SOPHOS

CONFIDENTIAL—SOPHOS INTERNAL AND CHANNEL PARTNERS ONLY—DO NOT REDISTRIBUTE

SYNCHROWORKS CONSULTING

COMPETITIVE INTELLIGENCE

MICROSOFT ENDPOINT BATTLECARD

Vendor Profile

Microsoft has over 100,000 employees and provides a wide range of platforms for home users and businesses: Windows, Azure, Office 365, and more. It has increased its focus on security both within its existing platforms and with premium add-ons integrated into those platforms.

Product	Description	Sophos Equivalent
Defender	Refers to a range of Microsoft endpoint protection features, such as anti-malware, EDR and exploit protection.	n/a
Defender Antivirus	The antivirus engine included in all recent versions of Windows.	Central Endpoint Protection or Intercept X
Defender ATP	Optional add-on that provides cross-platform AV, EDR, and security visibility/reporting.	Intercept X w/EDR
Endpoint Manager (formerly Intune)	Cloud-based mobile device and endpoint management tool, which includes management of Defender features.	Sophos Central

Competitor Strengths

Perceived low cost—Endpoint security is built into, or bundled with, Windows and Microsoft 365

Pre-deployed agent—Antivirus and EDR agents are installed by default in Windows 10 and Server 2016/2019

Strong brand—Worldwide adoption of core platforms, such as Windows and Office

Competitor Weaknesses

Difficult to achieve strong protection—Windows 10 and Server 2019 can be configured for strong security with native tools, but only with substantial time, expertise, and attention to detail. Advanced threat protection is not default enabled as in Intercept X.

Limited support for legacy Windows and other platforms—Protection for legacy Windows versions (e.g., Windows 7, Server 2012) and other platforms like macOS lacks key features and is not fully integrated into central management.

Confusing documentation and consoles—Defender includes numerous overlapping features and consoles with ever-changing names and documentation that is difficult to find and follow.

Why Sophos Wins

Better security out of the box
Sophos' industry leading prevention features, such as anti-ransomware and anti-exploit, are simply on by default, therefore setting a higher security baseline. In contrast, Microsoft recommends against deploying many of its anti-exploit features by default due to a high risk of compatibility and performance issues.

Lower total cost of ownership (TCO)
Every aspect of Microsoft's endpoint security, from configuration to management to incident response, requires more expert-level, hands-on work than the Sophos equivalent. This increases cost to the customer and puts added strain on already-stretched IT and security teams.

True cross-platform security
Sophos Central provides complete, centralized management and visibility across a broad range of platforms. Beyond added depth in macOS and legacy Windows versions, Central offers integrated and synchronized protection for network, mobile, cloud (AWS, GCP, *and* Azure), wireless, email, and more.

Endpoint License Comparison

		Sophos			Microsoft	
		Central Endpoint Protection	Intercept X Advanced	Intercept X Advanced with EDR	E3	E5/ATP
PREVENT	ML-based malware protection for Windows	✓	✓	✓	✓	✓
	Web Category Filtering	✓	✓	✓	✗	Windows only
	Category Based Application Control	✓	✓	✓	✗	✗
	Exploit Prevention	✗	✓	✓	✓	✓
	Malware protection for macOS	✓	✓	✓	✗	✓
DETECT	Advanced threat hunting	✗	✗	✓	✗	✓
	Behavior Based Ransomware Detection and Rollback	✗	✓	✓	Detection only	Detection only
	Active Adversary Mitigations	✗	✓	✓	✓	✓
RESPOND	Automated Malware Cleanup	✓	✓	✓	Basic	✓
	Synchronized Security Heartbeat	✓	✓	✓	✗	✗
	Live terminal for investigation/response	✗	✗	✓	✗	✓

