SOPHOS
Cybersecurity made simple.

Cybersecurity Fit for the Future –

Why a multi-layered approach is best

A Sophos Whitepaper August 2018

Introduction

Speaking to many of our customers, it has become apparent that there is a great deal of misunderstanding about what Windows Defender ATP is and isn't, and how it is compatible with Sophos technologies. Therefore, we have provided a brief explanation of how the two complement each other.

Windows Defender ATP is designed to complement and work alongside existing antivirus and endpoint security products, including Sophos Intercept X Advanced, and acts as a last line of defence from cyber threats. Intercept X Advanced offers anti-ransomware and anti-exploit capabilities above and beyond traditional malware protection.

In terms of endpoint protection, customers need to decide whether to rely just on the built–in technologies in Windows (like Defender antivirus) or to use additional endpoint capabilities.

Almost all businesses globally, have chosen to invest in additional endpoint protection on top of the built–in capabilities in Windows. We believe Intercept X Advanced continues to be the best choice for protection, and we've set out why here.

Following testing at early adopter sites, Sophos can confirm that no issues have been found when both Windows Defender ATP and Sophos Central Endpoint Advanced and/or Intercept X have been installed on the same machine. In fact, Windows Defender ATP complements Sophos' products, with ATP providing EDR capabilities in addition to the proactive protection provided by Sophos' products.

The integrated layers of protection that Sophos delivers with Intercept X Advanced goes far beyond traditional signature-based prevention, including protection for servers and Macs. It correlates suspicious behaviours and activities using real-time threat intelligence from SophosLabs, from malicious URLs to web exploit code, unexpected system changes, and command-and-control traffic. Using our products reduces the volume of incidents reported to Defender ATP, allowing staff to focus on the truly important alerts.

Crucially, Sophos keeps you better protected by being simple to configure and manage via a single management console. This is less complex to manage than the broader Microsoft Defender range of tools, reducing the risk of misconfiguration and consequently lessening the risk of infection. If an infection does occur, the advanced, forensic system cleaning technology from Sophos works alongside Defender ATP to restore system health.

Combined with Microsoft Windows Defender ATP, Sophos products deliver the strong data and cybersecurity, so that organisations benefit from true defence-in-depth protection as recommended by the National Cyber Security Centre (NCSC).

Over the following pages, we'll provide more detail about how Sophos solutions enhance the baseline security provided within the Windows 10 E5 licensing, and complement the Defender ATP component.

Defence-in-depth

The NCSC, in its guidance on 'Mitigating Malware' (9 February 2018), makes recommendations as to how organisations can reduce the likelihood of malware infection.[1]

They state that "as there are no mitigations that are completely effective against malware infection, you should develop a defence-in-depth strategy in your organisation. This consists of multiple layers of defence with several mitigations at each layer. This will improve your resilience against malware without disrupting the productivity of your users. You'll also have multiple opportunities to detect malware, and then stop it before it has the potential to cause damage to your organisation. Accepting the fact that some will get through will help you plan for the day when an attack is successful, and minimise the damage caused."

When building defences against malware, they recommend developing mitigations in each of the following three layers

- Layer 1: preventing malicious code from being delivered to devices
- Layer 2: preventing malicious code from being executed on devices
- Layer 3: increasing resilience to infection, and enable a rapid response should an infection occur

Sophos agrees that a comprehensive, defence-in-depth strategy using layers of overlapping protection has proven to be one of the best approaches to cybersecurity, and it's no coincidence this strategy is recommended by the NCSC.

The principle of defence-in-depth is that a layered approach to security increases the overall security of the system as a whole. If one layer of protection is breached there is the opportunity for the attack to be stopped by a second or third layer.

Sophos' solution includes multiple layers of proactive and detective security to stop the machine from being breached in the first place at a pre- and post-execution level, including preventing malicious code from being delivered to devices, being executed on devices, as well as increasing resilience to infection. Defender ATP then enables a rapid response should an infection occur. This is illustrated in the diagram below which shows the layers of protection provided by Sophos at the top with Defender ATP at the bottom.

