SOPHOS

CONFIDENTIAL – SOPHOS INTERNAL AND CHANNEL PARTNERS ONLY - DO NOT REDISTRIBUTE

SYNCHROWORKS CONSULTING

COMPETITIVE INTELLIGENCE

SYMANTEC (BROADCOM) ENDPOINT BATTLECARD

Vendor Profile

Symantec was one of the world's largest software vendors. Since late 2019 it is part of technology vendor Broadcom. It offers a broad product portfolio, including endpoint protection, DLP, encryption, web gateway, and systems management.

Note: Symantec products and services are currently being integrated into the Broadcom portfolio. Therefore, names and SKUs are likely to change and make some of the information in this battlecard out-of-date sooner than normal.

Product	Description	Sophos Equivalent
Symantec Endpoint Security (SES)	Anti-malware software installed on client machines. The latest version can be managed through a cloud console. The product is also referred to by its previous name, SEP.	Intercept X Advanced
Integrated Cyber Defense Manager (ICDm)	Cloud-hosted admin console for managing SES clients.	Sophos Central
SEP Manager (SEPM)	Traditional on-premise management console for managing SEP 14 and older versions.	Sophos Enterprise Console
SEP Cloud (SEPC)	Endpoint protection targeted at small businesses. It provides fewer management options and features than the enterprise SES or SEP product.	Sophos Central Endpoint / Intercept X

Competitor Strengths

Broad feature set – Along with core anti-malware defense, Symantec offers various protection features such as web filtering, device control, IPS, and a client firewall.

Brand awareness and market share – The company is well known and has a large market share.

3rd party test results – Symantec often achieves strong results in 3rd party tests and analyst reports.

Competitor Weaknesses

Unified management – Symantec is still transitioning to a cloud platform. However, there are still some products and technologies that require separate management.

Reduced protection against ransomware – Symantec lacks behavioral anti-ransomware technology equivalent to CryptoGuard and WipeGuard.

Lacks web control – Symantec endpoint security has no built-in web control to restrict web browsing and reduce the risk of visiting unapproved site. Similar functionality requires additional products or services.

Why Sophos Wins

Unified management
Sophos Central minimizes administration by enabling customers to manage multiple Sophos products from a single intuitive cloud console.

Ransomware protection
Along with strong proactive protection, Intercept X uses behavioral detection and automatic rollback to deliver industry-leading defense from ransomware.

Focus on partners and customers
Sophos focuses on delivering the best experience for customers and partners, particularly in the underserved midmarket.

Endpoint License Comparison

		Sophos					Symantec		
		Endpoint Protection Advanced	Endpoint Exploit Prevention	Central Endpoint Protection	Intercept X Advanced	Intercept X Advanced with EDR	Endpoint Protection Cloud (SEPC)	Endpoint Security Essential	Endpoint Security Complete
PREVENT	Web Security	✓	✗	✓	✓	✓	✓	✓	✓
	Web Control / Category-based URL Blocking	✓	✗	✓	✓	✓	✗	✗	✗
	Device Control	✓	✗	✓	✓	✓	✓	✓	✓
	Application Control	✓	✗	✓	✓	✓	Path based	✗	✓
	Data Loss Prevention	✓	✗	✓	✓	✓	✗	✗	✗
	Exploit Prevention	✗	✓	✗	✓	✓	✓	✓	✓
	Active Adversary Mitigations (e.g. Credential theft protection)	✗	✓	✗	✓	✓	✓	✓	✓
	Machine Learning	✗	✗	✗	✓	✓	✓	✓	✓
DETECT	Malicious Traffic Detection (MTD)	✓	✗	✓	✓	✓	✓	✓	✓
	Behavioral Ransomware Protection & Rollback	✗	✓	✗	✓	✓	✗	✗	✗
RESPOND	Synchronized Security with Heartbeat	✗	✗	✓	✓	✓	✗	✗	✗
	Endpoint Detection and Response (EDR)	✗	✗	✗	✗	✓	✗	✗	✓

