

# XGen Endpoint Security - Winning Against Sophos suites

## The Challenge and Opportunity

Sophos is focused on the mid to small business exclusively. The solutions remain overly simplistic for most mid-size and larger enterprises. Sophos new Intercept X is an additional layer that adds technologies which have been part of Trend Micro's core endpoint agent for years.

## Smart Protection Suite Advantage

**Maximum Protection:** Combines the broadest range of cross-generational technologies for the best detection while avoiding downsides of false positives and low performance. AV-Test (third-party testing) results have consistently scored the best for protection and performance / usability over multiple tests spanning the past 2 years.

**Minimum Impact:** Intelligently filters out threats using the most efficient technique for maximum detection without false positives. Connects and centrally manages multiple layers of cloud and on-premises security with single management console delivering comprehensive visibility in a timely and efficient manner.

**More flexible deployment and licensing:** Flexibility in SaaS or on-premises deployment models provides seamless support for your ever-changing environment. Mix between models at anytime with no changes to your commercial agreement.



**Proven Security Partner:** 25+ years of continual innovation. Gartner "Leader," and highest vision score, InfoTech "Champion," Ovum "Leader," SC Magazine 5-Star Rating with comprehensive protection for advanced threat protection.

## Suite Offerings and Included Functionality

Included Suite Functionality	TREND MICRO		SOPHOS			
	Smart Protection Endpoints	Smart Protection Complete	Endpoint Protection	Endpoint Prot. Web, Mail & Encryption	Cloud Enduser Prot.	Endpoint Prot. Adv + InterceptX
<b>Central Management</b>	✓	✓	✗	✗	✗	✗
<b>Endpoint Security</b> Anti-malware, Encryption, web filtering, intrusion prevention	✓	✓	✓	✓	P	✓
Machine learning	✓	✓	✗	✗	✗	✗
Behavior analysis and ransomware analysis	✓	✓	✗	✗	✗	✓
C&C blocking (aka "malicious traffic detection")	✓	✓	✗	✗	✗	✓
Application Control, DLP	✓	✓	P	P	✗	P
Forensics investigation tool	✗ (extra \$)	✗ (extra \$)	✗	✗	✗	✓
SaaS deployment option	✓	✓	✗	✗	✓	✗
<b>Mobile Security</b>	✓	✓	✓	✓	✓	✓
<b>Email Security</b> email gateway, email encryption, mail server	✗	✓	P	✓	✓	✓
Integrated Email DLP	✗	✓	✗	✓	✗	✓
API based Office 365 protection	✗	✓	✗	✗	✗	✗
Email APT protection	✗	✓	✗	✓	✗	✗
<b>Collaboration Security</b> SharePoint, IM (Lync), DLP	✗	✓	✗	✗	✗	✗
SaaS: Office 365 SharePoint, OneDrive, Box, Dropbox; threat & DLP	✗	✓	✗	✗	✗	✗
<b>Web Security</b> Web filtering, application control	✗	✓	✗	✓	✓	✗
Integrated Web DLP	✗	✓	✗	✗	✗	✗
On-premise	✗	✓	✗	✓	✓	✗
SaaS deployment option	✗	✓	✗	✓	✗	✗

This document is intended to provide general guidance to and for the exclusive use of Trend Micro field sales and marketing personnel and authorized partners. The contents represent the best information available to Trend Micro at the time of publication and is provided "AS IS," without warranty of any kind as to its accuracy, currency or completeness, express or implied. The contents may not be applicable in all situations, may not reflect the most current situation, and are subject to change without notice and at the sole discretion of Trend Micro. It is not intended and should not be construed to constitute legal advice and should not be relied upon as such. Neither Trend Micro nor any party involved in creating, producing, preparing or delivering the contents shall be liable for any consequences, losses, or damages, including direct, indirect, special, consequential, loss of business profits or special damages, whatsoever arising out of access to, use of or inability to use, or reliance upon, the contents of this document, or any errors or omissions in the content. Do not disseminate, publish, disclose or transmit this document, in whole or part, without the prior written permission of an authorized representative of Trend Micro.

