SOPHOS

Endpoint Security Buyers Guide

As cyber threats become ever more complex, the pressure to have the right endpoint solution in place has also grown. However, the endpoint security marketplace has become congested with many different solutions, and is so full of indefensible marketing claims that making an educated decision for your organization is increasingly difficult.

This guide provides clarity by walking you through the key endpoint security technologies to ensure you have the right protection in place. It also enables you to see how different vendors stack up in independent tests, helping you make an informed choice.

The uncomfortable truth about endpoint security

The endpoint security market is full of hype and extravagant claims. However, the reality is that 68% of organizations fell victim to a cyberattack in the last year[1]. That's why world-class protection is the foundation of any effective security strategy.

However, protection alone is not enough. Four out of five organization admit having a shortage of internal security expertise[1]. With this in mind usability is also essential if hard-pressed IT teams are to make best use of the protection capabilities. You should also assume that a threat will get through your defenses and equip your organization accordingly. This includes having full visibility into how threats enter the organization, where they went, and what they touched so that you can neutralize the attack and plug any security gaps.

Use this guide to understand the protection technologies available and make and informed choice of endpoint protection products.

Product Features and Capabilities

Endpoint security solutions, sometimes referred to simply as antivirus solutions, may include a variety of foundational (traditional) and modern (next-gen) approaches to preventing endpoint threats. When evaluating solutions, it is important to look for solutions that have a comprehensive set of techniques to stop a wide range of threats. It also is important to understand the threats you are trying to prevent.

Endpoint Threats

While the threat landscape is constantly evolving, below are some key endpoint threats to consider when evaluating different solutions:

- **Portable executables (malware):** When endpoint protection is considered, malicious software programs (malware) is often the primary concern. Malware includes both known as well as never-seen-before malware. Often, solutions struggle to detect the unknown malware. This is important, as SophosLabs sees approximately four hundred thousand pieces of unknown malware every day. Solutions should be adept at spotting packed and polymorphic files that have been modified to make them harder to identify.
- **Potentially unwanted applications (PUA):** PUAs are applications that are not technically malware, but are likely not something you want running on your machine, such as adware. PUA detection has become increasingly important with the rise of cryptomining programs used in cryptojacking attacks.
- **Ransomware:** More than half of organizations have been hit by ransomware in the past year, costing on average $133,000 (USD)[2]. The two primary types of ransomware are file encryptors and disk encryptors (wipers). File encryptors are the most common, which encrypt the victim's files and holds them for ransom. Disk encryptors lock up the victim's entire hard drive, not just the files, or wipes it completely.
- **Exploit-based and file-less attacks:** Not all attacks rely on malware. Exploit-based attacks leverage techniques to take advantage of software bugs and vulnerabilities in order gain access and control of your computer. Weaponized documents (typically a Microsoft Office program that has been crafted or modified to cause damage) and malicious scripts (malicious code often hidden in legitimate programs and websites) are common types of techniques used in these attacks. Other examples include man-in-the-browser attacks (the use of malware to infect a browser, allowing attackers to view and manipulate traffic) and malicious traffic (using web traffic for nefarious purposes, such as contacting a command-and-control server).
- **Active adversary techniques:** Many endpoint attacks involve multiple stages and multiple techniques. Examples of active adversary techniques include privilege escalation (methods used by attackers to gain additional access in a system), credential theft (stealing user names and passwords), and code caves (hiding malicious code inside legitimate applications).

Modern (next-gen) techniques vs. foundational (traditional) techniques

While it may have different names, antivirus solutions have been around for a while and are proven to be very effective against known threats. There are a variety of foundational techniques that traditional endpoint protection solutions have relied on. However, as the threat landscape has shifted, unknown threats, such as malware that has never been seen before, have become more and more common. Because of this, new technologies have come to the marketplace. Buyers should look for a combination of both modern approaches, often referred to as "next-gen" security, as well as proven foundational approaches. Some key capabilities include:

Foundational capabilities:

- **Anti-malware/antivirus:** Signature-based detection of known malware. Malware engines should have the ability to inspect not just executables but also other code such as malicious JavaScript found on websites.
- **Application lockdown:** Preventing malicious behaviors of applications, like a weaponized Office document that installs another application and runs it.
- **Behavioral monitoring/Host Intrusion Prevention Systems (HIPS):** This foundational technology protects computers from unidentified viruses and suspicious behavior. It should include both pre-execution and runtime behavior analysis.
- **Web protection:** URL lookup and blocking of known malicious websites. Blocked sites should include those that may run JavaScript to perform cryptomining, and sites that harvest user authentication credentials and other sensitive data.
- **Web control:** Endpoint web filtering allows administrators to define which file types a user can download from the internet.
- **Data loss prevention (DLP):** If an adversary is able to go unnoticed, DLP capabilities would be able to detect and prevent the last stage of some attacks, when the attacker is attempting to exfiltrate data. This is achieved by monitoring a variety of sensitive data types.

Modern capabilities:

- **Machine learning:** There are multiple types of machine learning methods, including deep learning neural networks, random forest, bayesian, and clustering. Regardless of the methodology, machine learning malware detection engines should be built to detect both known and unknown malware without relying on signatures. The advantage of machine learning is that it can detect malware that has never been seen before, ideally increasing the overall malware detection rate. Organizations should evaluate the detection rate, the false positive rate, and the performance impact of machine learning-based solutions.
- **Anti-exploit:** Anti-exploit technology is designed to deny attackers by preventing the tools and techniques they rely on in the attack chain. For example, exploits like EternalBlue and DoublePulsar were used to execute the NotPetya and WannaCry ransomware. Anti-exploit technology stops the relatively small collection of techniques used to spread malware and conduct attacks, warding off many zero-day attacks without having seen them previously.
- **Ransomware-specific:** Some solutions contain techniques specifically designed to prevent the malicious encryption of data by ransomware. Often ransomware specific techniques will also remediate any impacted files. Ransomware solutions should not only stop file ransomware, but also disk ransomware used in destructive wiper attacks that tamper with the master boot record.
- **Credential theft protection:** Technology designed to prevent the theft of authentication passwords and hash information from memory, registry, and off the hard disk.

- **Process protection (privilege escalation):** Protection built to determine when a process has a privileged authentication token inserted into it to elevate privileges as part of an active adversary attack. This should be effective regardless of what vulnerability, known or unknown, was used to steal the authentication token in the first place.
- **Process protection (code cave):** Prevents use of techniques such as code cave and AtomBombing often used by adversaries looking to take advantage of the presence of legitimate applications. Adversaries can abuse these calls to get another process to execute their code.
- **Endpoint detection and response (EDR):** EDR solutions should be able to provide detailed information when hunting down evasive threats, keeping IT security operations hygiene in excellent health and analyzing detected incidents. It is important to match the size and skillset of your team with the complexity and ease of use of the tool being considered. For example, selecting a solution that provides detailed threat intelligence and guidance, making it quick and easy to respond to a threat.
- **Extended detection and response (XDR):** XDR goes beyond the endpoint and server, incorporating other data sources such as firewall, email, cloud and mobile. It's designed to give organizations a holistic view of their entire environment, with the ability to drill down into granular detail where needed. All of this information should be correlated in a centralized location, typically known as a data lake where the user can ask and answer business critical questions.
- **Incident response/Synchronized Security:** Endpoint tools should at a minimum provide insight into what has occurred to help avoid future incidents. Ideally, they would automatically respond to incidents, without a need for analyst intervention, to stop threats from spreading or causing more damage. It is important that incident response tools communicate with other endpoint security tools as well as network security tools.
- **Managed Threat Response (MTR):** MTR delivers 24/7 threat hunting, detection and response delivered by a team of experts as a fully managed service. Analysts should be able to respond to potential threats, look for indicators of compromise and provide detailed analysis on events that took place, where, when, how and why.

The "power of the plus": combining multiple techniques for comprehensive endpoint security

When evaluating endpoint solutions, organizations should not just look for one primary feature. Instead, look for a collection of impressive features that encompass both modern techniques, like machine learning, as well as foundational approaches that have been proven to still be effective, and endpoint detection and response (EDR) for investigation and incident response. Relying on one dominant feature, even if it is best-in-class, means that you are vulnerable to single point of failure. Conversely, a defense-in-depth approach, where there is a collection of multiple strong security layers, will stop a wider range of threats. This is what we often refer to as "the power of the plus" – a combination of foundational techniques, plus machine learning, plus anti-exploit, plus anti-ransomware, plus EDR, plus much more.