Simplicity versus complexity: keep it simple to avoid risk

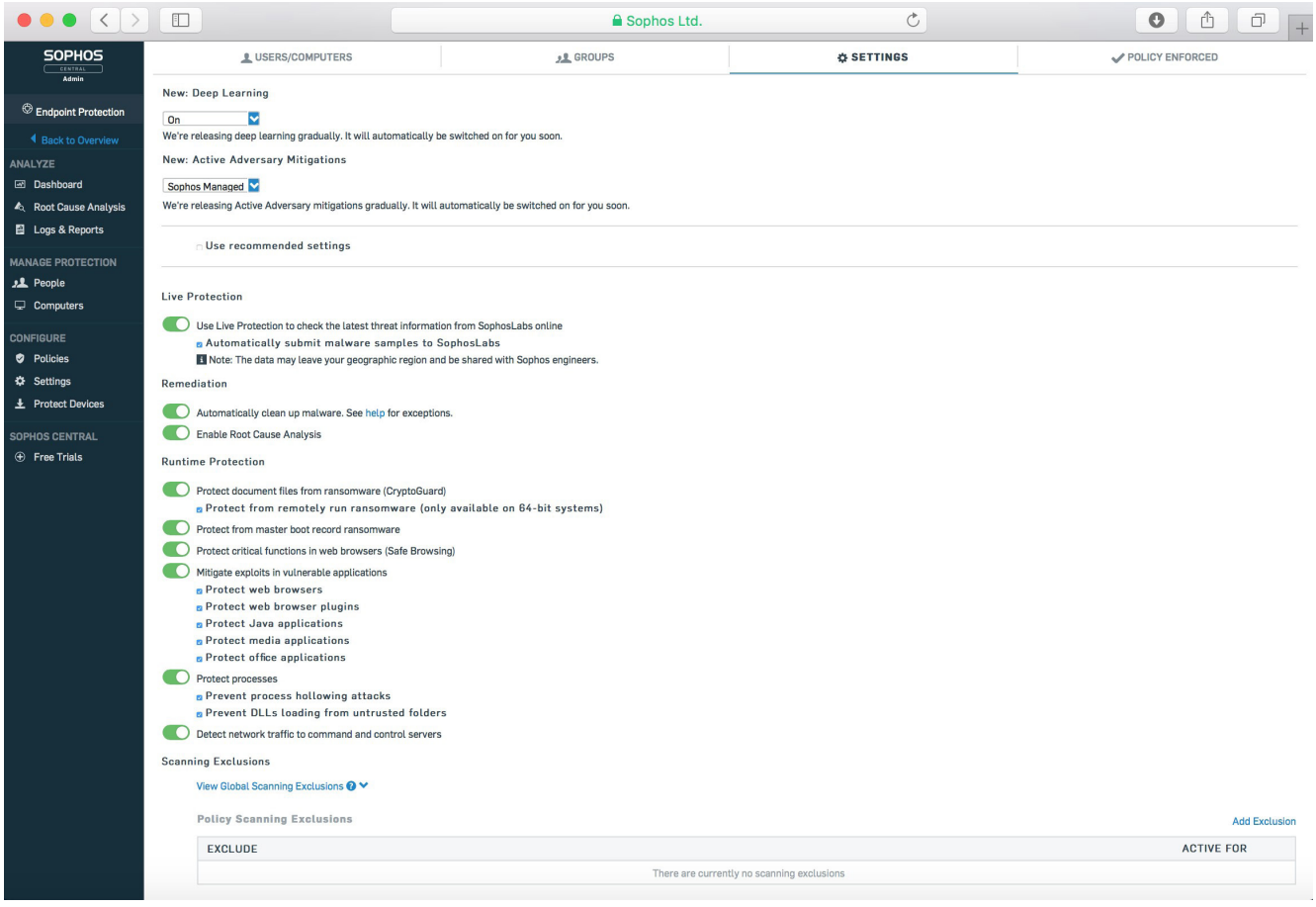
This means that systems need to be quick, simple, and easy to implement and manage, and they need to be able to work systematically to automate the tasks as much as possible, not just pumping information into logs, which are difficult to investigate and understand.

Complexity is the enemy of security and causes additional risk to an organisation. It is therefore important that security solutions are easy to deploy, configure and maintain on an ongoing basis so that management overheads are kept to a minimum.

