SOPHOS

Securing Financial Services Organizations Against Advanced Cyberthreats

Sophos MDR is the leading Managed Detection and Response service for the financial services sector

Financial service providers are a prime target for cybercriminals. Adversaries are increasingly attracted by the sensitive data they hold, and the opportunity to extort payments using ransomware and the threat of breach exposure.

As cyberthreats grow in both volume and complexity, many financial service providers are turning to the Sophos Managed Detection and Response (MDR) service for protection against advanced attacks that technology alone cannot prevent. This solution brief explores the cybersecurity challenges facing the sector and introduces Sophos MDR, the number one MDR service supporting the financial services sector today.

A Sophos Whitepaper. February 2023

The Cybersecurity Challenge Facing Financial Services

Financial service providers are a major target for cyberthreats

Over half (55%) of financial services organizations were hit by ransomware in 2021 up from 34% in 2020[1]. This 62% rise over the course of a year demonstrates the rapid acceleration of the cyberthreat challenge facing the financial services sector.

More broadly, the majority of IT managers working in the sector reported an increase in the volume (55%), complexity (64%) and impact (55%) of cyberattacks over the last year. As cyber criminals continue to leverage automation and the 'malware-as-a-service' model in their attacks, these numbers are only set to increase.

55% hit by ransomware in 2021

55% report an increase in attack volume

64% report an increase in attack complexity

55% report an increase in the impact of cyberattacks

The impact of advanced cyberthreats on financial services is severe

A major cyber incident has very considerable financial and operational repercussions for financial services organizations. In 2021, the average cost to remediate a ransomware attack came in at $1.59 million, with well over one third (37%) of the encrypted data remaining unrecovered after the incident.

Recovery costs are just part of the story. Nearly all (91%) financial service providers hit by ransomware said the attack impacted their ability to operate, while 85% of those in the private sector said it caused them to lose business/revenue. If IT systems go down, providers' ability to deliver services is often severely inhibited, with major repercussions for clients.

Recovery can be time-consuming, with over a quarter (26%) of financial services ransomware victims taking over a month to get back to normal after the attack.

US$1.59M average remediation cost

91%
of attacks impacted ability to operate

85%
of attacks resulted in lost business/revenue

1 The State of Ransomware in Financial Services, 2022, Sophos. Independent survey of 5,600 IT professionals including 444 from the financial services sector. Hit by ransomware is defined as one or more devices being impacted but not necessarily encrypted.

Financial services are struggling to keep pace with well-funded adversaries

The reality is that technology solutions alone cannot prevent every cyberattack. To avoid detection by cybersecurity solutions, malicious actors increasingly use legitimate IT tools, exploit stolen credentials and access permissions, and leverage unpatched vulnerabilities in their attacks. By emulating authorized users and taking advantage of weaknesses in an organization's defenses, malicious actors can avoid triggering automated detection technologies.

The only way to reliably detect and neutralize determined cyber attackers is with 24x7 eyes on glass delivered by expert operators who leverage diverse security alerts and real-time threat intelligence to identify and stop threats before the damage is done.

However, the complexity of modern operating environments and the velocity of cyberthreats make it increasingly difficult for most organizations to successfully manage threat detection and response on their own.

Organizations across all sectors, including financial services, are struggling to keep pace with well-funded adversaries who are continuously innovating and industrializing their ability to evade defensive technologies.

Sophos MDR: Securing Financial Service Providers

As the cybersecurity challenge continues to grow, financial services organizations are increasingly turning to the Sophos MDR service to help them stay ahead of today's advanced threats.

24/7/365 ransomware and breach prevention service

Sophos Managed Detection and Response (MDR) is a fully managed service delivered by experts who detect and respond to cyberattacks targeting your computers, servers, networks, cloud workloads, email accounts, and more.

- **Detect:** We monitor your environment 24/7, collecting, contextualizing, and correlating security data from the Sophos Adaptive Cybersecurity Ecosystem and your existing cybersecurity investments to identify suspicious activities
- **Investigate:** Expert human operators investigate potential incidents, leveraging our deep financial services sector and threat expertise to hunt for signs of adversarial activities
- **Remediate:** Analysts quickly remediate attacks across the broad range of your environment, before they turn into something more damaging such as ransomware or a wide scale data breach
- **Review:** Comprehensive root cause analysis of incidents together with regular health checks and weekly and monthly reporting enable you to improve security posture and prevent future recurrence

With an average time to detect, investigate and remediate of just 38 minutes, Sophos MDR is more than 5 times quicker than even the fastest in-house security operations team.

