Endpoint Competitive Overview

Sophos Advantages

- Award-winning endpoint protection with artificial intelligence and EDR delivers unmatched defense against malware, exploits, and ransomware
- Sophos Central provides unified management of endpoint, server, firewall, mobile, data, email, and wireless security
- Synchronized Security enables real-time intelligence sharing across product portfolio to better protect against advanced threats

Key competitors and products

Broadcom Symantec (Endpoint Security, SEP Cloud)

Key weaknesses

- Disjointed management – still in the process of moving towards a fully featured cloud management console
- Limited exploit prevention capabilities and no specific anti-ransomware technology
- Ownership woes – Broadcom has a history of buying tech companies, drastically cutting costs, and selling to only the largest customers

Watch out for

Symantec has a broad feature set and is a leader in the 2019 Gartner Endpoint MQ

Trend Micro (Apex One, Worry-Free)

Key weaknesses

- Multiple products are required to benefit from all features
- Separate components, consoles – plug-in-based architecture requires additional downloads, product activations, installs and disparate management consoles
- Server protection (Deep Security) is an expensive uplift

Watch out for

Endpoint license suites include multiple products and are often aggressively priced

Carbon Black (Endpoint Standard)

Key weaknesses

- Lacks machine learning anti-malware protection
- Few tools to prevent exposure to threats (no web protection, application control or device control)
- Lacks automated rollback, limited exploit prevention

Watch out for

'Live Response' feature for remote connection to client machines

CrowdStrike (Falcon Prevent, Falcon Insight)

Key weaknesses

- Threat exposure – lacks tools to prevent exposure to threats (no web protection or application control)
- Anti-exploit, anti-ransomware, and machine learning capabilities are less comprehensive than Intercept X
- Expensive – per Gartner, CrowdStrike licenses are expensive and products are rarely sold without accompanying services

Watch out for

CrowdStrike comes from a threat response background and offers granular EDR capabilities

Microsoft (Defender Antivirus, Defender ATP)

Key weaknesses

- Management and reporting split across several consoles
- Windows 10 focused – reduced protection on other Windows platforms, Mac, and Linux machines
- Complex configuration – Some features are centrally managed, others like Exploit Guard require manual deployment

Watch out for

Customers may be entitled to use endpoint protection features through their existing corporate Microsoft license

SentinelOne (Endpoint Protection)

Key weaknesses

- Lacks tools to prevent exposure to threats (no web protection or application control)
- Clean up – cannot clean existing infections
- Endpoint centric – no complimentary security products

Watch out for

Has a rollback capability to revert files to their pre-infected state

This comparison and information document is based on the Sophos interpretation of publicly available data as of the date of preparing this comparison. This document has been prepared by Sophos and not the other vendors listed herein. The features or characteristics of the products under comparison, which may have direct impact on the accuracy and/or validity of this comparison, are subject to change. The information contained in this comparison is intended to provide broad understanding and knowledge of factual information of various products and may not be exhaustive. Anyone using the document should make their own decision based on their requirements and should also research original sources of information and not rely only upon this comparison while selecting any product. Sophos makes no warranty as to the reliability, accuracy, usefulness, or completeness of this document. The information in this document is provided "as is" and without warranties of any kind either expressed or implied. Sophos retains the right to modify or withdraw this document at any time. This document is confidential and intended for private circulation to Sophos internal personnel and authorized partners only, and may not be disclosed to unauthorized third parties. Partners may use this comparison only if it is permitted in their jurisdiction and must use the most up- to-date version. - Copyright 2020 Sophos Group. All Rights Reserved.

MAY 2020

SYNCHROWORKS CONSULTING

SOPHOS

ESET (Endpoint Protection)

Key weaknesses

- Cloud console available for a maximum of 250 devices, otherwise on-prem console is required
- No app control; anti-exploit and anti-ransomware features are only a subset of those available in Intercept X
- Management complexity – an admin must work with ‘Tasks’ and ‘Triggers’ to perform common actions

Watch out for

ESET often performs well in 3rd party tests

McAfee (Endpoint Security, MVISION Endpoint)

Key weaknesses

- The McAfee ePO console has a steep learning curve
- Features such as EDR, device control, and application control require customers to deploy and manage additional products
- Limited exploit and file-less prevention capabilities, and no specific anti-ransomware technology

Watch out for

Most McAfee products can be managed through the ePO administration console

BlackBerry Cylance (Cylance PROTECT)

Key weaknesses

- Heavily focused on file-based malware; no web protection and limited exploit prevention
- Infrequent participation in 3rd party testing
- Lengthy deployment – recommends multi-day deployment by its professional services to reduce false-positive detections

Watch out for

Machine learning is key to CylancePROTECT and Cylance helped raise the profile of this protection technology

Webroot (SecureAnywhere Endpoint Protection)

Key weaknesses

- Few tools to reduce threat exposure (no web control, application control or device control)
- Anti-exploit and anti-ransomware capabilities are less comprehensive than Intercept X
- Limited participation in 3rd party testing

Watch out for

Webroot has a strong presence in the Managed Service Provider (MSP) market

Kaspersky (Kaspersky Endpoint Security)

Key weaknesses

- Limited cloud management – ‘Endpoint Security Cloud’ is designed for SMBs, and lacks the granularity of its on-premise counterpart – ‘Security Center’
- Limited anti-exploit and anti-ransomware capabilities – e.g. ‘Remediation Engine’ can remove newly created malicious files during a ransomware attack but is unable to roll back existing files and documents that may have been encrypted
- Kaspersky EDR requires its own management console (separate from Security Center and Endpoint Security Cloud), and is primarily designed for trained security analysts

Watch out for

Broad endpoint feature set – In addition to security configuration, the Security Center on-premise console enables administrative tasks, such as client operating system installs and remote connections to client machines, to be performed

This comparison and information document is based on the Sophos interpretation of publicly available data as of the date of preparing this comparison. This document has been prepared by Sophos and not the other vendors listed herein. The features or characteristics of the products under comparison, which may have direct impact on the accuracy and/or validity of this comparison, are subject to change. The information contained in this comparison is intended to provide broad understanding and knowledge of factual information of various products and may not be exhaustive. Anyone using the document should make their own decision based on their requirements and should also research original sources of information and not rely only upon this comparison while selecting any product. Sophos makes no warranty as to the reliability, accuracy, usefulness, or completeness of this document. The information in this document is provided "as is" and without warranties of any kind either expressed or implied. Sophos retains the right to modify or withdraw this document at any time. This document is confidential and intended for private circulation to Sophos internal personnel and authorized partners only, and may not be disclosed to unauthorized third parties. Partners may use this comparison only if it is permitted in their jurisdiction and must use the most up- to-date version. -

MAY 2020