## Trend vs. Sophos Capabilities

			Comments
Anti-Malware (top AV-Test scores 2014-2016)	★★★★	★	Trend performing best on 0-day with AV-Test. Sophos is worst of large vendors. Sophos also did not perform well in the NSS Labs Exploits & Evasions testing in Oct. 2015.
Performance (top AV-Test scores 2014-2016)	★★★★	★	Trend performance is the highest, with Sophos again near the bottom for performance .
Intrusion prevention(aka “vulnerability shielding”)	★★★★	☆	Trend’s endpoint HIPS technology comes from our industry leading Deep Security product line. Sophos doesn’t have this , they do patch assessment only.
Application control / whitelisting	★★★★	☆	Trend has full endpoint application control. Sophos claims some whitelisting but it can only submit a file to be whitelisted and is missing basic expected functionality - no cloud-based app list or categories, no application inventory capability, no trusted sources, no reputation info to use for creating dynamic rules.
Behavioral analysis & sandboxing	★★★★	★	Trend strong with sandbox, unknown attack protections, lateral movement protections, memory inspection, etc. Sophos limited based on AV-Test & NSS Labs results which show their 0-day protections to be poor. Behavior monitoring requires purchasing and deploying a second agent, Intercept X.
Ransomware Protection	★★★★	★	Trend includes specific technologies to detect and stop ransomware. Sophos is late to develop these technologies and requires purchasing a second agent, Intercept X.
Endpoint web reputation	★★★★	★	Trend base product uses kernel based technology to catch C&C call backs outside the browser. Sophos is browser based and easily defeated. To get equivalent functionality Sophos sells an add'l agent, Intercept X.
Encryption	★★★★	★★★★	Similar capabilities including Bitlocker & FileVault management options.
Data Loss Prevention (DLP)	★★	★	Trend DLP is across endpoints, cloud applications, messaging, web, IM and portals and includes data at rest, in motion and in use. Sophos only has DLP for email protection & endpoint and it’s on access scanning only.
Cloud App Security for Office365 & cloud file sharing (Box, Dropbox, Google Drive)	★★★★	No offering	Unique capability for Trend. Sophos only has a email gateway which can protect Office inbound email but not internal email, SharePoint, OneDrive, Box, Dropbox.
Email APT protection	★★★★	missing	Sophos Sandstorm cloud sandbox offering is not included. It’s an unproven cloud only offering (no NSS Labs sandbox testing).
SaaS Offerings	★★★★	★	Trend includes SaaS offerings for endpoint, email, SaaS applications, and web. Sophos has SaaS web security, limited endpoint SaaS capabilities and but missing SaaS email security and SaaS app security (i.e. no equivalent to Cloud App Security for Office 365, Box, Dropbox).
User-based visibility / central synthesis	★★★★	★★	Trend Micro's user-centric visibility manages and correlates security events from all endpoints and email / web access & presents them in an intuitive user view. Sophos has no central mgmt/visibility across layers.
Suite deployment	★★★★	★	Trend has a single deployment kit, activation key, that is interchangeable across on-prem and cloud.
Completeness of security architecture	★★★★	★	Trend has strong integration across it’s endpoint, gateway & network solutions with Connected Threat Defense. Sophos only has limited heartbeat across endpoint and firewall.

## How to Win:

- **Sell the solution**, not features – focus on value of the complete story and our Smart Protection Suite value.
- **Ask questions about the future** – highlight flexible solution that will evolve with their requirements.
- **Focus on great support and trusted partners** who can deliver on the customer's needs.

## Objection Handling (Cautions)

**How is Trend Micro positioned vs. Sophos in the Gartner Magic Quadrant (MQ) for Endpoint Protection?** Trend Micro is positioned as a “Leader” – a position we have held for 14 years. In the Dec. 2015 MQ, Trend Micro is now the highest rated for “Completeness of Vision. See the [Trend Responds document](#) from Sales Library and Trend Micro has secured distribution rights to share the MQ with your customers.

**I just need a simple solution!** Sophos promote the simplicity of their management console but in our analysis, customer feedback and also the Gartner MQ, it's been pointed out that simplicity of management becomes a liability when there are few options and flexible choices especially for mid-size and larger organizations. In fact, reporting is said to be almost non-existent. The Sophos cloud management interface is so simplistic that you have almost no management options, it's just on or off in many cases.

**Sophos says that they are next generation endpoint with Intercept X.** Sophos Intercept X provides technologies developed by Trend Micro and part of our core agent instead of an expensive add-on. For example, we developed malicious traffic detection 3 years before Sophos and specific anti-ransomware technologies 1 year before. Sophos doesn't offer anything like XGen™ which goes beyond next gen endpoint technologies by combine machine learning technology into both pre-execution and runtime detection layers.

**Trend Micro requires more agents than Sophos.** Not true. The only additional capability that Sophos has in their base agent is their claim of application whitelisting but its missing basic expected functionality (see chart on page 2). Sophos Intercept X adds another agent which includes function built into Trend Micro's base agent. Trend has more advanced antimalware functionality including high-fidelity machine learning.

## Questions to Ask Customers

**How have past security incidents gone for your organization?**

- Was the threat blocked?
- Did the vendor provide good support?
- Were you able to find out where the threat had spread?

**Does your security vendor cover all of the different devices, endpoint platforms, and web-based activities, and cloud services your employees use?**

- Are you covered across all of your platforms and OS (Windows, Mac, Linux, iOS, Android) as well as SaaS apps (Office365, cloud storage like Box, Dropbox)?

**How is the performance of your existing endpoints?**

- Are your users complaining about slowness?
- Does your endpoint solution use a lot of network bandwidth?

**Do you have multiple management consoles?**

- Do you have visibility across a user's devices and multiple platforms for rapid response?
- How do you manage cloud and on-premises security?

## Other Resources

- **Use the concentric circles chart in the latest endpoint customer presentation on sales hub to demonstrate our extensive next gen, advanced protection capabilities.**
- **Talk about our central visibility and management across endpoints, servers, gateways, breach detection, and SaaS.**
- **Tell our Connected Threat Defense story: how they can use our industry-leading Deep Discovery breach detection & sandboxing with endpoints and email to automatically protect with real-time local signatures for zero-day threats.**