SOPHOS

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

SYNCHROWORKS CONSULTING

COMPETITIVE INTELLIGENCE

KASPERSKY ENDPOINT BATTLECARD

Vendor Profile

Kaspersky is a privately owned computer security company founded in 1997. It has headquarters in Moscow and over 3,000 employees worldwide.

Product	Description	Sophos Equivalent
Kaspersky Endpoint Security (KES)	Endpoint protection software installed on client machines	Intercept X / Sophos Endpoint
Kaspersky Security Center	On-premise admin console for managing Kaspersky Endpoint Security clients	Sophos Enterprise Console
Kaspersky Security Center Cloud	Cloud-hosted admin console for managing Kaspersky Endpoint Security clients	Sophos Central

Competitor Strengths

Feature set - A broad range of protection features and management tools, including vulnerability analysis, patch management, and application control

Test results - Kaspersky regularly achieves strong protection scores during independent testing

Competitor Weaknesses

Endpoint centric - Kaspersky is an endpoint centric vendor and provides little protection beyond the endpoint

No Synchronized Security - Kaspersky lacks a next-gen firewall or UTM solution

Limited cloud management – Kaspersky Security Center Cloud is still developing and lacks features of the on-prem console

Why Sophos Wins

Security Ecosystem
Manage endpoint, server, firewall, mobile, encryption, email and Wi-Fi through the same cloud hosted Sophos Central console.

Advanced Threat Protection
Intercept X combines industry leading anti-exploit, anti-ransomware and deep learning malware protection.

Synchronized Security
On top of Kaspersky's offerings, Sophos can also provide gateway protection through next-gen firewall, web, email and UTM security. With Sophos Synchronized Security, the endpoint and firewall communicate and share information, allowing stronger and simpler security.

Endpoint License Comparison

		Sophos			Kaspersky		
		Central Endpoint Protection	Intercept X Advanced	Intercept X Advanced with EDR	Endpoint Security for Business Select	Endpoint Security for Business Advanced	Endpoint Detection and Response Optimum
	Management	Cloud	Cloud	Cloud	Cloud or on-prem	Cloud or on-prem	Cloud or on-prem
PREVENT	Web Control / Category-Based URL Blocking	✓	✓	✓	✓	✓	✓
	Device Control (e.g. USB)	✓	✓	✓	Windows only	Windows only	Windows only
	Application Control	✓	✓	✓	Windows only	Windows only	Windows only
	Web Protection	✓	✓	✓	✓	✓	✓
	Data Loss Prevention	✓	✓	✓	×	×	×
	Exploit Prevention	×	✓	✓	✓	✓	✓
	Machine Learning	×	✓	✓	✓	✓	✓
DETECT	Malicious Traffic Detection (MTD)	✓	✓	✓	✓	✓	✓
	Behavioral Ransomware Protection & Rollback	×	✓	✓	✓	✓	✓
RESPOND	Synchronized Security Heartbeat	✓	✓	✓	×	×	×
	Endpoint Detection and Response (EDR)	×	×	✓	×	×	Limited
OTHER	Device Encryption	×	×	×	×	✓	✓

Feature Shoot-Out

	Sophos	Kaspersky	See these **Detailed Comparison** sections for more info
Comprehensive cloud management	✓	×	'Cloud Management'
Simple administration	✓	×	'User Interface'
Integration of endpoint and firewall products	✓	×	'Synchronized Security'
Data loss prevention	✓	×	'Data Loss Prevention (DLP)'
Comprehensive macOS feature set	✓	×	'Anti-Ransomware,' 'Device Control,' 'Application Control'
Managed detection and response	✓	×	'Managed Detection and Reponse'

Third Party Views

	Comments	Context
Gartner	After previously appearing in the 'Leaders' quadrant, Kaspersky was demoted to the 'Visionaries' section in 2018 where it also remained in the latest **2019 Gartner Magic Quadrant for Endpoint Protection**.	The report acknowledges strong results in 3rd party tests. However, Gartner raises cautions over the management options, noting that the cloud console is only available for small to mid-size customers.
AV-Test	Endpoint Security achieved high scores in **recent tests** for Windows, but Kaspersky has not participated in recent tests for macOS and Android.	Intercept X regularly achieves high scores in the Windows test, as well as the macOS and Android tests.
SE Labs	Kaspersky has performed well in **SE Labs tests** and regularly achieves the AAA rating.	Sophos Intercept X Advanced also consistently achieves the AAA rating.

