details being compromised and over £16,000 paid in compensation for data breaches.[5]

[1] Cyber resilience in the public sector: lessons for UK Councils (techinformed.com)

[2] Cyber resilience in the public sector: lessons for UK Councils (techinformed.com)

[3] https://securityjournaluk.com/local-authorities-improve-cyber-resilience/

[4] https://securityjournaluk.com/local-authorities-improve-cyber-resilience/

[5] https://securityjournaluk.com/local-authorities-improve-cyber-resilience/

## Why are local councils so often the focus of cyber attacks?

### Sensitive data

Local councils handle a vast amount of sensitive information, ranging from personal details of residents to financial records and public service data. This makes them an attractive target for hackers seeking to exploit personal information.

### Limited resources

Local councils often operate with limited resources. Constrained budgets and smaller IT teams make it more difficult for councils to implement effective cybersecurity measures.

### Outdated infrastructure

Many local councils rely on outdated IT infrastructure and legacy systems, which may not have received regular updates or patches. Legacy technology is more susceptible to vulnerabilities.

### Insufficient training

Human error plays a large role in vulnerability to cyber attacks. Phishing and social engineering tactics exploit unaware staff members in order to breach private networks and data.

### Decentralised operations

Local councils are spread across departments and locations. This fragmentation makes it harder to implement a unified cybersecurity strategy that covers all network endpoints.

### Political motivation

Local councils play a crucial role in the delivery of public services. Disrupting their operations can have significant political implications, which may make them an attractive target.

## Assessing the threat landscape

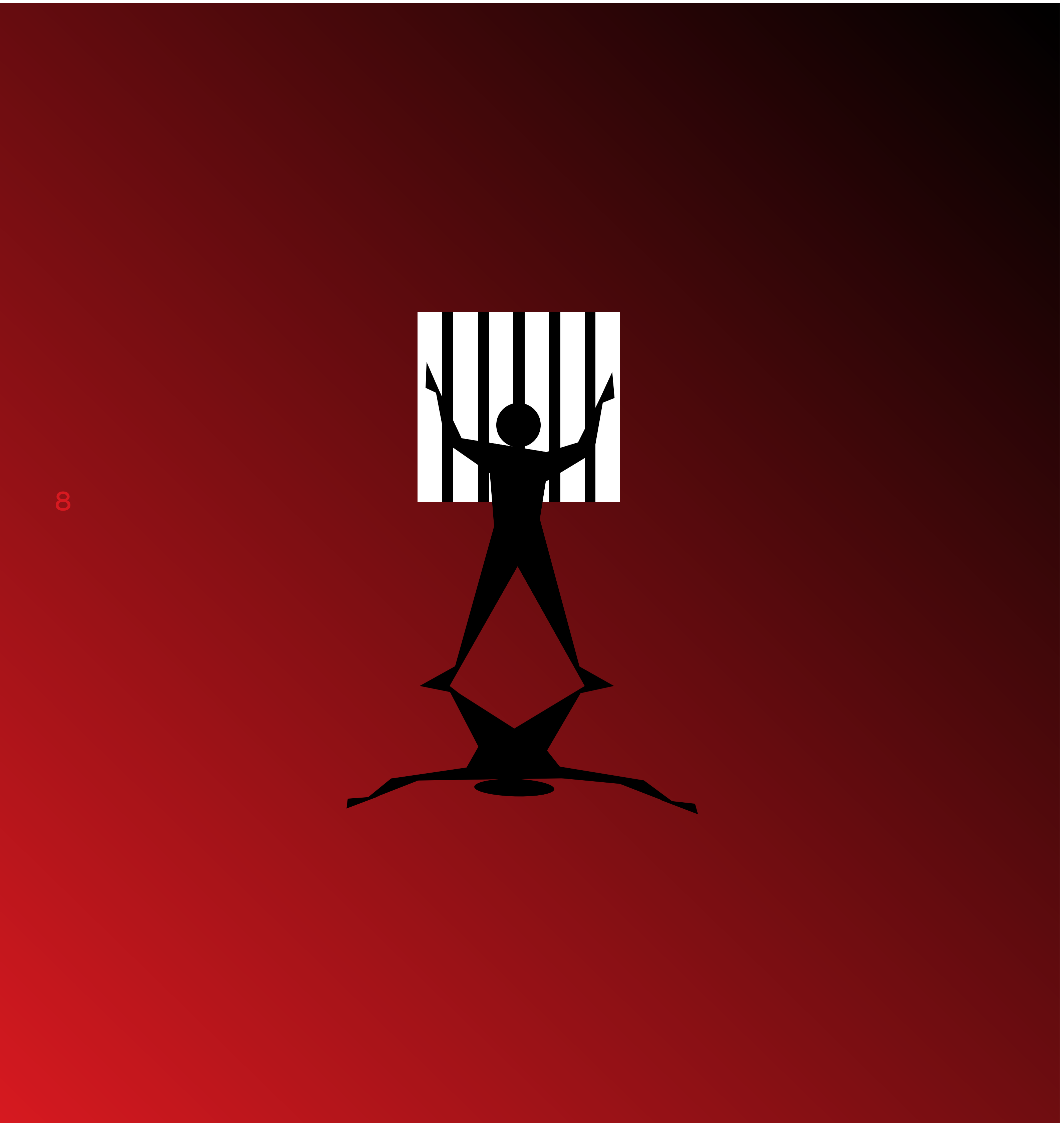
Changes in local government leadership significantly impact cybersecurity strategy. This new leadership can lead to shifting priorities and budget allocations, which may destabilise long-term cybersecurity investments and affect the consistency of maintaining strong, proactive cybersecurity measures. New political leadership in the central government can also have implications for the regulatory environment, affecting how local governments approach cybersecurity compliance and protection. A clear and consistent approach to risk management is vital for ensuring ongoing protection.