Feature Shoot-Out

	Sophos	Symantec	See these **Detailed Comparison** sections for more info
Behavioral ransomware protection and rollback	✓	✗	'Ransomware Protection'
Synchronized Security	✓	✗	'Synchronized Security'
Unified cloud management console	✓	✗	'Management'
Fully integrated endpoint detection and response (EDR)	✓	✗	'Endpoint Detection and Response'
Built-in web control and DLP	✓	✗	'Web Control', 'Data Loss Prevention'
Category- and name-based application control	✓	✗	'Application Management'
Protect Windows, Mac and Linux devices via a single console	✓	✗	'Multi-Platform Management'

Third Party Views

	Comments	Context
Gartner	Symantec was placed in the Leaders quadrant of the **2019 Magic Quadrant for Endpoint Protection.** The report highlights the addition of machine learning and other protection features.	Sophos is also a Leader. Gartner cautions that "Broadcom's goals may not align with Symantec's customers' aspirations for the products" and "Symantec [EDR] lacks guided investigation tips or contextual information, which makes it difficult to use for mainstream buyers."
AV-Test	Symantec receives strong Windows scores in **AV-Test**	Sophos also achieves strong AV-Test scores, not only for Windows, but also for macOS. Symantec does not participate in the macOS tests.
SE Labs	Symantec has performed well in recent **SE Labs Enterprise tests**, achieving the 'AAA' rating and earning the 'Best Enterprise Endpoint' award for 2019.	Sophos Intercept X Advanced has also achieved the 'AAA' rating and earned the 'Best SMB Endpoint' award for 2019.
NSS Labs	Symantec received the 'Recommended' rating in the **2019 Advanced Endpoint Protection test**, but it received significantly lower scores than Sophos in security effectives at a higher total cost of ownership.	Nineteen vendors participated in this test and Sophos had the best protection and the lowest total cost of ownership.

Watch Out For

Strong results in third party tests
Symantec often achieves strong scores from analysts and test organizations like Gartner and AV-Test. Of course, so does Sophos.

Single agent and console
Symantec promotes its single client and management console. It is true that many endpoint features do use the same agent, but note that supplemental features require additional deployment or management (e.g. EDR needs an additional appliance and console, Web control is also separate).

Isolation, Deception, Defense for Active Directory
Symantec offers optional features and products around endpoint security. 'Application Isolation' limits the actions low reputation applications can perform, while 'Deception' involves decoys being deployed to client machines. 'Threat Defense for Active Directory' monitors a customer's AD structure for signs of attack. These are all advanced tools that are potentially powerful but require extensive expertise to deploy and manage.

Detailed Comparison

	How Sophos does it	How Symantec does it	How we win
Machine Learning	Intercept X's deep learning model detects unknown malware and potentially unwanted applications. The model can take a file, extract millions of features, run it through the host-based model, and determine if it is malicious before it executes. It does all of this in about 20 milliseconds with a model that is under 20MB in size. Our machine learning experience began as part of a 2010 DARPA project, and we have proven high speed, low impact performance.	Symantec Endpoint Security includes machine learning technology for pre-execution analysis of files. Clients have 3 machine learning models at any given time, with a new one deployed every few weeks (at which point the oldest model is removed). Different levels of confidence are assigned to each model, with the oldest being the most trusted. It is an unusual approach as normally there is no reason why a newer model should not be more accurate than an older model, as it has been trained using more data and the latest threats. This approach hints at possible concerns over the precision of the machine learning models.	Proven effectiveness Data science leadership **Show:** Our extensive data science publications on our website. **Show:** The NSS Labs Advanced Endpoint Protection report, in which Symantec allowed through 4x as many threats as Sophos.
Exploit Prevention	Sophos anti-exploit technology protects against the techniques that attackers may use to exploit a software vulnerability. Intercept X delivers more than 25 exploit prevention techniques to ensure protection against attacks that leverage previously unknown vulnerabilities. Intercept X also uses an unused hardware feature in mainstream Intel processors to track code execution and augment the analysis and detection of advanced exploit attacks at run time.	SES has a Memory Exploit Mitigation module. Along with enforcing pre-existing OS features (e.g. DEP and SEHOP), it also has techniques to protect against other attacks (e.g. ROP exploits). SES has fewer than 15 exploit prevention techniques, whereas Intercept X delivers more than 25. We use our own Java protection, dynamic heap spray mitigation, and SEHOP protection techniques, rather than relying on operating system settings which can be identified and compromised by attackers.	Depth of exploit protection **Show:** Share the Exploits Explained whitepaper, which details our protections. Compare to Symantec's less-thorough KBA.
Ransomware Protection	CryptoGuard technology **detects ransomware through its behavior**, stopping it from encrypting files, and then automatically **rolls back** any files that were encrypted before detection. WipeGuard protects from attacks that encrypt the MBR and render the machine unable to boot into the operating system.	**Behavior**- SES does not have a specific anti-ransomware feature. Instead, Symantec highlights its other protection features (e.g. machine learning, IPS rules) as ways to detect ransomware. **Roll-back**- SES cannot roll back file or MBR changes if an attack gets past the initial defenses and begins to run.	Purpose-built anti-ransomware technology **Show**: CryptoGuard is enabled through a simple checkbox, and no configuration is required. Demonstrate using the Sophos Tester tool.