This is where Sophos can help. Our solutions are designed to keep cybersecurity simple to manage but also provide customers with the highest possible levels of protection.

The Sophos Central-hosted management platform provides a single definitive view of the status and health of cybersecurity across your entire estate, as well as providing you with the ability to configure all policies in one place. Therefore, you have one absolute version of the truth rather than having to correlate multiple reports from different consoles – meaning more peace of mind for you.

The Sophos Central interface was designed with simplicity in mind, with most features being enabled/ disabled by simply ticking a box as shown in the image below.



The fact that Sophos Central is hosted in the cloud means that organisations don't need to maintain and update a management server. You're always running the latest version of the console, and are notified of new features upon logging in.

Additionally, you always have visibility of your devices, wherever they are located, which makes life easier for organisations who are evolving towards a mobile working culture.

Sophos Central is much more than a management platform for endpoint and server protection. It offers the opportunity for further consolidation, including the ability to manage mobile devices, Bitlocker-encrypted devices, as well as web and email protection. Sophos Central is particularly helpful in securing mobile devices and will soon also provide management of Sophos' next-generation XG Firewall solution.

Automated protection

Rapid growth of complex, coordinated threats is outpacing the ability of many organisations to protect themselves. Point products can stop individual elements of an attack, but they don't work together to protect your data, devices, and network from sophisticated, coordinated cyberattacks. At the same time, overstretched IT departments struggle to respond fast enough to these threats. This is where Synchronized Security from Sophos helps.

Synchronized Security is a security system that enables your defences to be as coordinated as the attacks they protect against. It combines an intuitive security platform with award-winning products that work together to block advanced threats, giving you unparalleled protection, automated incident response, and real-time insight and control.

Endpoint and network protection operate as one integrated security system, comprised of products that share a common interface and exchange real-time information back and forth to respond automatically to threats.

Simplified management makes the framework easy to set up and manage without additional analysts and event managers, while automated detection, isolation, and remediation results in attacks being neutralised in seconds – not hours or days.

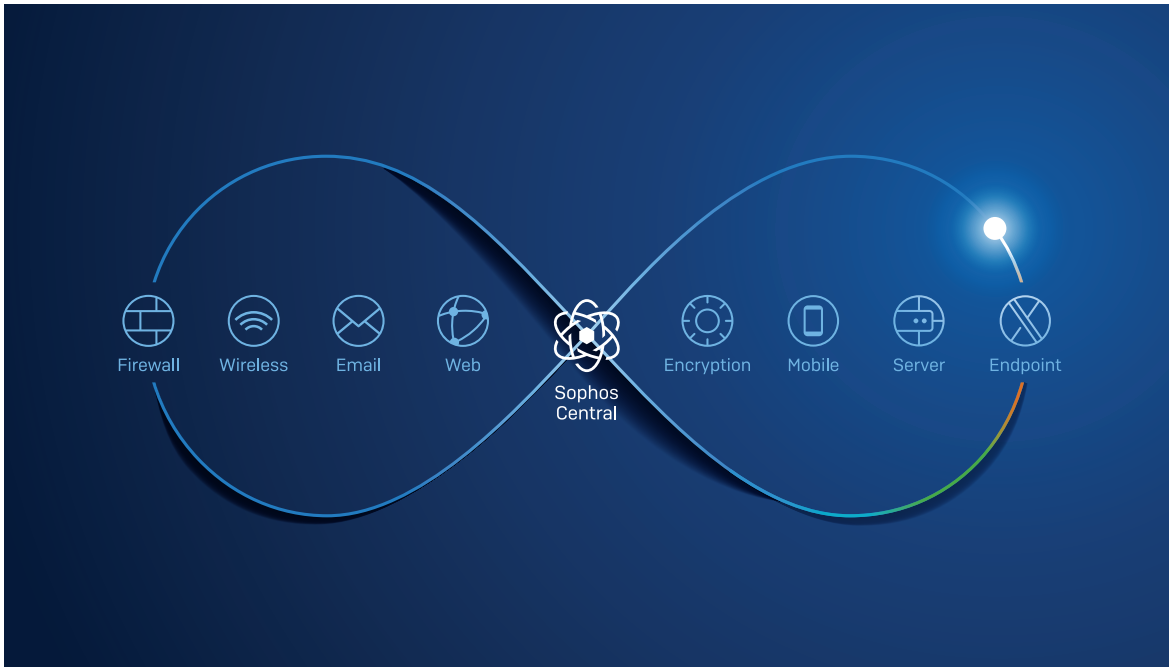
Communication between firewalls and endpoints is facilitated by the Sophos Security Heartbeat ™, an easy-to-deploy feature. Setup consists simply of entering your Sophos Central admin credentials into the Security Heartbeat section of the Sophos XG Firewall interface. Once that's been taken care of, the firewall will become visible in Sophos Central, any computers managed via Sophos Central will begin sending a Heartbeat connection to connected firewalls, and the connected firewalls will send a Heartbeat back to the computers.