Feature Shoot-Out

	Sophos	Microsoft	See these **Detailed Comparison** sections for more info
Simple setup and management	✓	×	'Setup', 'Management'
Automatic ransomware rollback	✓	×	'Ransomware Protection'
Cross platform protection	✓	×	'Multi-Platform Protection', 'Machine Learning'
Synchronized Security	✓	×	'Synchronized Security'
Strong default configuration	✓	×	'Management', 'Exploit Prevention'
Server specific protection	✓	×	'Server', 'Protection for Virtual Machines'
Managed threat response	✓	×	'Managed Detection and Response'

Third Party Views

	Comments	Context
Gartner	Microsoft are in the 'Leaders' section of the **2019 Magic Quadrant for Endpoint Protection**. The report notes that Windows 10 includes several security features.	Gartner highlight difficulties associated with management - *"The biggest challenge continues to be the scattered security controls, management servers, reporting engines and dashboards."* The report also notes that some advanced features (such as EDR) are only available in costly top-level Microsoft licenses.
AV-Test	In **this test**, Defender generally achieves strong protection results for Windows. It does not participate in the macOS or Android tests.	Sophos generally performs well on the Windows test, as well as the macOS and Android tests.
SE Labs	Microsoft has performed well in recent **SE Labs Enterprise tests**, achieving the AAA rating.	Sophos Intercept X Advanced has also consistently been awarded the AAA rating, often scoring slightly higher than Microsoft.
Forrester	Microsoft was rated as a 'Leader' in the **2019 Forrester Wave Endpoint Security Suites report**.	While acknowledging Microsoft's "*compelling vision for the future*", the report also notes that *"Management complexities still come up frequently in customer conversations"*. Sophos is also rated a Leader by Forrester.

Watch Out For

Protection included in existing license
Customers may be able to use the Defender endpoint protection features through their existing corporate Microsoft license. However, the significant time required to configure/administer the products means that the total cost of ownership may still be higher than Sophos.

Naming confusion
Microsoft increasingly uses the term 'Defender ATP' to refer to a range of protection technologies. Originally it referred only to the EDR product, but more recently it has been also applied to other components such as Defender Antivirus and Exploit Guard. This can lead to customers being unaware of which capabilities they have licenses for.

Integration
Microsoft's products integrate in various ways to provide enhanced functionality. For example, Defender ATP can integrate with Cloud App Security to give greater visibility into devices accessing cloud applications. It also has cross-product EDR/XDR for investigating incidents across Windows, Office 365, and Azure.