With Sophos MDR, you benefit from our team of over 500 security operations specialists who provide expertise across all elements of the detection and response cycle, from threat hunting and neutralization to malware engineering and security automation. With six security operations centers (SOCs) located across Australia, India, Europe, and North America, we provide seamless 24/7 coverage every day of the year.

A service designed around you

We understand that each financial services organization is different with their own existing security investments, IT/cybersecurity staff, and IT environment. Sophos MDR meets you where you are: you choose the level of support required, whether you want us to notify you of threats so your team can take remedial action, contain threats on your behalf, or provide full incident response and root cause analysis. Our security specialists will work with you to identify the right approach for your organization.

Elevate your protection using your existing investments

Today's advanced threats can come from any direction, and adversaries often deploy multiple tools, tactics and procedures in the course of their attacks. Sophos MDR analysts detect and respond to attacks across your entire environment using the Sophos and third-party security tools you already have in place. We can use your:

- **Endpoint telemetry** to spot malicious activities and attack behaviors
- **Firewall data** to detect intrusion attempts and beaconing
- **Network telemetry** to identify rogue assets, unprotected devices, and novel attacks
- **Email alerts** to pinpoint initial entry into the network and attempts to steal access data
- **Identity data** to detect unauthorized network entry and attempts to escalate privileges
- **Cloud alerts** to indicate unauthorized network access and efforts to steal data

The more we see, the faster we act. By detecting and responding to advanced attacks using your existing security tools, Sophos MDR reduces cyber risk while increasing return on your security investments.

Sophos MDR: The Number One MDR Service For Financial Services

Sophos is the number one MDR provider globally, securing more organizations than any other provider against ransomware, breaches, and other threats that technology alone cannot stop.

Sophos MDR secures over 500 financial service providers, giving us unparalleled depth and breadth of expertise into threats facing the financial services sector. We leverage this extensive telemetry to generate 'community immunity', applying learnings from defending one provider to all other customers in the sector, elevating everyone's defenses.

Of course, what matters most is the cybersecurity outcomes we deliver for our customers. Sophos is the highest rated and most reviewed MDR solution on Gartner® Peer Insights™ with a 4.8/5 rating across 271 reviews as on December 20th, 2022 and 97% of customers saying they would recommend us. Sophos is also rated the Top Vendor in the 2022 G2 Grid® for MDR Services serving the midmarket, as well as being named a Leader for MDR in the G2 Overall, Midmarket and Enterprise segments.

Number 1 for Financial Services

- ✓ **Most trusted:** over 15,000 organizations use Sophos MDR (Q1, 2023)
- ✓ **Highest rated:** 97% of customers would recommend us
- ✓ **Most reviewed:** 271 reviews on Gartner Peer Insights in 2022

Hear from our financial services customers

★★★★★

"The quality of the security, which gives us peace of mind knowing that we have a team watching our back and we aren't alone in keeping our business and client data safe."

50M – 250M USD Firm Size, North America. Full review on Gartner Peer Insights

★★★★★

"It has been a few months now and I am so happy with the ROI I can see. Even as a non-IT exec the monthly reports are great...we are completely compliant with our industry standards due to Sophos MDR."

<50M USD Firm Size, Asia-Pacific. Full review on Gartner Peer Insights

★★★★★

"With their timely action we succeed to bring back our network to normal stage without data lose. Also they provided an excellent report with the complete details as how it was happened."

1B – 3B USD Firm Size, EMEA. Full review on Gartner Peer Insights

Next Steps

To learn more about Sophos MDR and how we can support your business, speak with a Sophos adviser today or visit www.sophos.com/mdr

"The IT team has saved at least 40 hours a week that would otherwise have been spent in security operations tasks."

AAVAS Financiers Limited

"Sophos MDR helped us keep up with the growing volume and sophistication of cyberthreats without ramping up our security operations team."

Tourism Finance Corporation of India Limited

Sophos MDR

- 24/7 real-time threat monitoring and response
- Expert lead threat hunting
- Cross-product (Sophos and third-party) consolidation and correlation of security event data
- Full-scale managed incident response (unlimited number of hours; no additional fees or retainers)
- Best in class breach protection warranty
- Dedicated incident response lead assigned
- Direct call-in support to Sophos security operations centers (6 global SOCs)
- Weekly and monthly activity reports
- Monthly intelligence briefings
- Root cause analysis performed to improve security posture and prevent recurrence of future threats
- Regular Sophos account health checks to review configurations and ensure optimal performance

2023-02-27 (WP-NP)

SOPHOS