SOPHOS

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

SYNCHROWORKS CONSULTING

COMPETITIVE INTELLIGENCE

MCAFEE ENDPOINT BATTLECARD

Vendor Profile

McAfee is one of the largest security vendors and sells to both home and business customers. McAfee was previously entirely owned by Intel Corporation, but in 2016 it sold a 51% stake to investment firm TPG.

Product	Description	Sophos Equivalent
Endpoint Security (ENS)	Endpoint protection for Windows, Mac and Linux.	Intercept X
MVISION Endpoint	Endpoint product specifically designed to run alongside Windows Defender Antivirus. Available on Windows 10 only.	Intercept X
MVISION EDR	Endpoint detection and response product (EDR)	Intercept X with EDR
ePO (Enterprise Policy Orchestrator)	A central management tool for managing products such as Endpoint Security. Normally installed on premise, but a cloud version with reduced functionality is also available.	Sophos Central

Competitor Strengths

Unified management - Endpoint Security and ePO are highly customizable, and ePO can be used to manage most McAfee business products

Broad capabilities - Can offer most common endpoint protection features

Established brand - McAfee is a widely known brand among businesses and consumers alike

Competitor Weaknesses

Management complexity - The ePO management console is complex, time consuming and targeted towards large enterprises

Separate products – Features such as EDR, device control and application control are not part of the endpoint security product, and instead require the customer to deploy and manage additional products.

Low customer satisfaction - Feedback indicates frustration with the quality of products and the level of protection received

Why Sophos Wins

Simple
We focus on providing complete peace of mind. Sophos Central is easy and intuitive to use. With McAfee, the customer must do the work of tying products together. Complexity is the enemy of security and can lead to misconfiguration and holes in protection.

Complete
Sophos provides complete protection in an integrated endpoint agent. Additional protection technologies can be enabled with minimal effort, and do not require the installation and management of separate components.

Advanced Threat Protection
Combining Endpoint Protection Advanced and Intercept X layers next-generation anti-exploit, anti-ransomware, root cause analysis and advanced system clean on top of best in class anti-malware.

Endpoint License Comparison

		Sophos					McAfee		
		Endpoint Protection Advanced	Endpoint Exploit Prevention	Central Endpoint Protection	Intercept X Advanced	Intercept X Advanced with EDR	MVISION Standard	MVISION Plus	Complete Endpoint Threat Protection
PREVENT	Web Control / Category-based URL Blocking	✓	×	✓	✓	✓	✓	✓	✓
	Device Control (e.g. USB)	✓	×	✓	✓	✓	×	✓	✓
	Application Control	✓	×	✓	✓	✓	×	✓	✓
	Data Loss Prevention	✓	×	✓	✓	✓	×	×	×
	Exploit Prevention	×	✓	×	✓	✓	✓	✓	✓
	Machine Learning	×	×	×	✓	✓	✓	✓	✓
DETECT	Runtime Behavior Analysis / HIPS	✓	×	✓	✓	✓	✓	✓	✓
	Malicious Traffic Detection (MTD)	✓	×	✓	✓	✓	✓	✓	✓
	CryptoGuard Ransomware Protection	×	✓	×	✓	✓	×	×	✓
RESPOND	Synchronized Security Heartbeat	×	×	✓	✓	✓	×	×	×
	Endpoint Detection and Response (EDR)	×	×	×	×	✓	Add on	Add on	Add on

Feature Shoot-Out

	Sophos	McAfee	See these **Detailed Comparison** sections for more info
Simple management	✓	×	'Management', 'Cloud Hosted', 'Policy Model'
Comprehensive exploit protection	✓	×	'Exploit Prevention'
Detects and blocks ransomware behaviour	✓	×	'Ransomware Protection'
Synchronized Security between endpoint and gateway	✓	×	'Synchronized Security'
Integrated endpoint detection and response (EDR)	✓	×	'Endpoint Detection and Response'
Integrated device and application control	✓	×	'Application Control', 'Device Control'

Third Party Views

	Comments	Context
Gartner	McAfee remained in the 'Visionaries' quadrant of the **2019 Gartner Magic Quadrant for Endpoint Protection**. The report notes that the on-premise ePO console allows customers to manage all McAfee products.	While Gartner welcomes the MVISION cloud console, it also notes that McAfee "has been struggling to grow its EPP installed base".
SE Labs	McAfee Endpoint Security has received the AAA award in recent **Enterprise tests.**	Sophos Intercept X Advanced has consistently achieved the AAA award in the same tests and demonstrated a higher overall protection rating.
AV-Test	McAfee Endpoint Security has received generally strong scores in recent **tests**.	Note that the test focuses on Protection, Performance and Usability (false positives) rather than the administration effort and components required to deploy and manage complete endpoint protection.
Forrester	In the **2019 Forrester Wave for Endpoint Security**, McAfee was placed in the Strong Performers section.	The report also made a couple of important criticisms like; *"Mcafee is still catching up on detection efficacy compared with others in this study ".* Note that Sophos was rated a Leader in this report.
NSS Labs	Did not participate in the **2019 Advanced Endpoint Protest (AEP) test**.	Sophos Intercept X came top of this test, achieving the highest security effectiveness rating of all vendors.