As part of an endpoint security evaluation, ask different vendors what techniques are included in their solution. How strong are each of their components? What threats are they built to stop? Do they rely only on one primary technique? What if it fails?

Sophos vs. the Competition

Comparing products with different features is hard enough, but comparing their performance in simulated attacks, where an attacker's actions are potentially infinite and unknown, is nearly impossible. For those who choose to test on their own, an introductory testing guide can be found here. However, many organizations choose to rely on third party assessments to aid their buying decisions.

360 Degree Assessment & Certification

In the Q4, 2020 MRG Effitas endpoint test Sophos Intercept X blocked 100% of the tested attacks. In addition to Sophos Intercept X, Bitdefender Endpoint Security and Malwarebytes Endpoint Protection received the highest grade (Level 1). ESET Endpoint Security, F-Secure Computer Protection Premium and Microsoft Windows Defender received Level 2.

TEST EMPLOYED	SOPHOS RESULT
In the Wild 360 / Full Spectrum Test	100% block rate
Financial malware	100% block rate
Ransomware	100% block rate
PUA / Adware Test	100% block rate
Exploit/Fileless Test	100% block rate
False Positive Test	0 false positives

Avast Business Antivirus, Avira Antivirus Pro, Symantec Endpoint Protection and Trend Micro Security all failed the test. Read the full report here.

MRG Effitas Malware Protection Test

MRG Effitas conducted a commissioned test comparing the ability of different endpoint protection products to detect malware and potentially unwanted applications (PUA). Six different vendors, including Sophos, were reviewed in the test. Sophos ranked #1 at detecting malware, as well as #1 at detecting potentially unwanted applications. Sophos also had an impressive false positive rate.

MRG Effitas
Efficacy Assessment & Assurance

COMPARATIVE PROTECTION ASSESSMENT

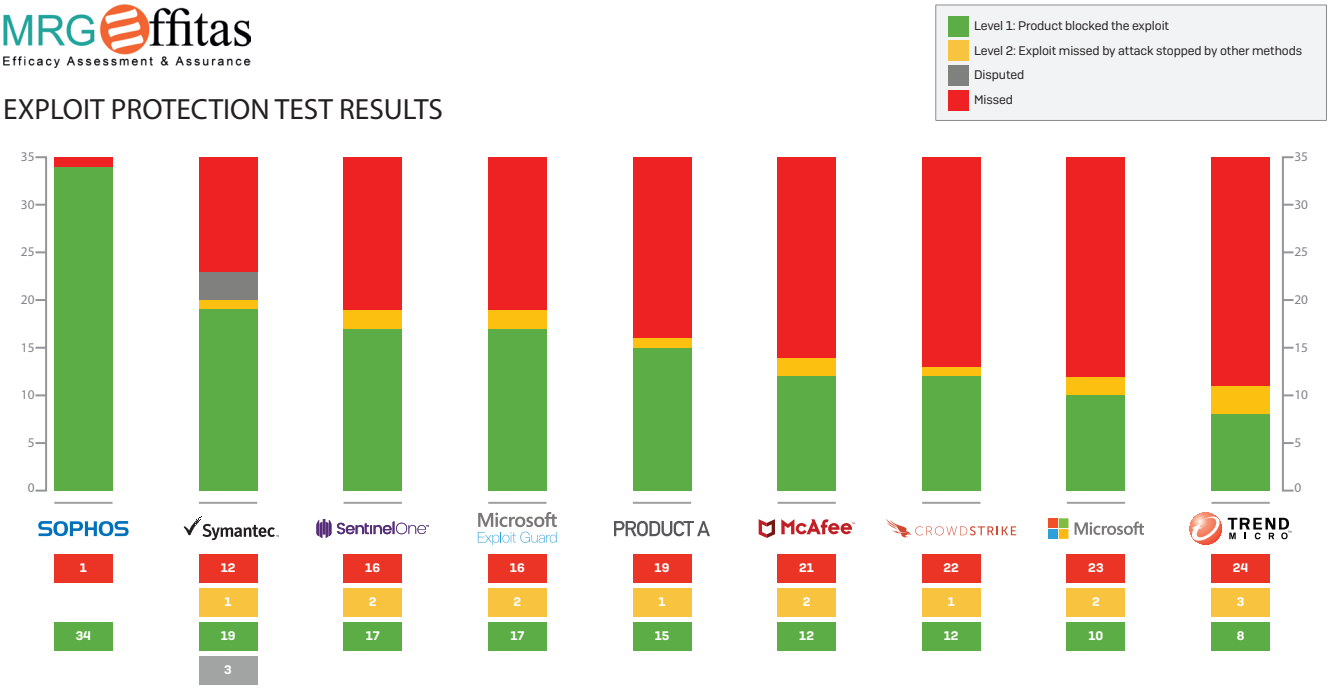
Read the complete results here.