Computers will automatically connect to the nearest firewall, while firewalls will check incoming connection requests from computers to ensure they're secured via Sophos Central. In turn, computers validate the firewall as well by checking that its security information matches up with Sophos Central. It all happens automatically: no complex rules, configurations, or updates.

With the firewall and endpoint clients connected, system health information begins to flow from the endpoints to the firewall via Sophos Central. On the XG Firewall dashboard, the Sophos Security Heartbeat widget indicates the health status of all your Sophos Central-managed endpoints. If any systems are running unwanted applications or are infected, they'll show here as yellow or red. Red indicators should be dealt with immediately, while yellow indicates risk but not urgency.

Firewall rules can be created to leverage changes in security status. For example, you could allow computers in yellow states to access the internet in general but block these machines from accessing sites that may contain sensitive information. In red states, with Sophos' CryptoGuard anti-ransomware technology you could automatically and instantly revoke encryption keys to mitigate data egress by advanced malware. Once remediated, the endpoint returns to a green state at which point internet access is restored.

Sophos XG Firewall is also able to detect if a previously healthy endpoint is generating network traffic without sending a Heartbeat. This could be an indication that the endpoint's malware protection has been tampered with or disabled by an intruder. Thanks to Synchronized Security and the Security Heartbeat, affected machines are clearly identified inside both the XG Firewall interface and the Sophos Central Admin interface. Machine name, logged-in user, and the process name that triggers an alert are all shared, which greatly reduces time spent investigating, detecting, and remediating threats. This could take hours or days of manual labour in traditional, protection-siloed environments where the investigator only has the transient IP network address to identify the source of the problem.



Servers almost invariably contain an organisation's most valuable data and, as such, they are highly sought-after targets for malware authors. It's important to protect servers against direct attacks, of course, but it's also imperative to protect against lateral movement from end-user computers that are connected to your servers. In the case of an attack, Sophos Server Protection can notify the XG Firewall of a change in health state, at which point the firewall can isolate the server both from the Internet and from other machines on the network to prevent data exfiltration and the possible spread of infection. Known as Destination Heartbeat, inbound connections to the server will be rejected by the firewall, and the server will be hidden from other devices on the network as well. Once remediated, network access and server visibility can be restored automatically. With two-way communication between firewalls, servers, and endpoints, Sophos Synchronized Security ensures immediate coordination to thwart the most sophisticated attacks. Automated identification and isolation of servers based on Sophos Security Heartbeat means less time spent responding to incidents. Combined with regular Heartbeat policy enforcement, this can effectively isolate a compromised system completely.

Protecting servers and systems

There are a few limitations to using Defender ATP. First, the Microsoft licensing package ATP is built into Windows 10 desktop operating systems, and can be deployed as an additional agent to Windows 7 SP1 and 8.1 devices for environments that still use older Microsoft operating systems. Also, organisations must agree to implement Defender ATP via the Service Agreement. There are some components missing organisations will want to have in terms of protection. For example, Defender does not include any protection or EDR capabilities for your all-important file servers, where critical information tends to be held, and does not protect non-Windows operating systems like Linux or Mac. The same goes for systems run from server operating systems.