Watch Out For

Manage multiple products within ePO
The on-premise ePO management console allows the majority of McAfee products to be managed from one place. However, ePO is a complex tool which can quickly become problematic unless significant time is spent on administration and maintenance.

Endpoint Security provides more features and integration than previous McAfee products
Note there are still some important features (e.g. Application Control, Device Control) which require deployment of further agents, along with associated configuration and administration. Does the customer know how many agents they will have to deploy and manage to get the full feature set they are paying for?

ePO can provide very granular control of machines and policy settings
This may be beneficial to large enterprises or customers with strict change control environments, but a complex system can quickly become unwieldy and lead to unintentional security holes. It also requires an investment of staff resources that could otherwise be used elsewhere.

Detailed Comparison

	How Sophos does it	How McAfee does it	How we win
Management	Sophos Central is intuitive and makes common tasks simple to perform. Default policies and recommended configurations ensure customers get the most effective protection from day one.	**Enterprise Policy Orchestrator (ePO)** ePO is McAfee's on-premise administration console. The interface is complex and even common tasks require the user to navigate through various screens and complete a number of steps. For example, to install Endpoint Security: 1. Download the software packages (each component is a separate package) 2. Check in the packages 3. Install McAfee Agent (which enables Client>ePO communication) on the client machine 4. Install each of the individual Endpoint Security modules The complexity of ePO means the customer needs to spend significant time learning and administering the product. McAfee recommends administrators attend training courses (at a cost).	**Intuitive management console** **No training required** **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 first hand.
Cloud Hosted	Managing security through Sophos Central means customers no longer need to install or maintain an on-premise management server. From a single web interface, customers can manage multiple protections such as endpoint and server protection, mobile management, device encryption, email and wi-fi.	**MVISION ePO** McAfee recently launched a new SaaS management console called ePO MIVISION, which is a slimmed down version of the on-premise counterpart. Being hosted in the cloud removes some administrative overhead, but there are still some key drawbacks to the product: ▪ It retains much of the traditional ePO complexity – there are multiple different policies for each product (see 'Policy Model' section below) ▪ Only a handful of products can be managed – the main ones are McAfee Endpoint Security (ENS) and MVISION Endpoint – there is no option to deploy McAfee products for encryption, device control or application control	**Unified management console** **Show**: Highlight the multiple products and features available in Sophos Central
Policy Model	Administrators can easily create and apply a security policy to Windows, Mac OS, and Linux computers in multiple groups. Settings are grouped into single, intuitive policies that require little or no expertise to use.	**Multiple policies** McAfee ePO forces complex policy creation and management, requiring multiple policies for every client. For example, just the Threat Prevention component of Endpoint Security requires 'Access Protection', 'Exploit Prevention', 'On-Access Scan', 'On-Demand Scan' and 'Options' policies. This is in addition to the policies contained within the Firewall, Web Control and other components of Endpoint Security. All this adds up to additional work for the administrator, and more chance of misconfiguration.	**Simple policy management** **Ask:** How many policies do you expect to have to manage? What would it mean to have better control over your settings? **Show:** Simple policy creation and enforcement in Sophos Central
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.	McAfee's Real Protect component uses machine learning to analyze file characteristics. It examines application code to see what it looks like and may do (pre-execution analysis) as well as monitoring what it does when running (behavior analysis).	**Proven effectiveness** **Show:** Our extensive publications on our website, Invincea NSS Labs report, invite the customer to look at historic VirusTotal feedback.
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.	The exploit prevention feature within Endpoint Security relies heavily upon McAfee issuing updates to protect against known vulnerabilities (normally after Microsoft patch Tuesday). Therefore, customers are reliant upon new vulnerabilities being identified by Microsoft, and McAfee creating and publishing timely protection. Other more generic techniques are available, including DEP and protection against some Stack Pivot attacks. However there is nowhere near the range of protection that is provided in Sophos Intercept X.	**Depth of exploit protection** **Ask:** What would it mean to you if you could run one of the industry's most comprehensive exploit protection without in-depth configuration? **Point out:** Sophos Intercept X covers more than 25 types of exploit prevention techniques