Detailed Comparison

	How Sophos does it	How Microsoft does it	How we win
Setup	**Sophos Central** The Sophos Central console requires no installation, and most advanced security settings are enabled by default, meaning customers get the most effective protection from day one. Deployment is straightforward and can be managed through the customer's existing tools or installed directly by users or admins.	**Initial deployment** The Defender agents are installed by default on recent versions of Windows. Older versions and non-Windows systems will require an additional deployment. However, it is still necessary to "onboard" Defender ATP devices, which requires executing a script on each endpoint. This is separate from, and is verified from a separate console than, standard Windows endpoint management. **Endpoint Manager** Endpoint Manager is hosted within Microsoft's Azure cloud platform. No installation is required, but getting up and running with the product requires a strong grasp of related components such as Azure Active Directory. Many security features have obscure names or descriptions, and some require importing an XML or text configuration file. Some legacy Windows versions and non-Windows features cannot be configured in Endpoint Manager. **Microsoft Defender Security Center** Customers using Defender ATP will have to configure some settings in Defender Security Center and others in Endpoint Manager. The former is used for reporting on security state and investigating security events, while the latter is used to configure endpoint protection policies. **SCCM** SCCM is a complex, legacy on-premises management tool, primarily designed for larger organizations. Installation is a significant undertaking which requires extensive configuration, such as extending the Active Directory schema, installing IIS, .NET and SQL server (full license required – SQL Express cannot be used). Endpoint Manager is intended to replace SCCM, but many enterprise customers still use it.	**Cloud hosted Sophos Central requires no installation** **Ask:** Who in your organization has the expertise in Microsoft tools to configure your security policies? How much time do you expect to spend deploying and configuring your endpoint protection? **Show:** Demonstrate Sophos Central as a single point of management and reporting for cross-platform endpoint protection and EDR (plus other products). **Show:** Show the baseline threat protection policy for Intercept X in Central. Note how most protections are enabled by default, and how easy it is to change settings.
Management	**Intuitive management** Sophos Central is intuitive and makes common tasks simple to perform. Administrators can easily create and apply a security policy to Windows, Mac OS, and Linux computers. Ongoing administration tasks, such as adding a Device Control exception or blocking an application, are straightforward and do not require specialized knowledge.	**Multiple consoles** As mentioned in the previous section, Microsoft Defender uses multiple consoles. Along with Endpoint Manager and Microsoft Defender Security Center, Microsoft 365 customers may also find themselves using the Microsoft 365 Security Center, which is a meta-console that pulls in information from other sources. **Confusing policies** Policies in Endpoint Manager do not typically provide a choice of "disabled" or "enabled" like in Intercept X. Instead, you'll see choices like "disabled" or "not configured" (meaning this policy does not override whatever is already set by another policy or the OS default). This makes it difficult to determine what the actual policy on a specific endpoint will look like. In some cases, it may leave room for a user to inadvertently change the policy locally.	**Simple policy management** **Ask:** Who will be responsible for managing client protection? How familiar are they with the intricacies of Windows security? How much time do you expect to spend on reading documentation in order to use the products? What are the potential consequences of misconfigured security products? **Show:** Simple policy creation and enforcement in Sophos Central
Multi-Platform Protection	Windows, Mac and Linux machines can all be managed from the Sophos Central management console. There is no need to set up and navigate between multiple consoles in order to manage machines. As an increasingly popular desktop OS, macOS gets extensive feature support from Intercept X: app, device, and web control; malicious website protection; CryptoGuard anti-ransomware; Live Discover (coming soon); Live Response (coming soon); and more. Live Discover is also available for Linux, with Live Response coming soon.	Microsoft Defender ATP offers clients for macOS and Linux (in preview as of May 2020). These include some combination of basic AV (for macOS) and EDR (threat hunting, but not live response). Mac and Linux report in their security events to the Microsoft Defender Security Center console. However, policy configuration is not available through that console or through Endpoint Manager. Instead, configuration is via text files that have to be pushed to the machines. With the appropriate license, Endpoint Manager can be used to configure some OS settings on macOS (equivalent to Sophos Mobile). There are no equivalents to web protection, app/device/web control, or CryptoGuard for macOS in the Defender ATP agent.	**Protect Windows, Mac, and Linux devices from the same management console** **Ask:** How do you plan to manage and secure Mac and Linux devices? **Ask:** Do you need to demonstrate that Mac and Linux machines are protected and have appropriate settings applied? **Show:** Demonstrate how policies in Central can be applied across operating systems, and how Central can show all of a user's devices and events in one screen.

