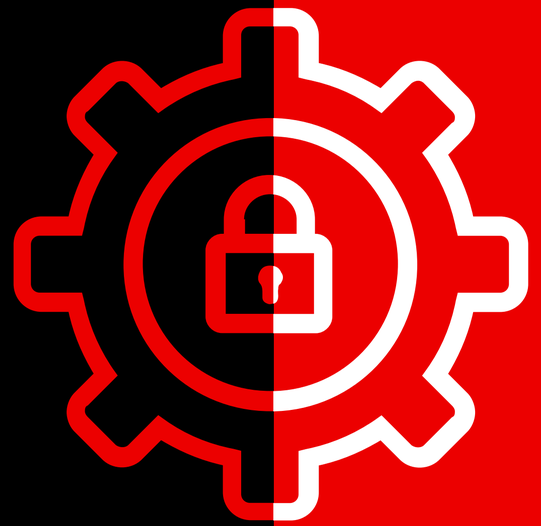
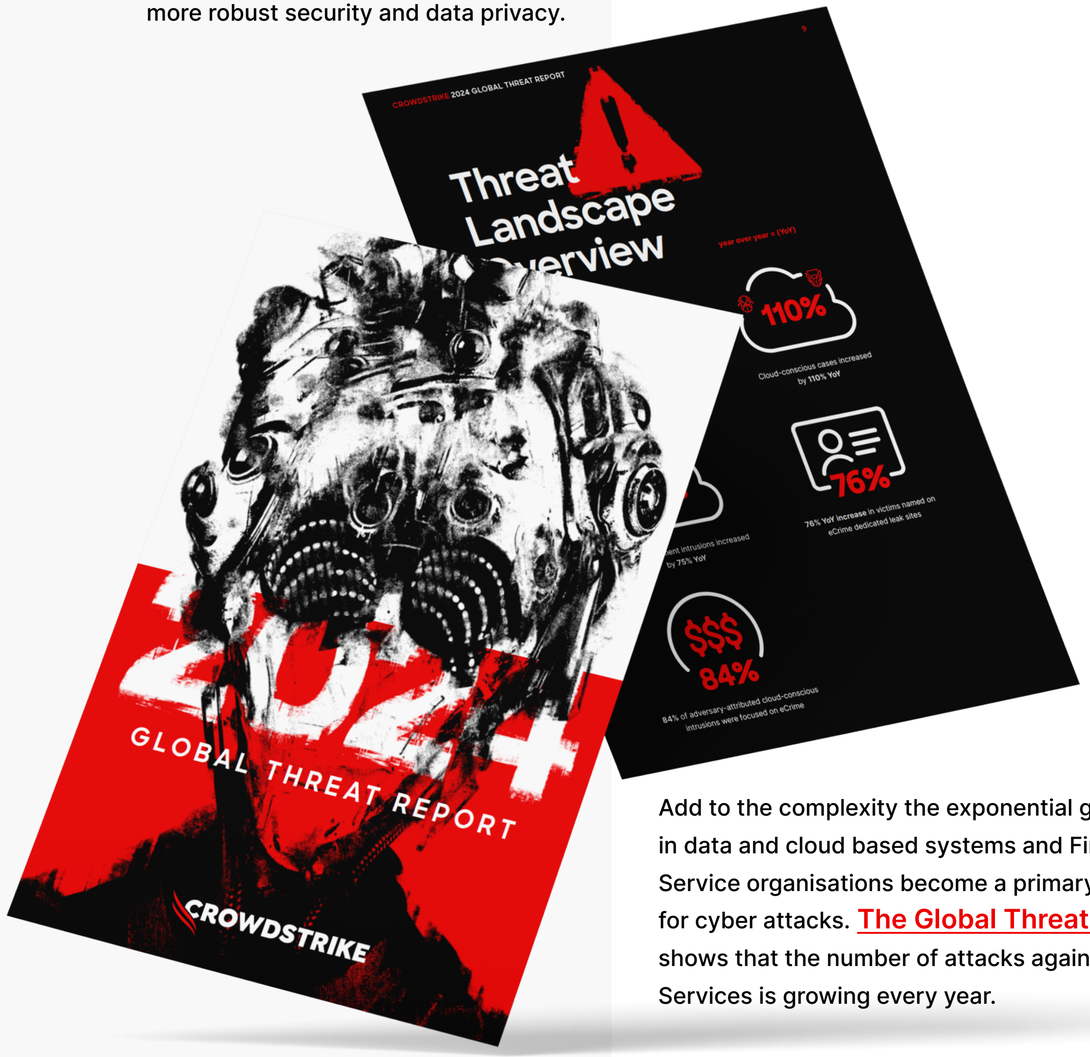
CROWDSTRIKE