Detailed Comparison

	How Sophos does it	How Symantec does it	How we win
Endpoint Detection and Response (EDR)	Intercept X Advanced with EDR suits both IT administrators and security analysts. While it is accessible to IT generalists by replicating tasks normally performed by skilled analysts, it also provides the core manual tools that trained analysts would expect. Threat Visibility: Deep Learning Threat Indicators and Analysis For the grey area between known-good and known-bad, deep (machine) learning prioritizes a list of suspicious files for further investigation. The comprehensive file analysis report enables customers to quickly determine if a suspicious file should be blocked or allowed. Threat Hunting: Live Discover search: Allows customers to quickly discover IT operations issues or to hunt down suspicious activity. - Flexible: Includes out-of-the-box, fully customizable SQL queries. Customers can create completely new, custom queries. - Comprehensive: Provides up to 90 days fast access to current and historical on-disk data. Data includes insight into artifacts' reputation and machine learning scores from SophosLabs and Sophos AI. Response Automatic response – The intelligent Sophos endpoint agent can automatically clean up or block threats. It is also capable of isolating the endpoint. Live Response command line: Customers can remotely access devices via a native command line to perform further investigation, install and uninstall software, or remediate any issues that Intercept X cannot address automatically. It can also be used for IT operational actions such as rebooting or installing and uninstalling software.	Symantec has two separate EDR components that are not well integrated. On-Premises Formerly known as ATP:Endpoint, the on-prem EDR solution uses the SEP agent along with a separate management appliance and console. It is a full-featured solution for trained enterprise security teams. It does not work with the cloud-managed version of Symantec Endpoint Security. Cloud The "agentless" EDR solution monitors network data to identify compromised endpoints. It uses an on-prem server to collect the data and send it to the cloud. Threat investigators can deploy a "dissolvable" agent to further investigate specific endpoints. The console for this is separate from both the SES console and the on-prem EDR console. Threat Visibility Files can be submitted to a sandbox and the results inspected. However, the data is presented in text format and less extensive compared to Sophos Threat Indicators and Analysis. Threat Hunting You can search the Symantec EDR database (Kibana based) of collected data using the Lucene Query Syntax (LQS). There is no way to directly query live data on endpoints. There are readymade queries and you can write your own. Response Response is performed from the management console from a list of predefined actions. There is no remote terminal option for precise, custom response actions.	Single cloud hosted management console Adds expertise, not headcount Ask: What resources do you have available to dedicate to threat hunting and investigation? Ask: What would it save you in time and money to avoid deploying on-prem appliances or servers and managing multiple consoles? Show: Demonstrate the Threat Analysis Center in Sophos Central.
Synchronized Security	With Synchronized Security, products communicate with each other both across the network and on endpoints to mitigate risks and stop data loss. Security information is shared and acted on automatically, isolating infected endpoints before the threat can spread and slashing incident response time. Synchronized Application Control also provides unprecedented visibility into network traffic.	Symantec Integrated Cyber Defense Exchange (ICDx) is a set of APIs and tools for interconnecting Symantec and third-party products. It has some useful integrations, particularly around enterprise DLP. However, ICD requires additional components and sometimes manual integration, unlike our turnkey Synchronized Security. ICD does not yet offer the level of automated remediation and endpoint-network communication provided by Synchronized Security. Symantec Advanced Threat Protection (ATP) is a hardware or virtual appliance consisting of four separate modules: Network, Endpoint, Email, and Roaming. Each requires its own license. The four modules work together to provide detection & response across the environment. However, there's little in the way of automation, and no equivalent to Synchronized Application Control. Further, ATP:Endpoint (also known simply as EDR) is only for on-prem SEP customers and uses a separate console from SEP.	Simple setup, powerful features Show: Enable Synchronized Security within a matter of clicks and demonstrate the XG Firewall automatically isolating a compromised endpoint client and providing Synchronized App Control.