MRG Effitas Exploit and Post-Exploit Protection Test

As a follow up to their malware protection test, MRG Effitas also release a report comparing different endpoint solutions stop specific exploitation techniques. Sophos Intercept X far outperforming the other solutions tested. In fact, Sophos was able to block more than twice the amount of exploit techniques relative to most of the other tools tested.

MRG Effitas
Efficacy Assessment & Assurance

EXPLOIT PROTECTION TEST RESULTS



The full report is available here.

SE Labs Endpoint Protection Report

SE Labs Endpoint Protection Report Sophos Intercept X Advanced achieved a 100% Total Accuracy Rating for both enterprise endpoint protection and small business endpoint protection in the SE Labs endpoint protection test report (Jan - Mar 2020). Intercept X Advanced has been given a AAA rating by SE Labs in every test they have conducted, dating back to April 2018.

TOTAL ACCURACY RATINGS			
Product	*Total Accuracy Rating*	*Total Accuracy (%)*	*Award*
Sophos Intercept X Advanced	1,136	100%	AAA
ESET Endpoint Security	1,136	100%	AAA
Kaspersky Small Office Security	1,136	100%	AAA
Symantec Endpoint Protection Cloud	1,117	98%	AAA
Trend Micro Worry-Free Security Services	1,114	98%	AAA
McAfee Endpoint Security	1,107	97%	AAA
Microsoft Windows Defender Enterprise	1,101	97%	AAA
Bitdefender GravityZone Endpoint Security	1,099.5	97%	AAA
Webroot SecureAnywhere Endpoint Protection	993	87%	A

Source: SE Labs Small Business Protection Jan-Mar 2020

TOTAL ACCURACY RATINGS			
Product	*Total Accuracy Rating*	*Total Accuracy (%)*	*Award*
Sophos Intercept X Advanced	1,136	100%	AAA
ESET Endpoint Security	1,136	100%	AAA
Kaspersky Small Office Security	1,136	100%	AAA
Symantec Endpoint Protection Cloud	1,117	98%	AAA
McAfee Endpoint Security	1,107	97%	AAA
Microsoft Windows Defender Enterprise	1,101	97%	AAA
Bitdefender GravityZone Endpoint Security	1,099.5	97%	AAA
Crowdstrike Falcon	1,089	96%	AAA
VIPRE Endpoint Security	1,087	96%	AAA
FireEye Endpoint Security	1,052	93%	AA

Source: SE Labs Small Business Protection Jan-Mar 2020

Gartner Magic Quadrant for Endpoint Protection Platforms

Source: Gartner (August 2019)

Gartner's Magic Quadrant for Endpoint Protection Platforms is a research tool that rates vendors on completeness of vision and ability to execute. Sophos has been named a "Leader" in the Gartner Magic Quadrant for Endpoint Protection Platforms for the twelfth consecutive report. Gartner praised Sophos for our strong endpoint protection, citing customer confidence in proven anti-ransomware defenses including rollback functionality, broad endpoint detection and response (EDR) threat hunting and IT operations capabilities and centralized management of all Sophos solutions via Sophos Central.

The Forrester Wave™: Endpoint Security Suites

Forrester Research, Inc. conducts extensive product evaluations to create their report, interviewing both endpoint vendors and their customers. They evaluate vendors based on the strength of both their product and their strategy. Sophos has, once again, been named as a Leader in the Forrester Wave for Endpoint Protection Suites.

The full report is available here.