Watch Out For

Strong Third-Party Testing
Kaspersky often scores well in tests from AV-Test, SE Labs and similar organizations. While third party testing is certainly important, note that it examines just one part of a product (anti-malware protection) and doesn't factor in other areas such as the overall management experience.

Mobile Security
Some Kaspersky endpoint SKUs include mobile security. However, this is not a full UEM offering, and advanced features such as a containerization and man-in-the-middle (MiTM) protection are not available.

Broad Range of Features
In addition to security configuration, the Kaspersky Security Center enables other administrative tasks, such as client operating system installs and remote connections to client machines, to be performed. However, it is likely that many customers will already have separate tools for performing these common tasks.

Detailed Comparison

	How Sophos does it	How Kaspersky does it	How we win
Cloud Management	Sophos Central provides one place to manage endpoint, mobile, firewall, email, server and wireless security. Using a common management platform, customers benefit from security intelligence sharing, policies that follow users, easy configuration, detailed and summary reporting, and automatically prioritized alerts.	**Security Center Cloud Console** Kaspersky Security Center Cloud Console is a relatively new management interface. It lacks many features of the on-prem console, including mobile security management, integration with AWS/Azure, encryption management, and scalability beyond 10,000 endpoints. The console focuses on endpoint protection but does not extend to other areas. Features such as full EDR and integration with AWS are only available in Kaspersky's on-premise products. **Endpoint Security Cloud** This is a separate cloud-managed product aimed at smaller businesses. It includes mobile security and encryption management, but it lacks granular controls, EDR, Linux support, and other features.	**Security ecosystem** **Point out:** Sophos Central extends beyond endpoint protection and allows administrators to manage server, public cloud, firewall, mobile, encryption, email and wireless from the same console.
User Interface	Sophos Central provides simple navigation, allowing tasks to be completed in a small number of steps. Dashboards present information such as the number of protected machines, alerts and web browsing statistics. Performing actions, such as triggering a scan or editing a policy, can be completed within a few clicks.	**Security Center Cloud Console** This is a port of the on-premises console. Its legacy roots show, as it requires opening multiple non-standard ports. Administrators who wish to use an on-prem caching server have to manually assign endpoints to a specific server. **Endpoint Security Cloud** Kaspersky Endpoint Security Cloud has a refreshed, cloud-native interface, but its lacks the granularity and advanced features of its on-premise counterpart.	**Intuitive management console** **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.
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 Management and Defense** Kaspersky 'Threat Management and Defense' includes the Kaspersky Anti-Targeted Attack (KATA) product. KATA is designed to detect advanced threats through network traffic sensors and a cloud sandbox. Also included is Kaspersky's full (on-prem) EDR product. There is no indication that either product has the ability to automatically isolate compromised machines and dynamically restore access based on endpoint health. Kaspersky does not offer its own next-gen firewall.	**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 and isolate it from the network? How long would it take to restore network access after cleaning up the endpoint?
Machine Learning	Intercept X's deep learning models detect unknown malware and potentially unwanted applications. Intercept X Advanced with EDR also uses machine learning to provide actionable intelligence about suspicious files. Our machine learning experience began as part of a 2010 DARPA project. The Sophos AI team continue to be recognized as leaders in the field, and their expertise is reflected in the growing role of machine learning throughout our products and services.	Kaspersky also claims to use deep learning models in its endpoint protection. It does not have an industry reputation as being a leader in the field of machine learning.	**Leaders in the field** **Show:** The Sophos AI website highlighting the team's research, blog posts, and demos.