As a long-time partner of the local government sector, Trend Micro understands its challenges. The cybersecurity landscape in the local government sector is growing increasingly complex, meaning local authorities must proactively develop network resilience and rapid response capabilities to contain emerging threats.

That's why we developed Trend Micro Vision One: a unified platform that combines Attack Surface Risk Management (ASRM) with Extended Detection and Response (XDR). We can help your council manage risk across your entire network attack surface, more efficiently, cost-effectively and simply.

## How does Trend Micro meet the needs of local government?

- **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.
- **Unified platform for modern and legacy systems:** Trend Vision One helps local councils overcome these challenges by offering a unified platform that is scalable, adaptable, and specifically designed to integrate legacy systems with modern cybersecurity defenses.



# SECTION 2: HANDLING SENSITIVE DATA

## What makes local government especially vulnerable to cyber attack?

UK local government oversees a broad range of sensitive data, including personal details, financial records, and information related to public services. This data is crucial for service delivery but presents significant cybersecurity risks. Cybercriminals target local government to access this data for identity theft, financial fraud, and ransomware attacks.

To mitigate these risks, local government must implement robust data protection measures, such as encryption, access controls and regular security audits. Staff training on data handling practices and awareness of phishing and social engineering attacks is also vital to prevent unauthorised access.

However, many councils face budget constraints and limited resources, making it difficult for IT staff to secure the necessary funding for critical cybersecurity projects and hindering their ability to implement comprehensive data protection strategies. This often results in a false economy, as building cybersecurity into systems from the outset is far more cost-effective and secure than addressing vulnerabilities after an attack. Local government must therefore prioritise cybersecurity investment and explore initiatives to enhance data protection and resilience.

For a local council strategic partnership group, where IT security systems for three local authorities are run through one lead, there was an increasing concern about an expanding attack surface as the cloud environment used grew. Trend Vision One monitors the attack surface for security gaps such as vulnerabilities and misconfigurations, and offers suggestions for remediation alongside automated actions. It also uses AI to supercharge the productivity of SecOps analysts, enabling them to see more and contain threats faster.

In this scenario, the local council strategic partnership group maintains its corporate risk registers, with cybersecurity prioritised as a critical focus area. The team found that Trend Vision One's operations dashboard, which presents a visual breakdown of risks into low and high categories, was instrumental in helping them contextualise cybersecurity threats and monitor their progress in mitigating these risks. This clear visualisation made the risks more tangible and easier to communicate to the business.

By helping the team better manage cyber risks and communicate that risk in a language that the board understands, Trend Vision One has helped the strategic partnership to allocate cybersecurity budget to the areas most in need, and inform its general strategy for threat defence.

### Attacks and their implications

Malicious actors are increasingly targeting local government due to the valuable data they manage. To maintain security, organisations at the local level must have systems and operations that are highly effective, intelligent and easy to manage.

Local government budgets are one of the areas of public services where real-terms spending remains lower in 2024/25 than it was in 2010/11. This has placed immense pressure on the quality and accessibility of local authority services. Since 2018, eight local authorities have issued section 114 notices, compared to just two in the previous thirty years. These financial pressures make it harder to implement and maintain robust cybersecurity measures, leaving organisations more vulnerable to attacks.

Given the influence that public sentiment exerts upon the outcome of future elections, any serious breach or outage can have a significant reputational and financial impact, also risking section 114 notices and necessitating cost reductions.

### Leicester City Council attack

In March 2024, Leicester City Council temporarily shut down its network due to a cyber attack. Within a few weeks, confidential data had been published online by a ransomware group. This data included rent statements, applications to purchase council housing and personal ID such as passport information. Later, the group published a further 1.3TB of sensitive data.

This attack had a significant impact on council services. In the short term, streetlights remained lit through day and night, and there were disruptions to child protection, adult social care and homelessness services. The longer-term financial cost of this attack remains to be seen.

### Gloucester City Council attack

In December 2021, Gloucester City Council was the subject of a ransomware attack which encrypted its servers and suspended council services. The initial attack was in the form of a single spear phishing email inserted into an existing email chain with a supplier.

Rebuilding servers and restoring operations cost approximately £845,000, and the resulting disruption to public-facing services lasted several months. For example, the democratic services team had no way to process changes or additions to the electoral roll, meaning approximately 21,000 postal voters were asked to complete their application forms again.

## How does Trend work to keep local government networks safe?

Trend Vision One secures diverse hybrid IT environments, automates and orchestrates workflows, and provides expert services. It simplifies and converges your security operations within a single platform, so you can shut down attacks more quickly and take greater control of cyber risks.

Your council can achieve holistic security management with Trend Vision One's comprehensive prevention, detection, and response capabilities, which are powered by leading threat research and intelligence. Trend's reliable protection gives value back to the taxpayer, and provides a smoother, more seamless experience that increases confidence in your administration.