SC Magazine Review:

SC Magazine gave Intercept X full marks, describing it as:

"...a worthy, easy-to-install endpoint security solution that adds expertise by delivering enriched contextual information without adding to security team headcount."

Read the review here.

AV Comparatives

Intercept X made its first public AV-Comparatives Business Security Test appearance and ranked #1 for malware detection. We earned a 99.7% detection rate with just one false alarm in the "real world" test, and 99.9% detection and zero false alarms in the "malware" test.

	MALWARE PROTECTION RATE	FALSE ALARMS ON COMMON BUSINESS SOFTWARE
Avast, Bitdefender, Panda, Sophos, SparkCognition	99.9%	0
Cisco, Symantec, Trend Micro	99.8%	0
K7, McAfee	99.7%	0
Seqrite	99.6%	0
FireEye, Microsoft	99.5%	0
CrowdStrike, Endgame, VIPRE	99.2%	0
Kaspersky Lab	99.0%	0
Fortinet	98.9%	0
ESET	99.5%	0

Source: AV-Comparatives Business Security Test Jan-Mar 2020

PC Magazine

PC Magazine noted that Intercept X is “an excellent malware defense solution for businesses of any size.” They went on to say that it provides “excellent detection and anti-exploit functionality”, “fully integrated Endpoint Detection and Response (EDR)” and “good policy control.”

Source: https://uk.pcmag.com/software/121154/sophos-intercept-x-endpoint-protection

AV-Test (Mac)

Sophos scored a 6/6 on protection, 6/6 on performance and 6/6 for usability.

Source: https://www.av-test.org/en/antivirus/business-macos/macos-catalina/june-2020/sophos-endpoint-9.9-202105/

Intercept X Third Party Test Results and Top Analyst Reports

SE Labs

- AAA Rated for Enterprise – 100% total accuracy rating
- AAA Rated for SMB – 100% total accuracy rating
- AAA Rated for Consumer - 100% total accuracy rating

AV-Comparatives

- Ranked #1 for Malware Protection (99.9% detection, zero false alarms)

MRG Effitas

- Ranked #1 for Malware Protection
- Ranked #1 for Exploit Protection
- 100% block rate, 0 false positives 360 Degree Assessment

PC Magazine

- Editor's Choice

AV-Test

- AV-Test (macOS): Perfect Score
- AV-Test (Android): Perfect Score

Gartner

- Leader: 2020 EPP Magic Quadrant

Forrester

- Leader: 2019 Endpoint Security Wave

IDC

- Leader: 2019-2020 Enterprise Mobility Management Marketscape
- Leader: 2020 Worldwide Mobile Threat Management Marketscape

Extending Your Security: Consider Complete Protection

An endpoint security solution is just one part of an overall security strategy. Today's organizations are wise to look beyond the endpoint toward protecting the entire environment.

Ideally, a single vendor provides solutions that work together to give you consistent protection and policy enforcement throughout your organization. Working with a single vendor can provide better security, reduce administration, and lower costs.

Some specific technologies to consider along with endpoint protection include full disk encryption, mobile device management, mobile security, secure email gateway, specialized server or virtual machine protection, and Synchronized Security between endpoint and network devices.

Extending Your Security: Endpoint Detection and Response

Sophos Intercept X Advanced is the first EDR solution designed for IT administrators and security analysts to solve IT operations and threat hunting use cases. It allows you to ask any question about what has happened in the past, and what is happening now on your endpoints. Hunt threats to detect active adversaries, or leverage for IT operations to maintain IT security hygiene. When an issue is found remotely respond with precision.

Ask detailed threat hunting and IT security operations questions such as:

- Are processes trying to make a network connection on non standard ports?
- Which devices have known vulnerabilities, unknown services or unauthorized browser extensions?
- Understand the scope and impact of security incidents
- Detect attacks that may have gone unnoticed
- Search for indicators of compromise across the network
- Prioritize events for further investigation
- Analyze files to determine if they are a threat or potentially unwanted
- Confidently report on your organization's security posture at any given moment

Next Level Visibility: Extended Detection and Response

Go beyond the endpoint and server, pulling in firewall, email and other data sources. Sophos XDR gives a holistic view of your organization's cybersecurity posture with the ability to drill down into granular detail when needed.

