Financial Services Business Resilience Report

TREND MICRO™ | Global Leader in Cybersecurity

Contents

1. Know the challenges to your business

Banks, insurance companies, and other financial services organisations are popular targets for cybercriminals.

The UK's financial services sector sees digitalisation as a key priority for driving sustainable growth, now and in the future. One December 2023 report[1] claims around a third of organisations see process automation, technology upgrades, and new product development as their most important investment areas for the coming 24 months. But while innovations like generative AI, blockchain, and predictive analytics can transform the customer experience, enhance productivity, and support better decision making, they also add complexity and expand the corporate attack surface.

That's a challenge in a world where threat actors often have an asymmetric advantage. The sector is increasingly under threat from both profit-driven criminal gangs and coordinated cyber espionage efforts. A majority **(72%) of financial services organisations** have told us they have been compromised by ransomware at least once over the past three years. Meanwhile, new and emerging threats such as data poisoning threaten to derail digital transformation, destroy value, and erode customer trust in financial institutions. That should set alarm bells ringing in a sector built on trust.

Organisations in your industry have a unique responsibility to keep personal and financial information and assets safe and secure in today's digital world. Regulatory requirements, such as the **NIS2 Directive, DARS, GDPR, PCI DSS and PSD2**, are adding further pressure. Non-compliance can have major financial and reputational repercussions, further chipping away at hard-won customer trust.

However, there is a way forward. This report outlines some of the key steps your organisation can take today to balance opportunity with risk and drive advantage for both your business and your customers.

2. Stay ahead of the latest cybersecurity threats

In 2024 we predict[2] an increase in threats such as AI data poisoning and cloud-native worm attacks, as well as the growing use of generative AI for impersonation and identity theft, and emerging blockchain security risks.

All could have a potential impact on financial services. Data poisoning might enable threat actors to sabotage fraud detection systems, leading to an escalation in unauthorised transactions and possible regulatory fines. Cloud-native worms might supercharge customer data theft and ransomware campaigns by making it easier to launch attacks at scale. And if private blockchains aren't properly stress tested and secured, malicious actors will be ready to pounce with extortion attacks that disrupt operations.

We also believe that malicious actors will attempt to infiltrate vendors' software supply chains through their continuous integration and continuous delivery (CI/CD) pipelines. By planting malware in third-party libraries and exploiting vulnerabilities in legacy components, they could infiltrate these pipelines. In a worst-case scenario, a bank may unwittingly send out malicious software updates to customers, which compromise their own devices, machines, and data.

of the IT and business leaders we spoke to admit they have blind spots when trying to secure their attack surface.

admit their method of assessing risk exposure is not sophisticated enough.

The threat to vendors' software supply chains through CI/CD systems is a serious and widespread one. In fact, a global study commissioned by Trend[1] highlights that over half of global organisations have had part of their supply chain compromised by ransomware.

say their attack surface is spiralling out of control.

Cyber threats are everywhere. And they could spell serious financial and reputational damage for your sector, with the potential to fatally erode customer trust. Gaining visibility across the entire attack surface is the first step towards staying ahead of the latest threats, and understanding and effectively mitigating risk – both within and outside your organisation.

This usually means having to manage multiple security technologies and making sure they all work together to mitigate cyber risk. It also means ensuring that any digital transformation and modernisation efforts align with your security strategy. **This can be difficult to achieve – particularly when business users bypass IT altogether when setting up new digital initiatives.**

Given the pace of technology innovation, the rate of digital investment, and the velocity at which the threat landscape is evolving, regular assessments are critical to gaining full visibility and improved control over the digital attack surface.

3. Discover, assess and reduce cyber risk with Trend Vision One™

Building a more risk-aware and resilient organisation involves three key steps:

1.
Gain visibility into all assets and attack vectors

2.
Analyse data to continuously calculate risk exposure

3.
Invest in the right controls to mitigate risk

Trend Vision One integrates Attack Surface Risk Management (ASRM) and extended detection and response (XDR) in a single, cloud-native security operations platform serving cloud, hybrid, and on-premises environments.

Having complete and continuous attack surface visibility enables security leaders to better understand, communicate and mitigate cyber risk across the enterprise. It means faster and more effective incident response to contain threats before they have a chance to spread and impact customer data. And it means being able to take proactive measures such as virtual patching to build resilience against attacks which may compromise key assets and data. This enables you to balance innovation and business growth whilst protecting your brand reputation in an industry where trust is paramount. Ultimately, it makes for a safer digital environment for your customers.