Due to the sensitive nature of data they hold, councils must know who is accessing their systems in order to protect their data. Extended Detection and Response (XDR) offers the ability to detect, hunt, investigate, analyse and respond to threats so that they can be rapidly contained. The platform inherently embeds zero trust, and is enhanced by AI to contextualise risk, reduce noise and help analysts prioritise and respond to alerts. Trend can provide complete and continuous attack surface visibility, recommended remediation tactics and automated actions to close gaps, fast.

## Trend Vision One proactively protects your reputation by detecting and preventing threats, 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.

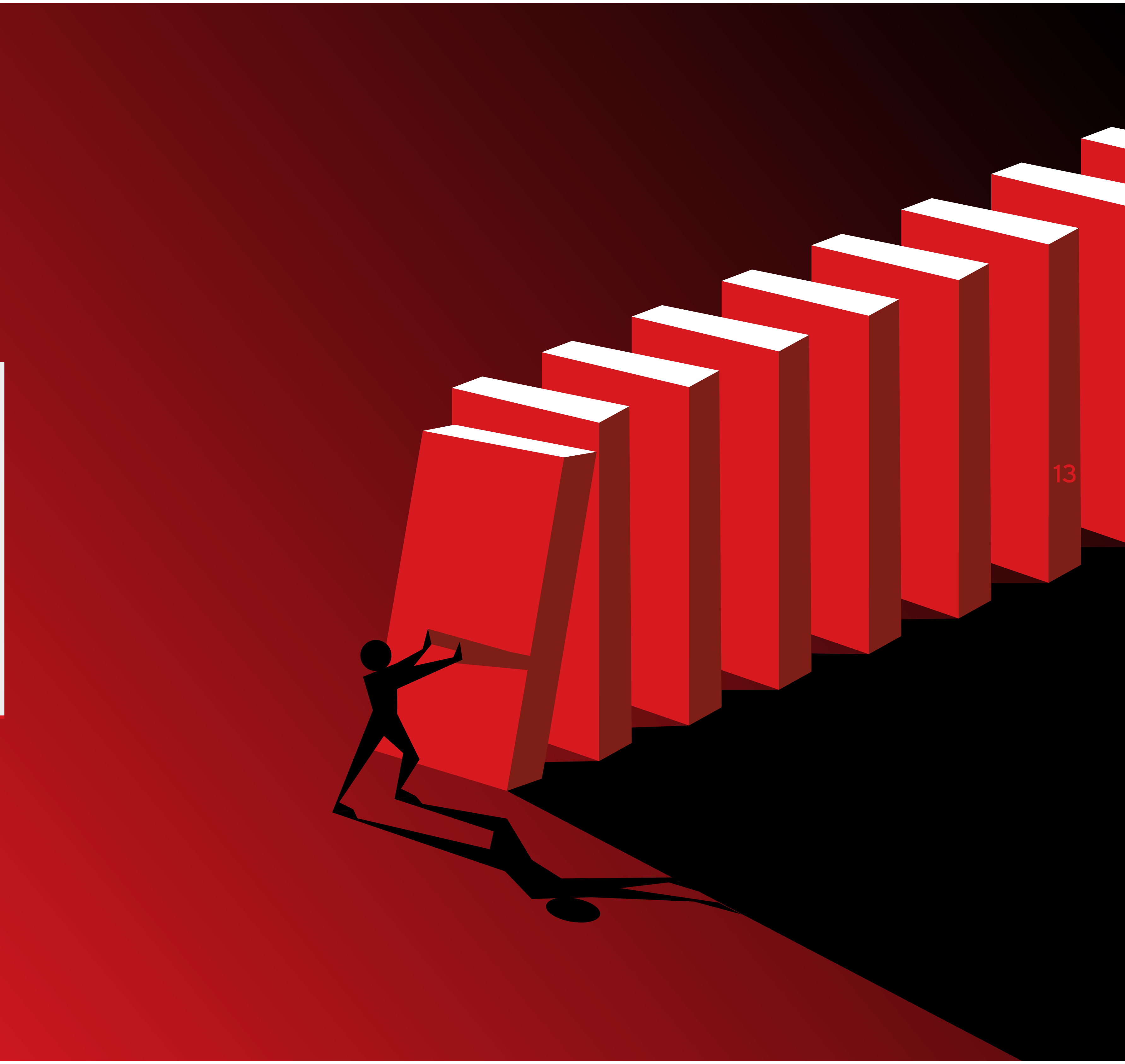
# SECTION 3: REGULATORY COMPLIANCE

## Navigating the patchwork of regulations, standards and codes

If you work within local government, you will be familiar with the patchwork of protocol that dictates how you must operate, and you will know that regulatory compliance is not only about avoiding penalties, it's also about ensuring the security and trust of your constituents. However, ensuring compliance is not simple, and often requires ongoing assessment and improvement.

**Is your authority's cybersecurity compliant with these measures?**

- DPA (Data Protection Act 2018)
- UK-GDPR (UK General Data Protection Regulation)
- DORA (Digital Operational Resilience Act)
- UK Operational Resilience Framework
- Computer Misuse Act 1990
- Telecommunications (Security) Act 2021
- PCER (Privacy and Electronic Communications Regulations)



## The risk of non-compliance

The UK GDPR and DPA 2018 set a maximum fine of £17.5 million for non-compliance (or 4% of annual global turnover, whichever is greater).