The question of servers is important. Servers are different from other computing endpoints. They contain the majority of organisation-critical data, and run applications. Servers are the lifeblood of any organisation, which is why they're so appealing for attackers. An attack on your servers has the potential to create serious harm to the organisation's reputation, damage to day-to-day operations, and in the worst-case scenario, could result in potentially devastating consequences for your customers if the right systems aren't available at the right time. Plus, attackers may want to compromise those servers so they deliver malware to others.

According to Verizon's 2016 Data Breach Investigations Report (DBIR), servers are the most frequently attacked area of the network. Since users need continuous access to servers for file storage and business applications, keeping them secure, available, and performing at optimum levels is critical.

Sophos Server Protection protects both virtual and physical servers, whether running Windows, Linux, or Unix (*) operating systems. The breadth of techniques listed below enables you to blunt attacks with the most appropriate approach, whether from a known exploit, a previously unknown or zero-day attack, or a ransomware attack.

With policy-based rules for server groups, as well as application, peripheral, and web control, Sophos makes it easy to control what happens on your servers, whether they be physical, virtual, or in the cloud.

Sophos Intercept X Advanced for Server includes the following features which keep your servers protected:

- **Server lockdown**
  Intercept X Advanced for Server is the only solution that locks down your servers with a single click, securing it in a safe state and preventing unauthorised applications from running. With that click, Sophos automatically scans the system, establishes an inventory of known-good applications, and whitelists just those applications. Other whitelisting applications require the manual creation of rules to secure scripts and other system files, but Sophos manages the connections between applications and the associated files, such as DLLs, data files, and scripts.
- **Deep learning**
  The artificial intelligence built into Intercept X Advanced for Server is a deep learning neural network, an advanced form of machine learning, that detects both known and unknown malware without relying on signatures.
- **Exploit protection**
  Intercept X denies attackers by blocking the exploits and techniques used to distribute malware, steal credentials, and escape detection. This allows Sophos to ward off evasive hackers and zero-day attacks in your network.
- **Active adversary protection**
  This defends against advanced hacking techniques performed by attackers to establish their presence on a device, steal credentials, escalate privileges, or gain more enduring access, including code cave mitigation and credential theft protection.

(*) UNIX operating systems are not managed as part of the Central Environment. On-premises alternatives are available.

- **WipeGuard**
  WipeGuard provides advanced anti-ransomware protection, preventing adversaries from encrypting the master boot record.
- **Root cause analysis (RCA)**
  RCA provides detailed, forensic-level analysis. It illuminates the root causes of attacks and their infection paths, and offers guidance to help remediate infections today and bolster your security posture.
- **Malicious traffic detection (MTD)**
  MTD monitors HTTP traffic for signs of connectivity to known bad locations, such as command and control servers, an early indicator that a new piece of malware may be present.
- **Synchronized Security Heartbeat**
  Synchronized Security simplifies and unifies defences with real-time intelligence sharing between your servers and firewall, meaning that you are better protected against advanced threats and therefore spend less time responding to incidents.
- **Web control**
  Web control provides control of potentially inappropriate websites for acceptable use by site category.
- **Application control**
  Application control gives you point-and-click blocking of applications by category or by name, enabling administrators to block certain legitimate applications from running on servers.
- **Peripheral control**
  Peripheral control monitors and manages access to removable media and peripheral devices connected to your physical servers.
- **Data loss prevention (DLP)**
  DLP is designed to reduce the risk of accidental data transfer to removable storage devices, Trust web browsers, email clients and IM clients. While Microsoft offers this through document management, it relies on expensive licences and only works within Office, so information copied into Wordpad or Notepad, or uploaded through Chrome or Firefox, is not protected by Microsoft.
- **Windows firewall control**
  Firewall control monitors and controls the native firewall on Windows servers.
- **Cloud workload discovery (AWS Map View)**
  Attackers take advantage of unused cloud regions to avoid detection. Sophos discovers workloads in every public AWS region, even the ones you are not actively using.

Focus on cybersecurity: it's all we do and we do it well

Sophos is a recognised leader in the IT security market. We have a highly-differentiated strategy to deliver advanced, innovative, and extremely effective cybersecurity solutions that, at the same time, are simple and easy to manage by organisations of any size.

The need for organisations to secure their IT infrastructure and data has never been greater, and the well-publicised cyberattacks of the past year have further raised awareness.

