

# XGen Endpoint Security - Winning Against Symantec suites

## The Challenge and Opportunity

Symantec lost their way several years ago with constant management changes. Symantec customers are frustrated by a lack of performance and innovation in their solutions.

## 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		Symantec		
	Smart Protection Endpoints	Smart Protection Complete	Endpoint Suite	Endpoint Suite w/ Email	Protection Suite Enterprise
<b>Central Management</b>	✓	✓	✓	✓	✓
<b>Endpoint Security</b> Anti-malware, machine learning, Encryption, web filtering, intrusion prevention, desktop virtualization	✓	✓	✓	✓	✓
Predictive machine learning for both file and process analysis	✓	✓	P	P	P
Application Control w/ dynamic rules	✓	✓	P	P	P
Integrated Endpoint DLP	✓	✓	✗	✗	✗
SaaS/hybrid deployment option	✓	✓	✗	✗	✗
<b>Mobile Security</b>	✓	✓	✓	✓	✓
<b>Email Security</b> On premise email gateway, SaaS email gateway, email encryption, mail server	✗	✓	✗	✓	✓
Integrated Email DLP	✗	✓	✗	✗	✗
API based Office 365 protection	✗	✓	✗	✗	✗
Email APT protection	✗	✓	✗	✗	✗
<b>Collaboration Security</b> SharePoint server protection & DLP	✗	✓	✗	✗	✓
SaaS: Office 365 SharePoint, OneDrive, Box, Dropbox, Google; threat & DLP	✗	✓	✗	✗	✗
<b>Web Security</b> Web filtering, application control	✗	✓	✗	✗	✓
Integrated Web DLP	✗	✓	✗	✗	✗
On-premise	✗	✓	✗	✗	✓
SaaS deployment option	✗	✓	✗	✗	✗

## Trend vs. Symantec Capabilities

			Comments
Anti-Malware & Performance (top AV-Test scores 2014-2016)	★★★★	★★	Trend performing best over 2.5 years of testing at AV-Test.org. Symantec touts a sponsored AV-Comparative test using their latest product vs. an old version of OfficeScan with 2 critical features turned off.
Machine Learning	★★★★	★	Trend has 11 years experience with machine learning for spam and website analysis. Unlike other vendors Trend uses endpoint machine learning in <u>both</u> file and process analysis and combines it with other techniques to reduce false positives. Symantec offers pre-execution machine learning only.
Intrusion Prevention	★★★★	★★	Trend incorporates superior technology from our Deep Security product line. Symantec lacks platform support & is slow on patches.
Application control	★★★★	☆	Trend has full endpoint app control. Symantec claims to have app control but is missing basic functionality - no cloud-based app list or categories (admin must know the exact file name/file path or checksum to block it), no user-based policies, no gold image/ trusted machine, and lock-down is painful.
Behavioral Analysis & Sandboxing	★★★★	★	Trend more experienced sandbox analysis, lateral movement detection, prevalence scoring integration, ransomware protections. Symantec was late to offer anything in this area and has struggled to catch up.
Ransomware Protection and Visibility	★★★★	★	Trend includes specific technologies to detect, stop, and restore encrypted files from ransomware and visibility into ransomware detections. Symantec doesn't offer anything specifically designed for ransomware.
Endpoint web filtering	★★★★	★	Trend uses kernel based technology to catch C&C call backs outside of the browser. Symantec is browser based and easily defeated.
Data Loss Prevention (DLP)	★★	Missing from suite	Trend integrated DLP is simple to setup and manage. Symantec has strong enterprise-class DLP but it's an expensive add on and hard to deploy.
Cloud App Security for Office365 & cloud file sharing	★★★★	No offering	Unique capability for Trend. Like other vendors Symantec has a SaaS web gateway which can protect Office inbound email but not internal email, SharePoint, OneDrive, Box, Dropbox.
Email APT protection	★★★★	Missing	Email sandbox malware analysis included with Hosted Email Security and Cloud App Security.
SaaS Offerings	★★★★	★	Trend includes SaaS offerings for endpoint, email, SaaS applications, and web. Symantec has limited endpoint SaaS capabilities and includes SaaS email security but not SaaS web security or 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 information then presents them all in an intuitive user view. Symantec clunky on synthesis across layers and no user centric visibility into security events making it difficult for admins spot trends.
Suite deployment	★★★★	★	Trend has simplified the suite experience with a single deployment kit, activation key, and user-based licensing 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.

## 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. Symantec in the Gartner Magic Quadrant (MQ) for Endpoint Protection?** Trend Micro is positioned as a “Leader” – a position we have held for 15 years. In the 2017 MQ, Trend Micro is now clearly in the top, right position of the Leader's quadrant surpassing Symantec on both execution and vision. See the [Trend Responds document](#) from Sales Hub and Trend Micro has secured distribution rights to share the MQ with your customers.

**Data Loss Prevention (DLP) is too complex and difficult to implement!** With Symantec this is the case but Trend Micro has taken a simplified approach to DLP by incorporating all of the functionality that customers require into our existing endpoint, messaging and collaboration, and web security solutions. Our integrated DLP (iDLP) functionality is centrally managed with Control Manager.

**I just need endpoint and email protection not web.** Besides endpoint, web and email our Smart Protection Complete suite includes collaboration security. We secure on-premises SharePoint and IM servers. Now we also include a cloud security gateway to provide advanced threat and DLP functionality for SaaS applications including Office 365, Box, Dropbox and Google Drive. This enables you to embrace the efficiency of the cloud while maintaining security.

**I know Symantec well but not Trend Micro.** We invest in great products instead of great advertising! Trend Micro has delivered top rated security solutions for over 25 years and is trusted by 48 of the top 50 global corporations. On the other hand, Symantec seems to have lost its way several years ago with continual management and strategy changes. Customers are moving to Trend Micro for our constant commitment to security.

## 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 Symantec 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

- **Show our leadership in the Gartner Magic Quadrant.**
- **Share our white paper on how we synthesize machine learning with our techniques for maximum protection and accuracy**
- **Talk about our central visibility and management across endpoints, servers, 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.**