Detailed Comparison

	How Sophos does it	How Microsoft 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.	Windows Defender includes machine learning for detecting the latest malware variants. Details on the type of machine learning models is not available, but there is nothing to indicate it uses deep learning models like those used in Intercept X. Machine learning protection is only available on Windows 10 machines, meaning Windows 7 and 8 machines receive reduced protection.	**Proven effectiveness** **Consistent protection for Windows 7, 8 and 10** **Show:** Our extensive research on security-specific machine learning.
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.	Microsoft provides some degree of ransomware protection in Windows Defender. It looks for suspicious behavior that could indicate a ransomware attack but appears to be quite tightly aligned to known variants, meaning it may struggle to detect new strains of ransomware. Microsoft has also added 'Controlled Folder Access', which allows specific folders to be locked down so that only explicitly allowed applications can write to the controlled folders. Two significant drawbacks to this are: 1) Administration of the folders and allowed applications is time consuming 2) It does not protect against legitimate applications that have been exploited (e.g., a malicious macro in a Word document) Both of the above protections are only available in Windows 10, meaning any other Windows client or server platforms do not benefit. CFA needs to be 'trained' to allow legit actions and reduce false positives.	**Comprehensive - behavioral detection protects against the latest ransomware, no 'training' of the product required** **Consistent protection for Windows 7, 8 and 10** **Show:** Demo CryptoGuard in action to show how users are protected and able to continue working without any action by the administrator.
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 otherwise unused hardware feature in mainstream Intel processors to track code execution and augment the analysis and detection of advanced exploit attacks at run time.	**Exploit Guard** Windows 10 and Server 2016+ include a feature called Defender Exploit Guard. Exploit Guard has a small number of device level mitigations, but most mitigations are applied on a per-application basis. Policies are assigned by exporting individual machine settings and distributing these to other clients. Exploit Guard is not available Windows 7 or 8 machines.	**Robust exploit protection, with no configuration required** **Consistent protection for Windows 7, 8 and 10** **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 **Share:** The Exploits Explained whitepaper details many of the Intercept X exploit mitigations.

Detailed Comparison

	How Sophos does it	How Microsoft 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. **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. A single click will clean up a malicious file across the estate and block it in the future. **Live Discover (hunting)** 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. **Isolation** Endpoints can be isolated and restored automatically (based on Security Heartbeat status). Administrators can also manually isolate an endpoint and return it to service when they are finished investigating or remediating a threat. **Live Response** 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.	Windows Defender ATP is designed for security teams who have the time and expertise to learn the nuances of Microsoft's environment and to apply judgment to the detailed information provided. **Threat Visibility and Response** Information on suspicious events is provided, including details of files, processes, network connections and users involved. Response actions, such as isolating machines, are available. Administrators can search across machines for artifacts and create their own Indicators of Compromise (IOCs) upon which they want to be alerted. **Threat Hunting** Customers can use prebuilt or custom queries to hunt for suspicious activity. Only 30 days of data is available, and it is limited to what has been collected in the cloud. Defender ATP uses Microsoft's proprietary Kusto Query Language instead of the standard SQL used by Intercept X. Data does not include any information about artifacts' reputation or threat level. Customers with a Microsoft 365 E5 license can take advantage of Microsoft Threat Protection, a separate console that allows hunting across endpoints, Office 365, and Azure services. **Live Response** Defender ATP provides a remote terminal for Windows systems only, allowing further investigation and interaction when needed.	**Add expertise, not headcount** **Ask:** What resources do you have available to dedicate to threat hunting and investigation? **Show:** Sophos EDR's guided investigations provide suggested next steps, such as investigating highlighted processes and isolating a machine. **Show:** The power and flexibility of Live Discover to search rapidly across endpoints for information such as installed browser plug-ins or low-reputation files.
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.	**Fragmented technologies** Microsoft offers a range of additional security technologies, such as BitLocker Management, Windows Information Protection, Azure Rights Management and others. On paper these suggest an integrated set of protections, however in reality they are a fragmented set of features that are managed through various products and consoles. Additionally, features are platform dependent, with the latest features only being available on Windows 10 devices. Some features require SCCM, others rely upon group policies, and others use consoles within Microsoft's Azure cloud platform. There is limited integration between features and, because Microsoft does not offer gateway firewalls, there is no opportunity to automatically isolate a compromised machine from the network.	**Simple setup, powerful features** **Ask**: If your firewall alerted you to suspicious traffic from an IP address on your network, how long would it take you to track down the computer, isolate it from the network? **Show**: Enable Synchronized Security within a matter of clicks and demonstrate the XG Firewall automatically isolating a compromised endpoint client