Ask and answer questions including:

- Why is the office network connection slow?
- Are there unmanaged or unprotected devices across my estate?
- Extend investigations to 30 days without needing to a bring a device back online
- Use ATP and IPS detections from the firewall to investigate suspect hosts and devices
- Compare email header information with other indicators of compromise
- Look back 30 days for unusual activity on a missing or destroyed device

Sophos Intercept X highlights include:

- EDR combined with the strongest endpoint protection
- XDR that includes firewall, email and other data sources to give a complete picture of your environment
- Advanced, pre-written SQL queries to get the details you need
- Deep Learning Malware Analysis to replicate the role of malware analysts
- On-demand curated threat intelligence from SophosLabs
- Machine learning detection and prioritization of suspicious events
- Guided investigations that make EDR approachable yet powerful
- Respond to incidents with a single click
- 24/7 Expert Coverage: Managed Threat Response

24/7 Expert Coverage: Managed Threat Response

Sophos MTR (Managed Threat Response) supports your organization with an experienced team of threat hunters and response experts who take targeted actions on your behalf to neutralize even the most sophisticated threats. Benefits include:

- 24/7 lead-driven threat hunting
- Security health checks
- Activity reporting
- Direct call-in support and a dedicated response lead
- Advanced protection against the latest threats with Intercept X

FEATURES	INTERCEPT X ADVANCED	INTERCEPT X ADVANCED WITH EDR	INTERCEPT X ADVANCED WITH XDR	INTERCEPT X ADVANCED WITH MTR STANDARD	INTERCEPT X ADVANCED WITH MTR ADVANCED
Foundational protection (inc. app control, behavioral detection, and more)	✓	✓	✓	✓	✓
Next-gen protection (inc. deep learning, anti-ransomware, file-less attack protection, and more)	✓	✓	✓	✓	✓
EDR (Endpoint detection and response)		✓	✓	✓	✓
XDR (Extended detection and response)			✓	See note	See note
Managed Threat Response (MTR – 24/7/365 threat hunting and response service)				✓	✓
MTR Advanced (Leadless hunting, dedicated contact and more)					✓

Note: The MTR team will have the ability to leverage XDR data and functionality for MTR Advanced customers. However, MTR customers will be limited to EDR functionality in their Sophos Central console, unless they purchase an XDR license.

Evaluating Endpoint Security: Top 10 Questions to Ask

To evaluate an endpoint protection solution, start by asking the vendor the following questions:

1. Does the product rely on foundational techniques, modern techniques, or a combination of both? Which specific features are core to the technology?
2. How does the product detect unknown threats? Does it utilize machine learning?
3. For products claiming to leverage machine learning, what type of machine learning is used? Where does the training data come from? How long has the model been in production?
4. What technology exists to prevent exploit-based and file-less attacks? What anti-exploit techniques are leveraged, and what types of attacks can they detect?
5. Does the product have technology specifically designed to stop ransomware?
6. Does the vendor have third party results validating their approach?
7. Can the product ask detailed threat hunting and IT security operations questions? How long is the data retention period for searches?
8. What visibility into an attack does the vendor provide, such as root cause analysis?
9. Does the product automatically respond to a threat? Can it automatically clean up a threat and respond to an incident?
10. Does the product have the capability to let you remotely access devices to perform further investigation and take any necessary actions?

Conclusion

As cyber threats continue to grow in both complexity and number it's more important than ever to have effective protection in place at the endpoint. Understanding the threats you need to block and the different security technologies available will enable you to make an informed choice of endpoint security, and give your organization the best protection against today's attacks.

Source:
1 Seven Uncomfortable Truths of Endpoint Security, March 2019. An independent survey of 3,100 IT Managers in 12 countries, commissioned by Sophos

2 State of Endpoint Security Survey 2018

3 MRG Effitas Comparative Malware Protection Assessment, February 2018

Gartner Magic Quadrant for Endpoint Protection Platforms, Ian McShane, Eric Ouellet, Avivah Litan, Prateek Bhajanka, 24 January 2018 Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

The Forrester Wave™: Endpoint Security Suites, Q3 2019, by Chris Sherman with Stephanie Balaouras, Merritt Maxim, Matthew Flug, and Peggy Dostie, September 23, 2019

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

2021-03-21 EN (MP)

SOPHOS