Detailed Comparison

	How Sophos does it	How Symantec does it	How we win
Management	**Sophos Central** Sophos Central provides one place to manage endpoint, mobile, encryption, email, server, and wireless security. Using a consolidated management platform, customers benefit from security intelligence sharing, policies that follow users, easy configuration, detailed and summary reporting, and automatically prioritized alerts.	**Integrated Cyber Defense Manager (ICDm)** Symantec ICDm is a relatively new cloud management console that strives to bring together Symantec products. At this time, it is fairly limited in the products it can manage. Some other cloud products are available through single sign-on in other consoles. **SEP Cloud (SEPC)** This product is marketed to SMBs with 5+ users by Norton LifeLock and aims to provide a simplified interface. Minimal configuration options are provided to the customer; for example, device control settings allow high level Read Only or Block options but do not provide the option to specify particular device types or models. This may limit the real-world usefulness of the feature. Additional integrations like EDR or ICDx are not available in SEPC.	Intuitive management console **Ask:** If your main administrator were unavailable, how easy would it be for other staff to understand and use the console in their absence? **Show:** Get Sophos Central in front of the prospect, either in person, as a trial, or with the online demo. Nothing speaks to our strengths as strongly as seeing the product firsthand.
Web Control	Sophos Endpoint provides integrated web control. This allows administrators to easily block endpoints from accessing inappropriate sites such as adult, gambling, hate, or crime sites.	Web control is not included in Symantec Endpoint Security. Although it is possible to manually create firewall rules to block specific websites, there is no simple method to block categories of sites. Instead, Symantec recommends that customers buy either Symantec Web Security Service or Symantec Web Gateway. The former redirects traffic from roaming users to the SWSS and Symantec CASB using a PAC file. Alternatively, Symantec Web Gateway is an on-prem appliance that integrates through REST APIs. Both products are more complex and costly than the built-in web security and control in Sophos' endpoint.	Prevent users accessing inappropriate websites **Ask:** Do you need to demonstrate compliance with company policies on responsible internet usage? **Show**: Create a policy to block access to social media sites.
Device Control	Sophos enables administrators to define which storage devices or network interfaces to block, set to read only, or allow full access to. It is simple to set exceptions for specific devices by choosing from a list of detected devices.	SES Complete offers device control as an optional add-on. Administrators can block or allow devices by manually specifying device details or selecting from a list of devices discovered in their environment. SEPC has only limited Device Control.	**Ask:** How do you currently control which devices are allowed on your network? How much time do you spend tuning this?
Data Loss Prevention	Basic DLP is integrated into Sophos endpoints. No additional plugins are required, and it is simply enabled and configured in the endpoint policy. There are a large set of predefined detection rules for common data types, and, if required, customers can build their own custom rules using regular expressions.	A DLP product is sold separately. This product has extensive capabilities and integrations with other Symantec products, including SES. However, it requires separate deployment and complex management and will incur additional acquisition and maintenance costs.	Simple DLP built-in to endpoint protection **Ask**: What measures do you have in place to prevent important data leaving the organization? How much time do you have available to manage these measures?
Application Control	Administrators can control installation, track usage, or block execution of more than 1000 applications within a few clicks using a applications list maintained by SophosLabs. Once the selection of controlled applications or categories has been made, no further maintenance is required. Sophos application control effectively reduces the risk of data loss and assists employee productivity while keeping administrative effort to a minimum.	**Symantec Endpoint Security (SES)** Administrators create rules based on applications discovered in their environment or using conditions such as the path or certificate of an application. Although this allows granular control, it requires more work for the customer than simply selecting from a pre-populated list of categories and applications.	Quickly define applications to block on client machines **Show**: Demonstrate how easy it is in Sophos Central to create a policy that blocks file sharing tools such as BitTorrent.
Multi-Platform Management	In Sophos Central, you can manage all endpoints using the same easy-to-use controls, regardless of whether they run Windows, Mac, or Linux.	**Symantec Endpoint Security (SES)** Windows and Mac clients can be managed through the cloud console, but Linux machines can only be protected via an on-premises installation of SEP Manager. Alternatively, the customer would need to use Symantec's separate server product Cloud Workload Protection.	Protect Windows, Mac and Linux from the same cloud-hosted console