Detailed Comparison

	How Sophos does it	How McAfee does it	How we win
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.	**DAC** Dynamic Application Containment (DAC) prevents files with an unknown reputation from performing certain actions (e.g. modifying specific registry settings, deleting files). The file/application will continue to run in this mode until it is known to be either good or bad. McAfee refer to this feature as being anti-ransomware, although there is nothing specific within it that identifies ransomware behavior. To confirm whether a file is malicious, McAfee suggest sending files to the customer's McAfee ATP (sandboxing) or Active Response products (which are separate products/licensing/management/installation). If the customer doesn't have these products, endpoints continues running the application in the containment mode until the file/application is seen elsewhere and its reputation provided by McAfee Labs. The DAC feature is off by default, and McAfee suggest testing and modifying the settings (i.e. what specific actions are blocked) before applying in a live environment. Also note that DAC is a component of McAfee Endpoint Security (ENS) and therefore not available within MVISION Endpoint.	**CryptoGuard requires no configuration or additional components and is enabled by default** **Automatic roll back of affected files** **Ask:** Are you aware of the need for further McAfee products in order to make the most of the DAC feature? **Show**: CryptoGuard is enabled through a simple checkbox, and no configuration is required
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.	**Threat Intelligence Exchange (TIE)** McAfee offers the Threat Intelligence Exchange (TIE) product as an intermediary that connects different products together. The idea is that TIE can be used by different McAfee products to query the reputation of files, to determine if they have been seen elsewhere on the network (or globally) and are known to be good/bad. TIE cannot automate actions such as isolating infected machines from the network or removing encryption keys. **Additional Overhead** TIE is a Linux virtual server which operates in addition to ePO and other McAfee products such as Endpoint Security. For best overview and integration you should combine TIE with McAfee Enterprise Security Manager (SIEM) which will correlate and track historical data. This is yet another product.	**Simple setup, powerful features** **Show**: Enable Synchronized Security within a matter of clicks and demonstrate the XG Firewall automatically isolating a compromised endpoint client
HIPS	The Sophos heuristics engine examines any sample file to look for snippets of code that may indicate it will perform actions such as deleting other files, making registry changes or installing other files. Sophos Endpoint also includes an on-device emulator that detonates executables in a controlled environment. The emulator is primarily used to allow malware to uncloak and expose cyphered execution components, and to collect indicators of compromise like registry modifications and access to other files/applications.	**McAfee HIPS** McAfee also offer a separate HIPS product (not all of the features are integrated into Endpoint Security). Therefore, existing McAfee customers that are using the HIPS product would need to decide whether to lose some of the functionality or run HIPS alongside Endpoint Security (which means additional configuration and maintenance for the administrator).	**Included with Sophos Endpoint**
Application Control	Administrators can control installation, track usage or block execution of unauthorized applications within a few clicks. Administration is kept to a minimum as detection identities are automatically updated and maintained by Sophos Labs.	Application Control requires installation and configuration of a separate product called McAfee Application Control (based on the acquisition of SolidCore). This is a powerful product, but the fact that it is a separate tool means yet more configuration and administration.	**Available in Sophos Endpoint** **No additional component required** **Show**: Demonstrate how easy it is in Sophos Central to create a policy that blocks file sharing tools such as BitTorrent
Device Control	Sophos Endpoint enables customers to define which storage devices or network interfaces to block, set to read only or allow full access to. The feature is built into the endpoint agent and requires no additional installation.	McAfee Device Control is separate from Endpoint Security, meaning the customer has to install and maintain another product.	**Available in Sophos Endpoint** **No additional component required** **Show:** Demonstrate blocking USB drives, and then create an exception for a drive that was previously plugged in

Detailed Comparison

	How Sophos does it	How McAfee 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.	McAfee offers a dedicated EDR product called MVISION EDR. **Threat Visibility** MVISION EDR highlights suspicious events, and provides details on the machines, files and processes involved. More in depth analysis can be performed via 'Investigations' which provide a visual representation of the threat chain along with answers to common questions (e.g. Does the endpoint contain uncommon running processes?). Detailed threat hunting capabilities are also available. **Hunting and Management** MVISION EDR can be managed through either the on-premise or cloud ePO management console. In both cases it requires an additional endpoint client to be deployed to devices. Data is uploaded to the management server (whether on prem or cloud) and can be stored for up to 90 days. It is possible to also directly query live data on endpoints. . **Response** McAfee does not offer a command line terminal for precision response actions. The respondent can choose from a number of predefined actions such as killing the process or quarantining the file.	**Single agent** **Point out:** Sophos EDR and endpoint protection features are provided through a single agent and cloud hosted management console
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	McAfee does not offer its own MDR service to customers. Managed EDR is provided by a third-party McAfee MSP (DXC Tech). Other MSPs are expected to follow. The McAfee MSP will not have the same internal view as the Sophos MTR team and not be able to raise and hand over tickets to the technical support team if required.	