Stopping Cyber Threats in Financial Services

Comply with regulations, not adversaries, in an era of escalating cyber threats



The competitive and operational landscapes for Financial Service organisations are evolving and changing. Demand for seamless and personalised experiences create a need for more robust security and data privacy.



Add to the complexity the exponential growth in data and cloud based systems and Financial Service organisations become a primary target for cyber attacks. The Global Threat Report shows that the number of attacks against Financial Services is growing every year.

Regulatory compliance is non-negotiable

Are you adapting fast enough to foil your adversaries?

Are you doing enough to comply with upcoming regulations such as the EU NIS2 Directive and the Digital Operational Resilience Act (DORA)?

Keeping on top of cybersecurity trends helps you avoid the operational, financial, and reputational fallout from an attack. It also prevents you incurring significant fines for non-compliance.

Penalties for Financial sector companies failing to comply or report incidents:

€10m

up to 10 million EUR or 2% of total annual worldwide turnover for NIS2.

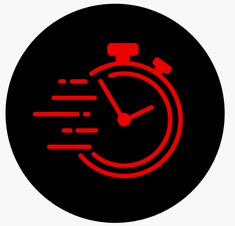
€5m

up to 5 million EUR or 2% of total annual worldwide turnover for DORA.

▶ **Our cybersecurity experts can help you navigate the latest regulatory changes.**

What's happening in the world of cybersecurity, and what does it mean for Financial Services?

7 KEY TAKEAWAYS FOR FINANCIAL SERVICE ORGANISATIONS FROM OUR 2024 **GLOBAL THREAT REPORT**



1. Attacks are more sophisticated and happen faster

Time taken to access a network has dramatically reduced:

- Average breakout time is >25% quicker than in 2023 at 62 minutes.
- Fastest attack recorded was just 2 minutes 7 seconds.

WHAT CAN YOU DO?

Compliance

Update and test incident response plans regularly to meet NIS2 requirements for swift incident reporting and management.

Action

Accelerate threat detection and response times with advanced endpoint detection and response (EDR) solutions.

- **Get up to speed fast. Rely on adversary focused technology with the fastest time to detect (tested by MITRE ATT&CK® Evaluations), tailored for the Financial Services sector.**

2. Malware and attack methods are evolving

75% of attacks are now malware-free, compared with 40% in 2019.

As threat identification improves, adversaries find new ways to evade security. Stolen identity credentials and social engineering attacks make breaches harder to spot.

WHAT CAN YOU DO?

Compliance

Implement strict access controls and monitor user activities to meet NIS2 requirements for securing network and information systems.

Action

Enhance identity protection with multi-factor authentication (MFA).

- **Use cyber threat hunt services to alert you to new adversary techniques.**

3. Cloud intrusions have surged

Cloud-conscious intrusions have risen **110%** in one year.

Cyber adversaries exploit weaknesses in cloud security configurations to attack from within the victim's cloud service.

WHAT CAN YOU DO?

Compliance

Ensure cloud providers adhere to NIS2 standards and best practices to protect cloud-based data and services.