Detailed Comparison

	How Sophos does it	How Symantec does it	How we win
Server Protection	Fully integrated solution Advanced protection features such as deep learning, exploit prevention, and anti-ransomware are coupled with server specific capabilities such as cloud workload discovery, server lockdown, file integrity monitoring, and automatic scan exclusions. Server Protection is managed through the same Sophos Central console as endpoint protection, encryption, mobile and more.	**Management overhead** Although Symantec Endpoint Security can be installed on server platforms, it does not offer server specific settings or features. Instead, Symantec offers a dedicated server product called Symantec Cloud Workload Protection, which focuses on locking down servers in AWS and Azure environments. The predecessor to this product, Symantec Data Center Security, is also available but is installed on-premises. Both Symantec Cloud Workload Protection and Data Center Security are managed separately from Symantec Endpoint Security, meaning more administrative effort for the customer.	Advanced server features without using a separate product Ask: Are the same people managing protection for your workstations and servers? How would it help to have workstation and server policies and reporting integrated in a single console? Show: Trigger one-click lockdown on a server. Show: Demonstrate file integrity monitoring.
Protection for Virtual Machines	Hypervisor agnostic Sophos for Virtual Environments (SVE) is specifically designed for virtualized environments, providing centralized scanning, malware protection, customer defined file exclusions, advanced caching, and clean up. SVE supports Hyper-V and VMware hypervisors. Thin agent or full agent options SVE uses a thin agent installed on guest virtual machines to provide optimized performance. Alternatively, if customers prefer our complete next-gen feature set, the full Sophos Endpoint agent can be installed and managed from Sophos Central in the normal way. Simple licensing Sophos provides simplified licensing by including SVE in Intercept X for Server or on-prem Server Protection licenses. Customers can mix and match between the supported hypervisors with the appropriate license.	**SES for virtual machines** SEP has two features specific for virtual machines, both of which are only available via an on-premises installation of the SEP Manager console. The 'Shared Insight Cache' allows virtual machines to skip scans for files that are known to be clean. The 'Virtual Image Exception' tool enables customers to bypass scanning on the base image of a virtual machine. Virtual desktop infrastructure (VDI) Symantec also offers a bundle of Symantec Endpoint Protection and Symantec Data Center Security, designed for VDI environments. The SEP agent is installed in Hyper-V and KVM environments, whereas VMware and Citrix environments can achieve agentless protection via a virtual appliance that caches scan results. SEP and Data Center Security are two separate products that the customer would need to set up and maintain on premises.	Lightweight agent for VMware and Hyper-V Ask: How do you plan to protect virtual machines in your environment? What would it mean to be able to manage virtual machines from the same cloud console as the rest of your security?
Managed Detection and Response	Sophos Managed Threat Response (MTR) is a fully managed threat hunting, detection and response service that provides organizations with a dedicated 24/7 security team to not only detect but neutralize the most sophisticated and complex threats. Regardless of the service tier selected (Standard or Advanced), customers can opt to have the Sophos MTR team operate in any of three Response Modes to accommodate their unique needs. - Fully managed – allows customer to effectively outsource its SOC if needed - Three operational modes – Notify, Collaborate, or Authorize - Any size customer – from SMB to enterprise - Best protection – based on Intercept X ensure maximum protection	**Symantec Managed Endpoint Detection and Response (MEDR)** services is aimed at larger enterprises that most likely already have a SOC team. While Symantec can take remediation actions, these are limited to a predefined set, mainly involving killing processes and triggering endpoint isolation. There is little by way of cleanup. A strength of MEDR is the customer portal that shows details of all incidents.	Discuss the flexibility of MTR and how it can adjust to the needs of the customer.