However, in the case of public authorities, the UK Information Commissioner has announced that fines will be issued in only "the most egregious cases". In practice this will mean an increase in public reprimands and the use of wider powers, including enforcement notices.

This year (2024), the Information Commissioner's Office reprimanded Hackney Council for failing to prevent a ransomware attack in 2020 that led to the encryption of more than 400,000 files throughout the council's IT estate and left some services disrupted for almost two years.

The ICO had "originally considered imposing a fine" but instead issued a reprimand, in part due to the "positive actions" taken by the council to mitigate the risks caused by the incident.

## Adapting to the evolving regulatory landscape

The new Cyber Assessment Framework (CAF) imposes stringent measures to protect personal data and ensure system integrity, and local government authorities must align to its parameters by the end of this year (2024).

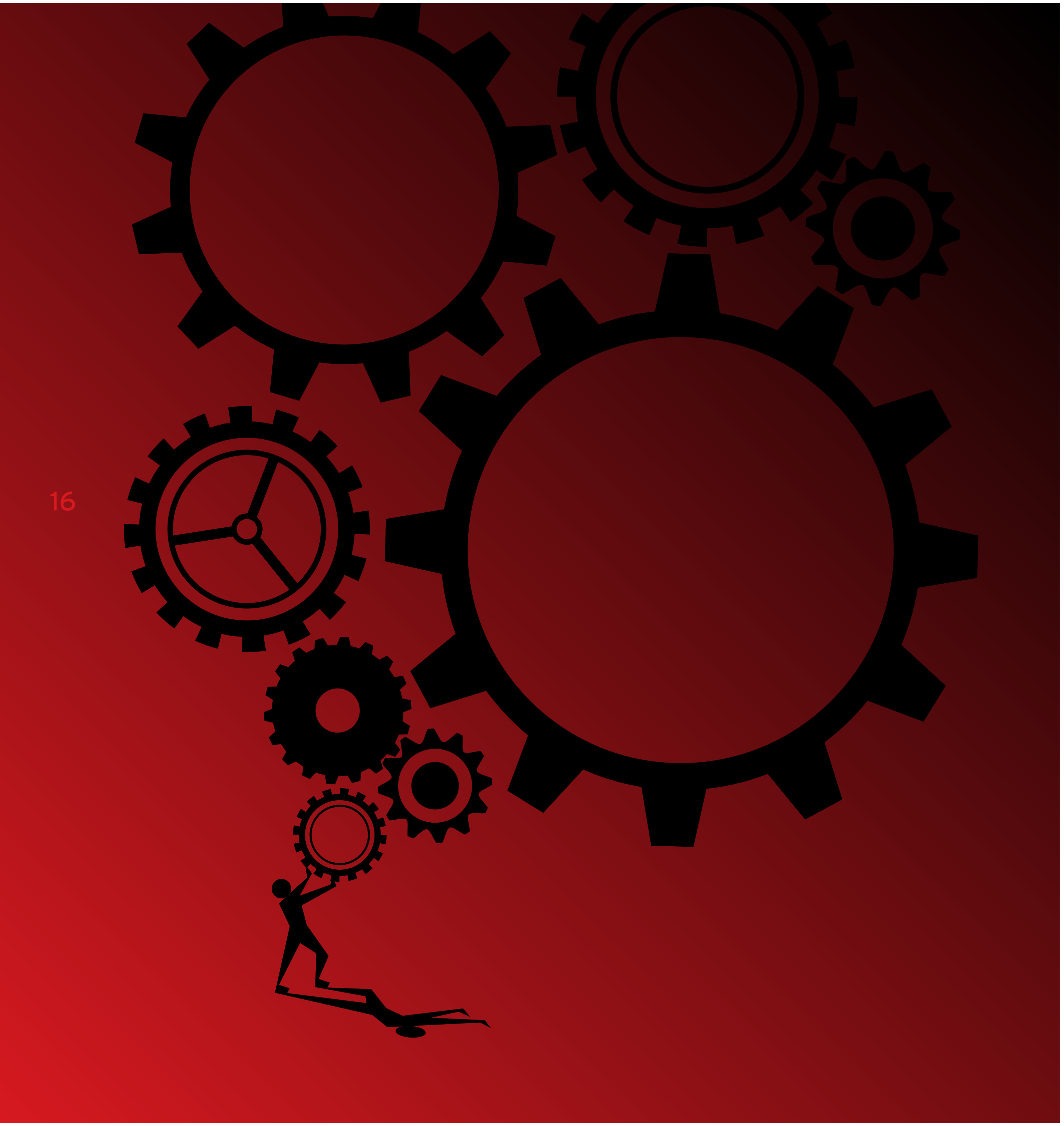
Councils will need to invest time and resources in understanding and implementing these regulatory requirements, which may also involve updating IT systems, revising policies and procedures, and providing training to staff.

To aid in this effort, the Ministry of Housing, Communities and Local Government (MHCLG) is developing a cybersecurity baseline for local authorities, based on the Cyber Assessment Framework, which will give councils a comprehensive way to assess how well they are managing cyber risks to their essential functions. It encourages users to reflect not only on technical aspects, but also on governance, people and processes.

Looking ahead, local governments should anticipate more stringent regulation, as the MHCLG is also considering what reporting requirements and external validation should look like. Councils that proactively invest in their cybersecurity infrastructure now will be better positioned to meet regulatory demands in the future.