Detailed Comparison

	How Sophos does it	How Microsoft does it	How we win
Web Protection	**Actionable information for Windows and Mac** Sophos integrates web protection into Windows and Mac endpoint clients. URL filtering blocks known malicious sites, and scanning with script emulation and behavioral analysis blocks malware even on reputable sites. Web protection events are reported back to the management console, meaning administrators have visibility of events occurring for both local and roaming users.	**Windows only** Microsoft's SmartScreen filter is used in Internet Explorer and Edge to check whether a site is suspicious or malicious. Additionally, a reputation check is performed on any files that are downloaded, to check for malicious content. On Windows 10 devices, it is possible to expand this feature to filter all traffic (rather than just protecting IE/Edge), through the Network Protection feature of Application Guard. As SmartScreen and Network Protection are part of Windows browsers and operating systems, these features are not available for Mac endpoints. **Visibility** Alerts are not reported into the Endpoint Manager console, meaning only Defender ATP customers have a central way of identifying trends or specific users who could benefit from advice on safe browsing.	**Cross platform protection** **Ask:** How will you stop Mac users from accessing malicious websites? **Show:** Reporting of web protection events in Sophos Central
Web Control	Web control allows the administrator to block access to unwanted websites on Windows endpoints, Windows servers, and macOS endpoints. Website categories come pre-configured, meaning administrators can easily block endpoints from accessing inappropriate categories such as adult, gambling, hate, or crime.	Web filtering is available only through Defender ATP, and then only for Windows 10 endpoints.	**Simply 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 device control is simple yet powerful. It can control access to a wide range of devices, and exclusions can be made per make or model, giving administrators flexibility and control. These features are integrated in Sophos Endpoint and require no additional download or components to be installed. Device control is available on both Windows and macOS.	Device control has recently been added to Windows 10 and is managed through Endpoint Manager device configuration profiles. There is no option to run in discovery mode (e.g. report which USB devices have been installed without blocking them), and adding exclusions involves the administrator manually adding device IDs. It is not possible to use device control on other platforms (e.g. Windows 7 and Mac devices).	**Cross platform device control** **Show**: Create a policy to block USB drives, and then show how to add an exception for a drive the user plugged in.
Application Control	Administrators can control installation, track usage, or block execution of more than 1000 applications within a few clicks. The list of applications is maintained by SophosLabs and is updated on a regular basis. Sophos application control enables employee productivity and reduces the risk of data loss, while administrative effort is kept to a minimum. This is all configured through the same management console as anti-malware and all other protection modules. Application control is available on both Windows and macOS.	**Defender Application Control and Windows AppLocker** Application Control is a whitelisting approach, where only trusted applications are allowed to run. It involves significant administration from the customer to ensure any legitimate business applications (which are not on Microsoft's predefined list of trusted applications) are allowed to run. Defender Application Control is only available on Windows 10 and Server 2016+. The predecessor to Defender Application Control is AppLocker. This allows specific applications to be blocked based on a variety of criteria, but again there is no pre-configured list of applications and the administrator has to add these details in themselves using complex configuration files. In summary, in order to achieve application control, it is necessary to perform significant configuration and maintenance.	**Cross platform support** **Simply choose applications from a pre-populated list** **Ask:** How do you currently control which applications are allowed on your network? How much time do you spend tuning this? **Show**: Demonstrate how easy it is in Sophos Central to create a policy that blocks file sharing tools such as BitTorrent