Action

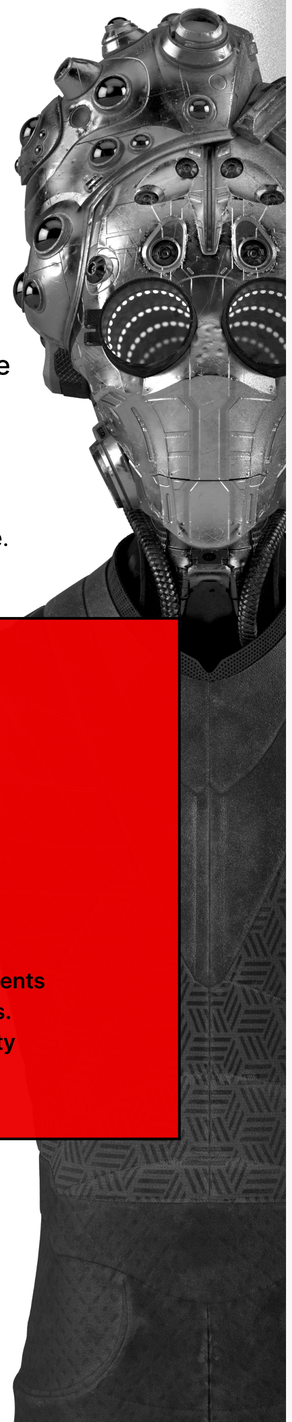
Adopt comprehensive cloud security frameworks, including identity and access management (IAM), encryption, and continuous monitoring.

- **Don't wait for adversaries to breach your financial systems. Seek experts to prevent attacks.**

4. Third-party relationships are being exploited

Commercial software originating from the technology sector was the origin of most compromised trusted relationships.

Adversaries increasingly target third-party vendors and supply chains to access financial institutions' networks, exploiting their interconnected and trusted nature.



WHAT CAN YOU DO?

Compliance

Develop and enforce third-party risk management policies to meet enhanced NIS2 requirements for supply chain security.

Action

Conduct rigorous security assessments and audits of all third-party vendors. Implement contractual cybersecurity requirements for vendors.

- **Adversaries get high ROI from third-party relationship attacks. Ensure supplier security standards are as rigorous as your own.**

5. Adversaries are leveraging generative AI

AI has the potential to be misused for adversary information operations, particularly where audiences are less digitally-literate.

Generative AI has lowered the barrier to entry for sophisticated and widespread attacks.

WHAT CAN YOU DO?

Compliance

Regularly update cybersecurity strategies to address emerging AI threats and align with the NIS2 focus on proactive threat management.

Action

Stay informed about AI-driven threats and consider incorporating AI-based cybersecurity tools to detect and counteract advanced techniques.

- **Use the transformative power of generative AI across security workflows to defend your business.**

6. Identity protection must be a top priority

Our 2024 Global Threat Report shares real-world examples in which phishing and exploitation of software vulnerabilities enabled credentials to be harvested.

Identities are a primary target for cyber intrusions, with an increasing number of attacks leveraging stolen credentials to gain unauthorised access.

WHAT CAN YOU DO?

Compliance

Adopt industry best practices for identity and access management (IAM), as we have in action, to comply with the NIS2 identity protection requirements.

Action

Implement robust identity and access management (IAM) solutions, including real-time monitoring and anomaly detection.

- **Outpace modern threats with a unified platform to avoid identity-based attacks.**

7. Incident detection and response times must be minimised

Adversaries typically seek to expand their access beyond the initial point of compromise, taking around an hour on average. They can then wreak havoc in just seconds.

Rapid detection and response to cyber incidents are critical. Delays can exacerbate any damage caused by a breach.

WHAT CAN YOU DO?

Compliance

Develop and regularly test incident response plans to ensure swift action, meeting the NIS2 stringent reporting timelines.

Action

Invest in advanced monitoring and analytics tools that provide real-time visibility into network activity.

Regulatory compliance is non-negotiable, particularly for financial institutions. Going it alone exposes your organisation — and your clients — to unnecessary risk.

Establish a dedicated compliance team to monitor regulatory developments and ensure cybersecurity practices are up to date. Make sure they conduct regular compliance audits and update policies to align with NIS2, DORA, and other relevant frameworks.

Cybersecurity experts can help you navigate the latest regulatory changes.

Read our CrowdStrike 2024 Global Threat Report

7 key takeaways from the CrowdStrike 2024 Global Threat Report

1. Attacks are more sophisticated and happen faster
2. Malware and attack methods are evolving
3. Cloud intrusions have surged
4. Third-party relationships are being exploited
5. Adversaries are leveraging generative AI
6. Identity protection must be a top priority
7. Incident detection and response times must be minimised

DOWNLOAD REPORT

CROWDSTRIKE

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritised observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike. We stop breaches.