## Trend Vision One provides comprehensive security and adaptability for new regulatory requirements:

- Helps local government in **complying** with local and national data protection laws, ensuring **data sovereignty** while managing sensitive information effectively.
- Gain 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.
- **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 to respond to complex scenarios more swiftly, mitigating the skills shortage and improving outcomes
- Vision One provides **automated response capabilities** that mitigate damage and includes **disaster recovery plans** that ensure rapid restoration of operations, safeguarding critical services and minimising disruption.



# SECTION 4: OVERCOMING POLITICAL AND FINANCIAL BLOCKERS

## Tight budgets can lead to difficult choices and risky compromise

The challenge for local government will always be finding a cost-effective way to mitigate cybersecurity risks and to fulfil compliance obligations. In recent years, spending on public services has been notoriously limited, which means that local government must find ways around budgetary constraint to ensure they do not fall behind on cybersecurity.

Several councils have declared "bankruptcy" due to rising costs in essential social services leaving less funding for other services such as IT and cybersecurity. This underfunding leads to outdated IT systems, leaving local governments more vulnerable to cyberattacks[6].

Budget limitations restrict investments in advanced technologies and skilled personnel, leaving councils vulnerable to cyber threats. Cybersecurity competes with other priorities, and political considerations often influence budget allocations.

The recent change in political leadership may also cause budgetary complications, while changing priorities and potentially affecting the consistency of existing cybersecurity measures. New leadership often shifts priorities, which can lead to the need for adaptations in compliance strategies to align with frameworks such as the Cyber Assessment Framework (CAF). As these frameworks outline obligations for data protection and security, councils must ensure their existing systems can meet these requirements while maintaining operational effectiveness.

These practical and financial pressures can lead authorities to accept generic, pre-bundled cybersecurity solutions, which may appear to be cost-effective. However, this can be a false economy, as a breach of sensitive data resulting from inadequate cybersecurity can have far greater reputational and financial costs.

[6] https://www.instituteforgovernment.org.uk/publication/fixing-public-services-labour-government/local-government

## Comparing with generic security solutions in the market

Taking Microsoft as a specific example, it is especially complicated when integrating with any non-Microsoft devices.

Secondly, whilst coverage is generally good, it tends to produce a high-volume of false positive alerts, which means your team must take time to resolve them. Making the most of the tools requires extensive configuration, which takes even more time and training. Then finally, legacy Windows environments offer limited support and require additional costs.

Not only does all of this lead to a less comprehensive coverage of your attack surface, particularly where legacy and on-prem environments are concerned, but it creates an increased administrative burden for your IT teams, which means a longer time to respond to true positives.

## Can local government "do more with less" when it comes to cybersecurity?

One approach to mitigating budgetary constraints is through collaboration and resource sharing. The National Cyber Security Centre (NCSC) and the Ministry of Housing, Communities and Local Government (MHCLG) are working closely with councils to provide support and resources.

Since 2020, more than 180 local authorities have put bespoke Cyber Treatment Plans in place to defend against security risks and vulnerabilities, with help from the MHCLG's local digital team cyber support programme[7].

In today's climate of restricted spending, justifying cybersecurity budgets to decision-makers is crucial. Boards need to see the clear return on investment (ROI) for cybersecurity, particularly when budgets are tight.

Councils should explore cost-effective solutions and shared services to get maximum economy from their cybersecurity investments. This could include leveraging cloud-based security services, participating in joint procurement initiatives, or sharing cybersecurity expertise across multiple councils.

Ultimately, overcoming political and budgetary constraints requires a combination of education, advocacy and strategic planning, but it is possible to "do more with less" when the right solution is adopted. Local government leaders need to be educated about the critical importance of cybersecurity, and cybersecurity professionals need to effectively communicate the risks and potential impacts to secure necessary funding and support.