Detailed Comparison

	How Sophos does it	How Kaspersky does it	How we win
Anti-Exploit	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.	Kaspersky's anti-exploit feature looks specifically for executable files attempting to be run by vulnerable applications. There is also reference to protection against memory based attacks (e.g. Stack Pivot and Heap Spray Allocation), but there is limited information on the specifics of this. In summary, there is no indication that Kaspersky Endpoint offers the same depth of exploit prevention as Intercept X.	**Depth of exploit protection** **Point out:** Sophos Intercept X covers more than 25 types of exploit prevention techniques
Anti-Ransomware	Sophos CryptoGuard blocks the spontaneous encryption of data and automatically rolls data files back to a pre-encrypted state. It can protect against both local and remote processes, which is especially valuable on file servers or on workstations compromised over the network. CryptoGuard is available on both Windows and macOS.	Kaspersky has a similar behavioral ransomware detection and rollback feature. However, it has some limitations compared to CryptoGuard: • It is available for Windows only. • It does not protect against attacks from remote devices on the network.	**Protection for Windows, macOS, and file servers** **Point out:** CrytoGuard provides more comprehensive protection by defending devices against network-based attacks and supporting macOS.
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.	Kaspersky has two separate EDR solutions. **Kaspersky Endpoint Detection and Response Optimum** This is a lightweight EDR that primarily offers root cause analysis (similar to our Threat Cases) and response actions (e.g., isolate endpoint). It does not offer robust hunting tools like Live Discover. Optimum is managed via the Security Center Cloud Console, though it requires installing an additional plug-in **Kaspersky EDR** Kaspersky EDR requires its own management console (separate from Security Center and Endpoint Security Cloud) and is primarily designed for trained security analysts. Features such as threat hunting, file deletion/retrieval, sandboxing and threat chain visualization are available. Customers can drill down into more details by looking up files on the Kaspersky Threat Intelligence Portal. There is no third-party opinion input like Virus Total. Kaspersky EDR utilizes the normal Endpoint Security agent however management is performed through the broader 'Kaspersky Anti Targeted Attack Platform' (KATA). This requires its own server and management console and is geared up for trained security analysts who have the resources and skills to interpret the information presented to them. Data is stored centrally and live endpoint data cannot be queried. It does not allow for remote console action from the KATA console. You can however establish an RDP connection from the separate endpoint security management console.	**Single cloud hosted console** **Add expertise, not headcount** **Point out:** Full EDR and endpoint protection features are provided through a single agent and cloud hosted management console **Show:** Sophos Live Discover provides useful pre-built queries and allows extensive searching of live endpoint data.

Detailed Comparison

	How Sophos does it	How Kaspersky 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.	Kaspersky does not offer data loss prevention and instead relies on device controls to limit how data can escape, such as by blocking all USB drives if desired.	**Simple DLP integrated into the endpoint** **Ask**: What measures do you have in place to prevent important data leaving the organization? How much time do you have available to tune these settings?
Device Control	Provides granular device access which allows control based on individual devices. A list of devices is automatically gathered centrally.	Device Control is available in both Kaspersky's on-premise and cloud managed endpoint security but is not supported on macOS.	**Cross platform support** **Point out:** Sophos provides device control for both Windows and macOS devices
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 Sophos Labs and is updated on a regular basis. Application control assists employee productivity, and reduces the risk of data loss, while administrative effort is kept to a minimum.	**Security Center Cloud Console** Application control relies upon machines reporting information about the programs they are running back to the Security Center. The administrator can then use this information in policies to block/allow specific applications. Policies can be applied per user or per machine. Kaspersky's application control does offer significant features, however each of the configuration steps required means a considerable amount of work is required by the customer to use and maintain application control. **Endpoint Security Cloud** Application control is unavailable in Kaspersky's smaller business cloud solution.	**Control which applications run on client machines** **Simply choose from a pre-populated list** **Show**: Demonstrate how easy it is in Sophos Central to create a policy that blocks file sharing tools such as BitTorrent.
Web Control	Sophos Endpoint provides integrated web control. This allows administrators to easily block endpoints from accessing inappropriate sites such as adult, gambling, hate, crime.	Web control is available in both Endpoint Security Cloud and the on-premise Security Center. Administrators can block access based on site category or content type (e.g. videos or executable files).	
Unified Endpoint Management (UEM)	**Consolidate Management** Sophos Central's unified admin interface enables customers to manage mobile devices alongside endpoint protection and other Sophos technologies such as encryption, email or wi-fi. For customers who prefer an on-premise installation, there is feature parity across the platforms, meaning customers do not miss out on functionality by selecting one option over another. **Security** A rich set of management capabilities and powerful containers secure sensitive business information on mobile devices. Deep learning anti-malware technology and man in the middle (MiTM) detection protect users and devices from advanced attacks.	**Mobile Management** Endpoint Security Cloud offers management of iOS and Android devices, and malware protection for Android. Kaspersky's enterprise Security Center Cloud Console does not support mobile management. **Reduced Features** Kaspersky does not provide a full range of UEM features. Key features such as containerization and mobile content management are missing, while advanced security features such as man in the middle (MiTM) protection are also absent.	**Secure Unified Endpoint Management (UEM)** **Ask**: What is your plan for protecting mobile devices?

