SOPHOS

Securing Small Businesses Against Advanced Cyberthreats

Sophos MDR is the leading Managed Detection and Response service for small businesses

Small businesses are a prime target for cybercriminals because they often lack the cybersecurity technologies and resources required to combat today's advanced threats. As cyberthreats grow in both volume and complexity, many small businesses 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 small businesses and introduces Sophos MDR, the number one MDR service supporting small businesses today.

A Sophos Whitepaper. February 2023

The Cybersecurity Challenge Facing Small Businesses

Small businesses are a major target for cyberthreats

59% of small businesses were hit by ransomware in 2021, up from 23% in 2020[1]. This 157% rise over the course of a year demonstrates the rapid acceleration of the cyberthreat challenge facing small businesses.

More broadly, IT Managers within small businesses reported a significant increase in the volume (48%), perceived complexity (50%) and impact (46%) 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.

157% increase in ransomware attacks on small businesses in 2021

46% of small businesses report increase in attack complexity

50% of small businesses report increase in attack volume

The impact of cyberthreats on small businesses is severe

A major cyber incident has very considerable financial and operational repercussions for small businesses. In 2021, the average ransom paid by small businesses was a crippling $1.12 million[2]. While this includes a small number of very large payments, almost half (45%) paid between $100,000 and $500,000. Furthermore, the average overall cost to remediate a ransomware attack for these organizations was $750,000, with over a quarter (28%) of encrypted data remaining unrecovered after the incident.

Recovery costs are just part of the story. Over three quarters (77%) of small businesses hit by ransomware said the attack impacted their ability to operate while 72% said it caused them to lose business/revenue. If IT systems go down, the ability of many small businesses to serve their customers is often severely inhibited, with major commercial consequences. In addition, recovery can be time-consuming with a quarter (25%) of small business ransomware victims taking over a month to get back to normal after the attack.

US$1.12M average ransom paid

77%
of attacks impacted ability to operate

72%
of attacks resulted in lost business/revenue

1 The State of Ransomware 2022, Sophos. Independent survey of 5,400 IT professionals including 551 from small businesses, defined as those with 100-250 employees. Hit by ransomware is defined as one or more devices being impacted but not necessarily encrypted.

2 Based on ransom payment information from 56 IT professionals in small businesses with between 100 and 250 employees that had data encrypted and paid the ransom

Small businesses 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 to successfully manage threat detection and response on their own. Organizations of all sizes are struggling to keep pace with well-funded adversaries who are continuously innovating and industrializing their ability to evade defensive technologies.

Sophos MDR: Securing Small Businesses Worldwide

As the cybersecurity challenge continues to grow, small businesses 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 understanding of small businesses 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 small business 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 Small Businesses

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

Sophos MDR protects many thousands of small businesses around the world, giving us unparalleled depth and breadth of expertise into threats facing smaller organizations. We leverage this extensive telemetry to generate 'community immunity', applying learnings from defending one small business to all other customers with a similar profile, 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 Small Businesses

- ✓ **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 small business customers

★★★★★

"Sophos MDR provides us the best and cost-effective solution to monitor all our systems and proactively respond to incidents and threats - day or night, workdays & holidays."

<$50M revenue, IT Services, North America. Full review on Gartner Peer Insights

★★★★★

"The MDR Solution has been great from the onboarding to deployment. It has been a few months now and I am so happy with the ROI I can see. We are a small IT team and don't have time to do everything, now we have time to do our other tasks."

<$50M revenue, Finance (Non-Banking), Asia-Pacific. Full review on Gartner Peer Insights

★★★★★

*"Sophos MDR is by far one of the best solutions that performs a 24*7 human-led threat hunting, detection and containment of suspicious threats that can otherwise affect your daily operations significantly. I am fully satisfied with the service and resolution that MDR team continues to perform."*

<$50M revenue, Services (Non-Government), Asia-Pacific. Full review on Gartner Peer Insights

★★★★★

*"Sophos MDR service is really a value addition for the customers who doesn't own a 24*7 SOC team. We do not need to worry about the skills required for the incident handling. They are proactive in taking actions."*

<$50M revenue, IT Services, EMEA. Full review on Gartner Peer Insights

Next Steps

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

"We appreciate that Sophos keeps on top of the latest activity and threats, so we can focus on delivering a secure, world-class service for customers and artists."

CD Baby, U.S.

"We don't need to spend time firefighting or worrying about breaches or security threats. This enables us to spend more time working on strategic priorities, safe in the knowledge that our security is being monitored 24/7 and managed by a reliable team of experts."

Forest Traffic Services, United Kingdom

"Sophos is there 24/7 so my team doesn't need to be."

Celayix, Canada

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

2023-02-02 (WP-NP)

SOPHOS