## Unlocking the economic value of Trend Vision One

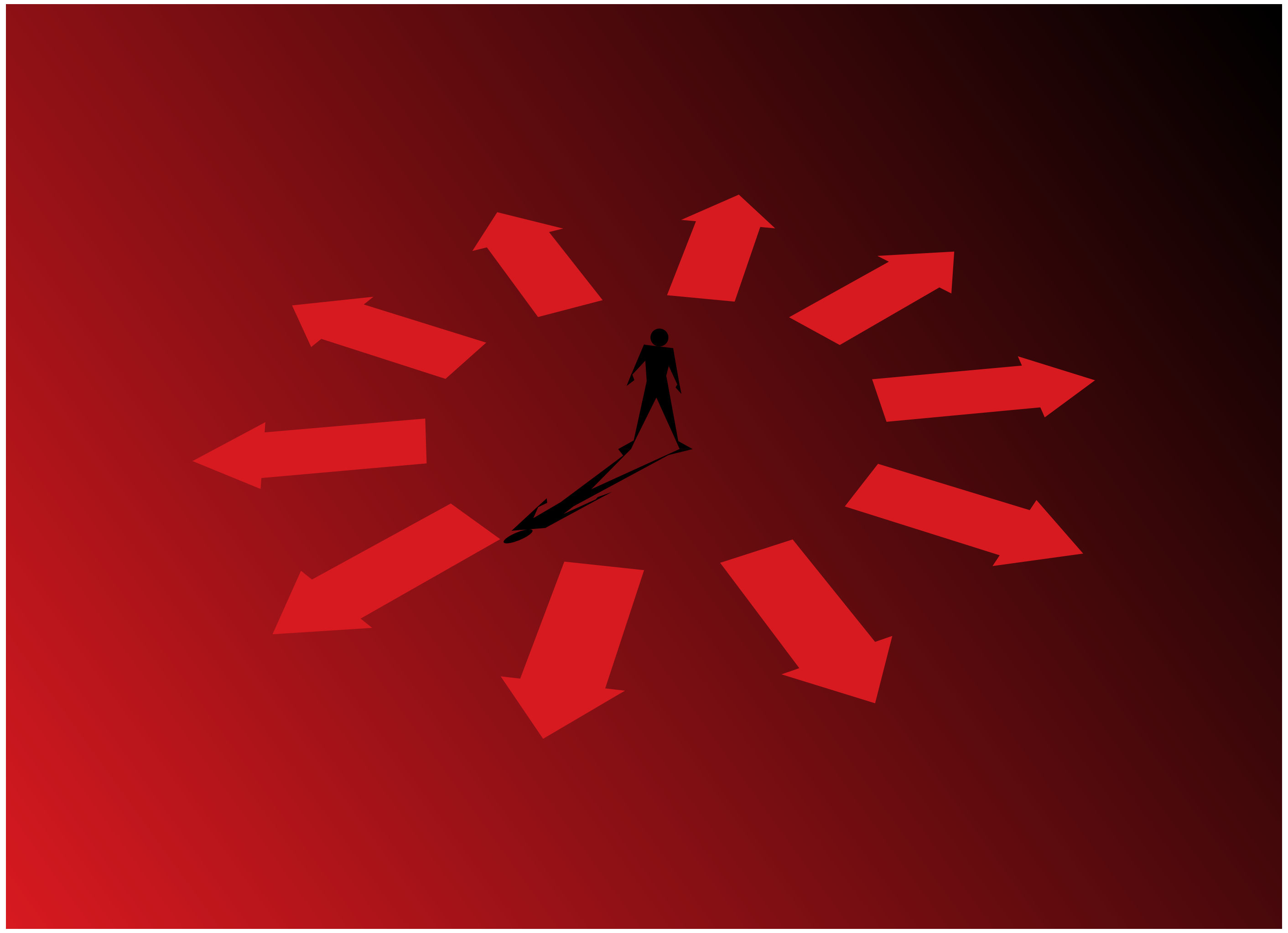
- The Enterprise Strategy Group's economic validation of Vision One demonstrated a **70% reduction in cybersecurity cost**, combined with a **17% reduction in data breach risk** and **20% reduction in employee turnover**.
- It demonstrated a **reduction of alerts per day from 1,000 to 4** and **reduced the average cost of a data breach by £1m**.

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

[7] https://www.governmentbusiness.co.uk/features/how-councils-can-keep-ahead-cyber-threats

## Trend Vision One can help you create a strong business case for cyber security investment:

- Improves **visibility**, insight and **total security posture**. One of the top benefits customers mention is their improved ability to identify and proactively manage risk.
- Generates a significant **ROI of 188%**, relieving the burden upon overworked IT security teams and **improving operational efficiency** for the entire department.
- Provides a consolidated list of opportunities to improve your security posture from an operations dashboard.
- **Risk Insights** provide real-time understanding of your security posture. **Remediation suggestions** and **automations** fix vulnerabilities, misconfigurations and other issues.



# SECTION 5: RESOURCE OPTIMISATION

## Compounding financial pressures for cybersecurity in local government

As public bodies subject to significant scrutiny, local and regional authorities will always find there is a need to demonstrate cost-efficiency while mitigating the risk of cyber attack and demonstrating that compliance obligations are being met.

The boards that sit within local government authorities frequently see cybersecurity as "just another cost centre". They are often not aware of the impact that new legislation such as the Cyber Assessment Framework will have upon their organisation if compliance is not achieved by the end of 2024, and do not therefore appreciate the urgent need for alignment, nor the costs that may result from non-compliance.

There is also a significant cybersecurity skills gap, which board level executives must recognise so investment can be made to improve this situation. In this case, local government recruiting power must compete with the deep pockets of private sector organisations, which is bound to be costly.

Beyond finding the specialised staff, other limitations on resources pose significant challenges. Many councils have under-resourced, under-equipped IT teams, which restricts their ability to manage complex cyber environments.

Frequently, local government will have only one or two individuals who are responsible for cybersecurity. This means the limited workforce they have is stretched thin. They must advocate for the importance of cybersecurity, but they often have little support and their voices may not be heard. Inevitably, they will also be short on time due to their volume of work, so their concerns aren't noted and the network will remain exposed to growing risks.

Finally, the board's desire for maximum cost-efficiency can lead to limited investment in much-needed modern technologies and training, which results in outdated infrastructure and inadequate protection. The risk of successful cyber attack becomes greater, which creates a high degree of pressure and stress on the cybersecurity professionals, leading to high staff turnover, which weakens the cybersecurity posture even more.

## Demonstrating the financial benefits of cybersecurity investment

Those responsible for cybersecurity in local government must be able to effectively communicate its value to the board. Trend Micro's Vision One can help them to do it.