Detailed Comparison

	How Sophos does it	How Kaspersky does it	How we win
Server	Sophos Central protects physical and virtual Windows and Linux servers. 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 and automatic scan exclusions. Unlike solutions that are designed for end-user workstations, Sophos Server Protection protects servers while minimizing the impact on performance. Intercept X Advanced with EDR also includes a subset of features from Cloud Optix. These features allow you to see and secure your entire cloud inventory.	**Security Center Cloud Console** Windows Server is treated as a standard endpoint. There are no server-specific capabilities. Ransomware behavior cannot be detected, blocked, and rolled back if it is launched from a client or another server on the network. Linux servers receive file integrity monitoring and some additional features that are not available in Intercept X Advanced for Server. **Endpoint Security Cloud** The smaller business version includes malware protection for Windows Server, but there are no server specific protections such as File Integrity Monitoring (FIM) or Server Lockdown. Protection for Linux servers is unavailable. **Hybrid Cloud Security** Kaspersky offers a separate cloud workload protection solution called 'Hybrid Cloud Security.' It includes a connector to allow visibility and protection of servers in AWS and Azure. In addition to anti-malware protection, the product offers a wide range of options and features, such as optimizing performance through scanning only modified files and allocating server resources based on pre-defined priorities. However, administrators would need to spend a significant amount of time to test, deploy and maintain these granular settings.	**One-click server lockdown** **Cloud Security Posture Management** **Ask**: How much time do you plan to spend configuring and managing protection policies for your servers? **Show this**: Trigger lockdown on a server. **Show this:** Demonstrate the Cloud Optix features available in Intercept X Advanced with EDR.
Licensing	Sophos provide simple licensing without the need to manage lengthy activation keys.	In addition to uploading a license key to the Security Center, the Endpoint Security client also requires a license key to be applied to it. Administrators can automate this process by selecting an option for keys to be assigned automatically when a machine reports in, however the process can still require manual intervention if protection is being installed on a standalone machine or one that will not immediately report to the console. Admins need to keep a continuous watch for license usage to make sure it is not exceeded across the managed estate.	**Simple licensing** **Ask:** How long do you want to devote to managing product license keys?
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	Kaspersky offers two managed endpoint/detection services, neither of which is quite equivalent to Sophos MTR: **Kaspersky Managed Protection** This is an instance of Kaspersky Endpoint Security and Kaspersky Anti Targeted Attack Platform (on-prem) that is managed by Kaspersky. Kaspersky provides monitoring and threat hunting, but it only provides automated response, not manual action where needed. **Targeted Attack Discovery** This is a SIEM-based service that uses on-prem data collectors to aggregate log and event data. Kaspersky uses the data to hunt for threats in the customer's environment and alert the customer. Kaspersky provides remediation recommendations, but it does not directly take response actions.	**Managed response, not just detection and alerting** **Ask:** How long would it take you to respond to an advanced threat during the night or on a weekend? **Ask:** Would you prefer to deploy a primarily on-prem or cloud-based solution?