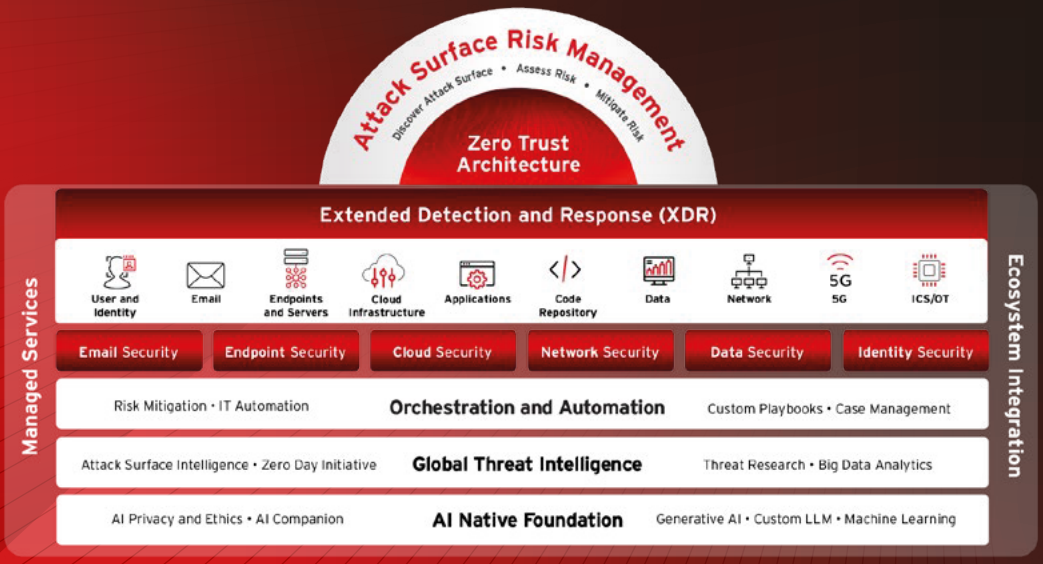
According to ESG, organisations with Trend Micro XDR are 2.2x more likely to detect an attack, save up to 79% on security costs, and improve response times by 70%. Cost savings are strategically of tremendous value, as they can be redirected to enhance customer service or ensure pricing is competitive. Yet over half (53%) of businesses still erroneously view cybersecurity as a necessary cost rather than a business enabler.

savings from a unified security approach that mitigated siloed tools, overstretched teams, and alert fatigue

The most complete attack surface coverage

Our ASRM capabilities provide the most complete attack surface coverage in the industry, enabling you to proactively take charge of risk in actionable ways. It also ensures you can improve cyber risk resilience with real-time assessments and prioritised, actionable risk insights featuring recommendations and proactive risk remediation.

The platform reduces cost and complexity by removing the need for multiple tools and streamlining workflows, and automatically scans against compliance and best practice checks. Its XDR capabilities ensure rapid response to and recovery from new threats, thus minimising the impact on customer organisations. Our Zero Day Initiative (ZDI) – the world's biggest vendor-agnostic bug bounty program – accounted for 64% of publicly disclosed CVEs in 2022. The threat intelligence it generates is pushed straight back into our solutions and services. These include a Virtual Patching feature designed to drive business continuity by protecting critical assets from known and unknown threats, even before official updates are available.



4. Take charge of your cyber risk today

As a global leader in cybersecurity, Trend Micro is trusted by 9 of the top 10 Fortune Global 500 companies, and our Trend Vision One cybersecurity platform protects over 500,000 organisations around the world.

We have over 450 in-house threat researchers and a further 10,000 registered security researchers from 100 countries monitoring and reporting on the latest threats to business security. All of this intelligence feeds into our solutions and services to deliver pre-emptive threat protection, alongside powerful insight for rapid incident response and containment.

We can help you:

- Proactively uncover, evaluate and prioritise attack surface risks
- Leverage attack surface insights to make confident risk-informed decisions
- Assess and report overall risk levels to the board with actionable insights
- Gain control over your entire attack surface
- Ensure there isn't anything lurking in your cybersecurity blind spot
- Reduce your cyber risk footprint

Why you can trust Trend Micro

Trend Vision One
achieved the highest score in the Current Offering category in XDR Evaluation in The Forrester New Wave™ Report

OMDIA
Leader in Global Vulnerability Research and Discovery since 2007

Ranked #1
in IDC's Worldwide Cloud Workload Security Market Shares report

Ranked #1
in MITRE Engenuinity ATT&CK Evaluation for ensuring early attack prevention

Learn more about Trend Micro

To find out more about how we are helping financial services organisations to navigate the growing threat landscape, visit our website.

trendmicro.com/financialservices

[1] Consultancy UK, Digitalisation and automation top focus for financial firms in 2024 (December 2023)

Available at: https://www.consultancy.uk/news/36152/digitalisation-and-automation-top-focus-for-financial-firms-in-2024, https://www.consultancy.uk/news/36152/digitalisation-and-automation-top-focus-for-financial-firms-in-2024

[2] Trend Micro, Stepping Ahead of Risk: Trend Micro 2023 Midyear Cybersecurity Threat Report, (August 2023)

Available at:
https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/stepping-ahead-of-risk-trend-micro-2023-midyear-cybersecurity-threat-report


TREND
MICRO™