Trend Vision One's attack surface risk management provides orchestration and automation capabilities that improve the efficiency and productivity of under-resourced security teams which are tasked with securing an especially chaotic and fast-moving attack surface environment. Trend Vision One's automated workflows can improve productivity and reduce the time spent on manual tasks, as well as mitigating the need to hire additional staff to cope with these pressures.

Also, a single, centralised platform that covers email, endpoint, cloud, network, data and identity security means less money will need to be spent on maintaining individual point solutions.

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

70%

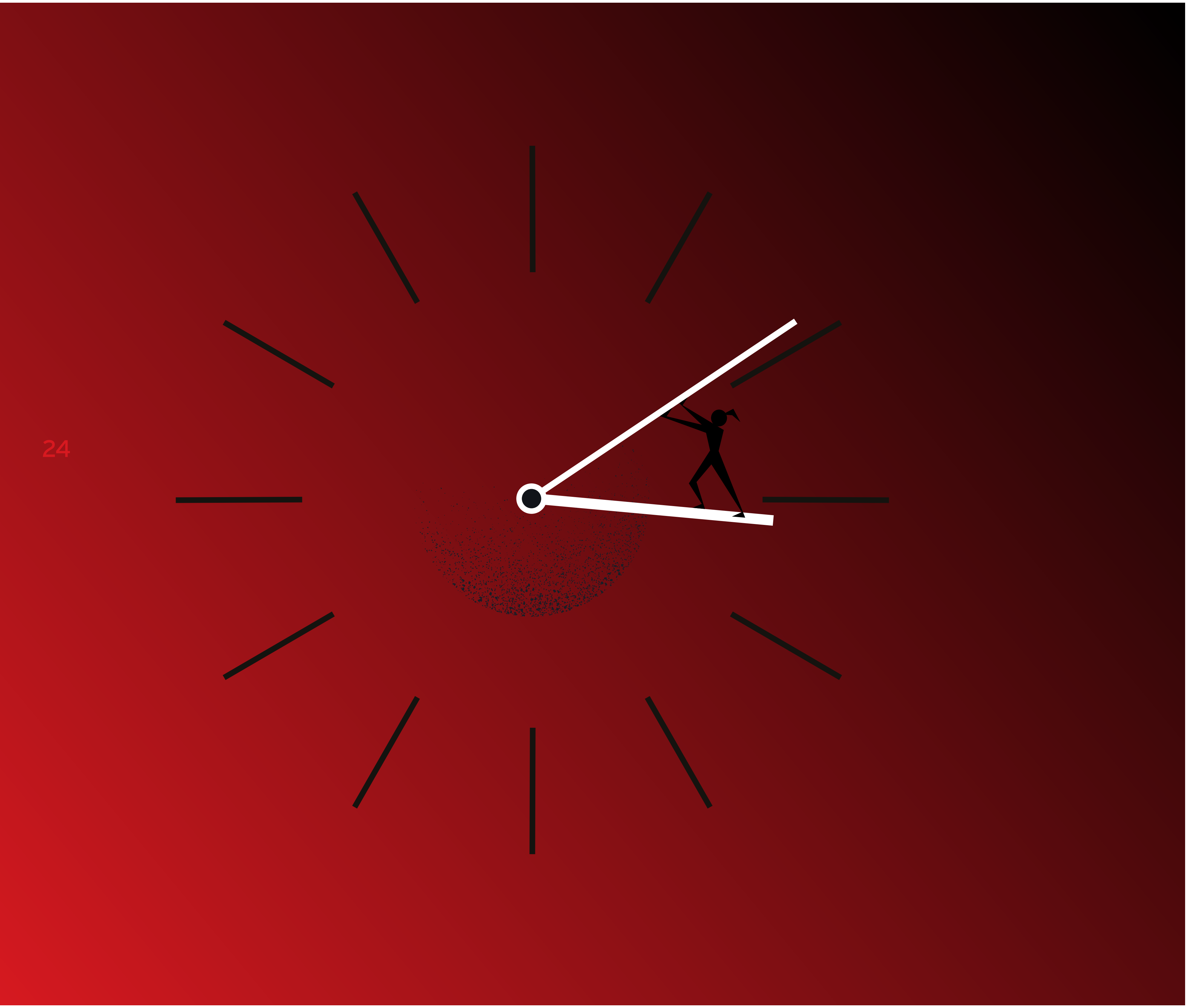
**Reduction in cyber security costs**

£1.3m

**Average cost reduction of data breach**

79%

**Decrease security spend**



# SECTION 6:
# SECURING LOCAL GOVERNMENT

## WHY TREND MICRO IS A TRUSTED CYBERSECURITY PARTNER

### Evolving threats require an evolving cybersecurity solution

The cybersecurity landscape for local government is complex and challenging, but there are clear paths forward for improving security and resilience.

Threats are significant and growing, with UK councils facing over 10,000 cyber attacks daily in 2022[8], and a 24% increase in cyber attacks on local authorities between 2022 and 2023[9].

Despite these challenges, the sector has made notable progress. More than 180 local authorities have implemented bespoke Cyber Treatment Plans since 2020, with help from the MHCLG local digital team's cyber support programme. The development of a clear cybersecurity baseline for local authorities, based on the NCSC's Cyber Assessment Framework, is another positive step.

However, significant work remains. Nearly two-thirds of senior council leaders acknowledged that their approach to cybersecurity was "outdated," with over a quarter reporting a failure to make any progress[10]. This underscores the need for continued investment, education and strategic planning in local government cybersecurity.