Sophos continues to prioritise its investment in research and development as it delivers innovative new capabilities and products at a rapid pace to maintain its leadership position. We are committed to IT security and we believe we have an advantage over competitors who often seek to address disparate and unrelated areas of technology.

Our company mission statement is "to be the best in the world at delivering innovative, simple, and highly-effective cybersecurity solutions to IT professionals and the channel that serves them," and that goal is behind everything that we do.

Our industry-leading technologies are amongst the most innovative, advanced, and effective available in the market, but are simple and easy to deploy, manage, and use. Sophos believes that simple, integrated solutions deliver better security and are easier to manage for organisations of any size.

We continue to make progress on our multi-year strategy to integrate our products and enable a Synchronized Security approach for our customers. Synchronized Security delivers added protection for customers in addition to enhanced automation.

Sophos has grown rapidly in recent years, and we plan to continue prioritising investment in technology and innovation. We have a robust pipeline of exciting new product innovations, especially in our strategic pillars of next-generation endpoint, next-generation firewall, Sophos Central, and Synchronized Security.

Sophos has more than 30 years of experience and has built a portfolio of products that protect over 100 million people in 150 countries and 100,000 businesses.

But don't just take our word for it. Sophos holds the following plaudits from third parties for Intercept X Advanced:

- Gartner Magic Quadrant for Endpoint Protection Platforms 2018 – Positioned as a Leader[2]
- Gartner Magic Quadrant for Unified Threat Management 2017 – Positioned as a Leader[3]
- SE Labs AAA Certification for Endpoint Protection[4]

In addition, MRG Effitas has recently proven the effectiveness of Sophos solutions compared to others, including Microsoft, against exploits that attackers use to gain access and control over computers.

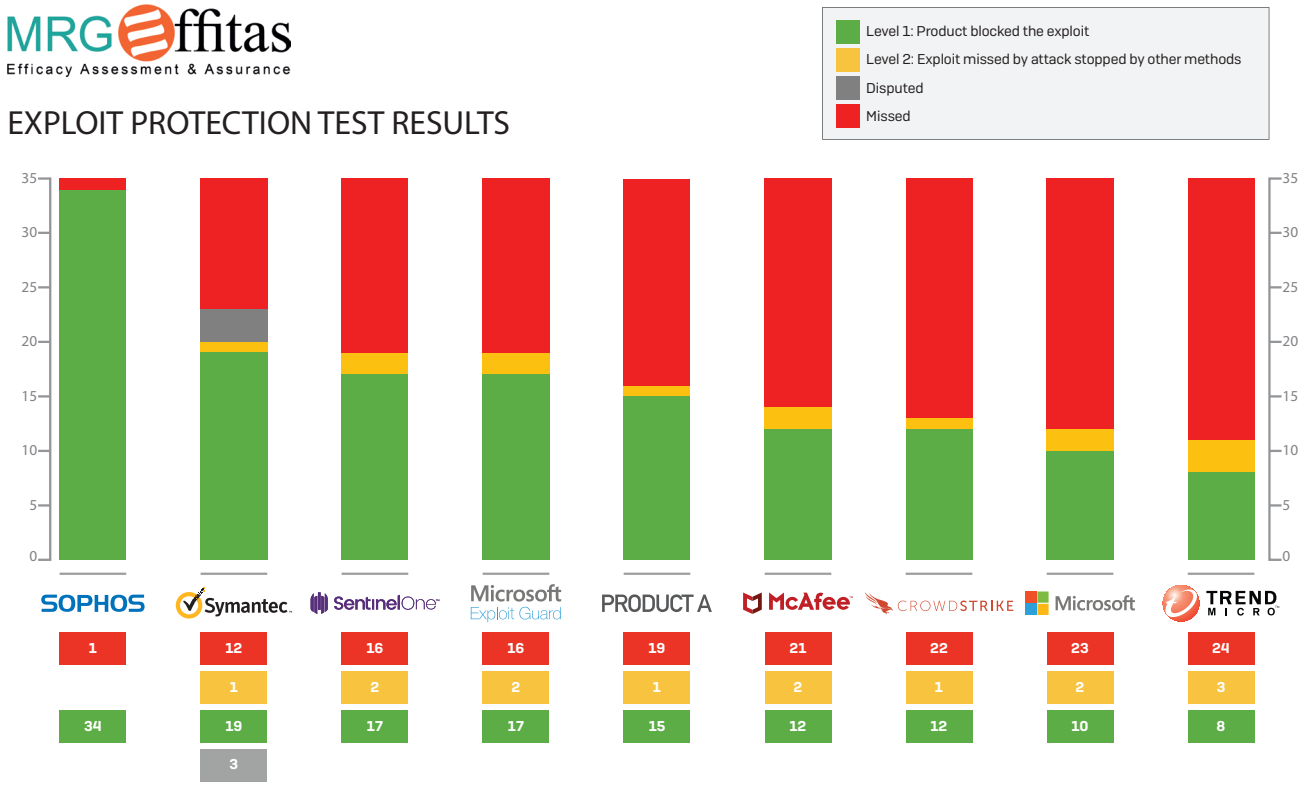
Common bugs and vulnerabilities found in popular, legitimate software can be leveraged as exploits to steal data, hold files for ransom, perform reconnaissance, or simply to deploy malware.