Detailed Comparison

	How Sophos does it	How Microsoft does it	How we win
Data Loss Prevention (DLP)	DLP is integrated into Sophos endpoints, meaning no additional plugins are required. 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.	**Windows Information Protection** Endpoint Manager has no specific DLP policies but can instead be integrated with Windows Information Protection (WIP). WIP is designed to prevent data loss, and involves administrators specifying which applications and devices can access and share encrypted documents. WIP relies upon features within multiple products and technologies (Azure Rights Management, Bitlocker, Office365), meaning more administration for the customer. **Office 365** Microsoft Office 365 (which provides cloud hosted versions of Outlook, Word, Excel, etc.) includes the ability to set DLP policies. Administrators can select from 51 built in policies, or create their own, in order to block access when a user tries to send sensitive data outside the business. **Azure Rights Management** Microsoft Azure Rights Management is another tool for protecting sensitive information. It uses encryption and rights management to ensure that people outside the organization cannot access files unless authorized to do so. Office 365 and Azure Rights Management are both cloud based management consoles. Therefore, unless the customer is already using these products, they would need to configure and maintain another product to achieve DLP functionality.	**Simple configuration** **Ask**: What measures do you have in place to prevent important data leaving the organization? How much time do you have available to configure and tune these settings?
Encryption	Sophos Central Device Encryption protects data and ensures regulatory compliance in the event of a lost or stolen device. It provides centrally managed full disk encryption for Windows and macOS, taking advantage of the technology built into the operating system. Users who forget their keys can use the Sophos Central Self Service Portal to recover. If more advanced features are required, Sophos SafeGuard Enterprise offers automatic, always-on file-level encryption on endpoints, mobile devices, and in cloud storage — across Windows, Mac, iOS, and Android. Synchronized Encryption proactively protects data by continuously validating the user, application, and security integrity of a device before allowing access to encrypted data.	**Intune** Customers with an Intune license can manage Bitlocker and Filevault full disk encryption policies. Self service recovery is not available, meaning IT must be involved. **Windows Information Protection** Windows Information Protection (WIP) involves administrators specifying which applications and devices can access and share encrypted documents. WIP relies upon features within multiple products and technologies (Azure Rights Management, Bitlocker, Office365), meaning more administration for the customer. **Azure Rights Management** Microsoft Azure Rights Management is another tool for protecting sensitive information. It uses encryption and rights management to ensure that people outside the organization cannot access files unless authorized to do so.	**Self-service recovery** **Streamlined management**
Server	Intercept X for Server protects physical and virtual Windows and Linux servers. Advanced Windows Server protection features such as deep learning, exploit prevention and anti-ransomware are coupled with server specific capabilities such as server lockdown, file integrity management, and automatic scan exclusions. All features are managed through Sophos Central. Intercept X for Server integrates with both Azure and AWS. This makes it easy for customers to see all of their EC2 and Azure VM instances, identify which are protected, and automatically remove terminated/deleted instances from the Central console.	**Windows Server security** Recent versions of Windows Server include many, though not all, of the endpoint security features in Windows 10. There is no equivalent to our server lockdown, file integrity management, or CryptoGuard anti-ransomware. **Limited Linux support** Defender ATP offers a Linux agent in public preview as of May 2020. Configuration is not available through Endpoint Manager. Instead, the customer has to manually edit a JSON configuration file and push it out to Linux systems through a third-party management tool. **Azure integration** There is limited Azure integration in Defender ATP. It allows alerts to be cross-referenced between Azure ATP and Defender ATP. In addition, Microsoft Threat Protection allows customers to query events across Windows, Azure, and Office 365. Neither Defender ATP nor Endpoint Manager automatically discovers and removes Azure virtual machines. There is no integration with AWS.	**Protection and policies tailored to server operating systems** **AWS and Azure support** **Ask**: Do you have workloads in AWS or Azure? **Show**: Trigger lockdown on a server **Show**: Demonstrate file integrity monitoring

Detailed Comparison

	How Sophos does it	How Microsoft does it	How we win
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 vSphere/ESXi. **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 Server licenses. Customers can have a mix and match between the supported hypervisors, as long as they have enough licenses.	Microsoft does not have a thin agent, centralized scanning solution like SVE. Endpoint Manager provides no features specific to virtual machines.	**Lightweight agent for VMware and Hyper-V** **Ask**: How do you plan to protect virtual machines in your environment?
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 -	Microsoft Threat Experts (MTE) provides threat hunting and allows customers to request additional analysis and advice. It does not provide hands-on or guided response. - **Not a fully managed service** - **No remediation actions** - ***Requires* customer to have its own SOC** MTE is an add-on to the top level E5 license, which is already expensive.	**Fully managed service with response** **Ask**: How confident are you about your ability to identify and remediate advanced threats on your own?