For the local government sector, the implications are clear. Cybersecurity must be viewed as a critical, ongoing priority - not a one-time investment. This requires a multi-faceted approach that includes:

1. **Continuous improvement of technical defences**
2. **Regular staff training and awareness programs**
3. **Strategic resource allocation and optimisation**
4. **Collaboration with other councils and national cybersecurity bodies**
5. **Adoption of risk-based approaches to prioritise efforts**
6. **Proactive compliance with evolving regulatory requirements**

[8] https://ppl-ai-file-upload.s3.amazonaws.com/web/direct-files/30065011/204b6a7b-e6e9-45c6-adc8-db8aa4060774/Local-Government_Industry-Brief-Skeleton.docx

[9] https://securityjournaluk.com/local-authorities-improve-cyber-resilience/

[10] https://securityjournaluk.com/local-authorities-improve-cyber-resilience/

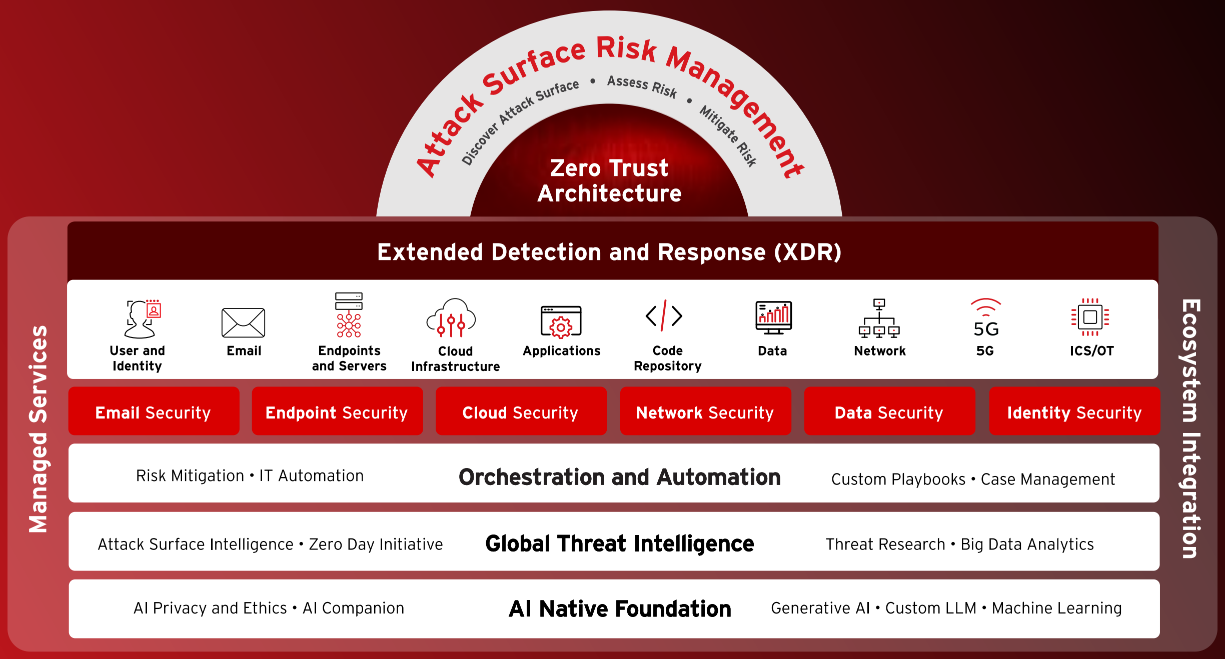
The future of local government cybersecurity will likely involve increased use of advanced technologies, such as artificial intelligence for threat detection, and greater emphasis on shared services and collaborative defence strategies. The sector must also prepare for the cybersecurity implications of emerging technologies, such as the Internet of Things (IoT), which are increasingly being adopted in smart city initiatives.

Ultimately, the goal is to create a resilient local government sector that can effectively protect sensitive data, maintain public trust, and ensure the continuity of critical services in the face of evolving cyber threats. While the challenges are significant, the necessary tools, knowledge, and support are available for local governments seeking to enhance their cybersecurity posture. The key lies in prioritising these efforts, fostering a culture of cybersecurity awareness, and maintaining a proactive, adaptive approach to cyber defence.

## 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 constituents' data. It can help you transform cybersecurity from a cost centre into a strategic enabler, ensuring robust protection while enhancing operational efficiency.


Attack Surface Risk Management
Discover Attack Surface • Assess Risk • Mitigate Risk
Zero Trust Architecture
Managed Services
Ecosystem Integration
Extended Detection and Response (XDR)
User and Identity
Email
Endpoints and Servers
Cloud Infrastructure
Applications
Code Repository
Data
Network
5G
5G
ICS/OT
Email Security
Endpoint Security
Cloud Security
Network Security
Data Security
Identity Security
Risk Mitigation • IT Automation
Orchestration and Automation
Custom Playbooks • Case Management
Attack Surface Intelligence • Zero Day Initiative
Global Threat Intelligence
Threat Research • Big Data Analytics
AI Privacy and Ethics • AI Companion
AI Native Foundation
Generative AI • Custom LLM • Machine Learning

## 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™:*

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 the trusted Local Government cyber security advisors

**Speak with us >**

Start your complimentary 30-day trial

**Activate here >**