Attackers rely on exploits – without them, it would be like going into battle unarmed. And despite being extremely popular for attackers, many defences remain vulnerable to exploits, since the software often being exploited – Microsoft Office or Adobe Reader for example – is generally considered 'safe' by security products.

This would seem to make exploit testing a no-brainer for vendor comparison services. The problem, however, is that due to the constantly evolving nature of software vulnerabilities, exploit-based attacks are some of the most difficult scenarios to test.

Fortunately, MRG Effitas managed to develop reliable and repeatable exploit testing scenarios and has recently released its "Exploit and Post-Exploit Protection Test" report. The report compares the exploit-stopping abilities of nine different endpoint products.

As you can see in the chart below, Sophos far outperformed other vendors at stopping exploits: Level 1 means that the product blocked the exploit and Level 2 means that the exploit was missed but the attack was stopped via other methods.



Sophos blocked 34 out of 35 exploits tested, while the next highest score was 22 out of 35. In fact, most vendors weren't even able to stop half of the exploits that Sophos was able to stop.

This test was a follow-up to MRG's previous report on malware protection. In that report, Sophos ranked first for both malware protection and potentially unwanted application (PUA) protection.

To summarise the test results from the two MRG Effitas reports:

- Sophos is ranked #1 in exploit prevention
- Sophos is ranked #1 in malware protection
- Sophos is ranked #1 in potentially unwanted application prevention

For further details on this important anti-exploit report, visit here: https://secure2.sophos.com/en-us/security-news-trends/ reports/mrg/exploit-protection.aspx

Should you require assistance, our 24/7/365 telephone support means that when you call you will be speaking to an engineer who knows and understands our products and has access to our world-class SophosLabs threat researchers and data scientists.

Source:

1 National Cyber Security Centre 'Guidance - Mitigating Malware': https:// www.ncsc.gov.uk/guidance/mitigating-malware; National Cyber Security Centre's 'Guidance - 10 Steps: Malware Prevention', published on 8 August 2016: https://www.ncsc.gov.uk/guidance/10-steps-malware-prevention

2 Magic Quadrant for Endpoint Protection Platforms, Gartner Research Note G00325704, Ian McShane, Eric Ouellet, Avivah Litan, Prateek Bhajanka, 24 January 2018, https://www.gartner.com/technology/media-products/newsletters/sophos/1-49ZKXG7/gartner.html

3 Magic Quadrant for Unified Threat Management (SMB Multifunction Firewalls), Jeremy D'Hoinne, Rajpreet Kaur, Adam Hils. 20 June 2017 https://www.gartner.com/technology/media-products/newsletters/sophos/1-430JRBG/index.html

4 SE Labs Enterprise Endpoint Protection, January-March: https://selabs.uk/download/enterprise/jan-mar-2018-enterprise.pdf

5 MRG Effitas Comparative Exploit Protection Assessment: https://secure2.sophos.com/en-us/security-news-trends/reports/mrg/exploit-protection.aspx

Try Sophos Endpoint Protection now for free.

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

2018-08-07 WP-UKI (PC)

SOPHOS