







XGen™ Endpoint Security--Winning Against “Next-Gen” Endpoint

The Challenge & Opportunity

Upstart competitors that are being referred to as “next-gen” endpoint players are promoting the value of advanced endpoint protection and customers/prospects are listening and interested which is good for the endpoint security market. The challenge is that many of these next-gen competitors are trying to position Trend as old school technology that only has traditional signature-based AV which is not true. Our opportunity is to inform customers that not one of these vendors provides enough protection. XGen Endpoint Security delivers the most complete blend of cross-generational threat defense techniques that intelligently apply the right technique and the right time and gives IT the centralized visibility and management simplicity they require.

Trend XGen Endpoint Capabilities vs. Next-Gen Endpoint Players

(NOTE: Cylance is not included here – there is a dedicated Cylance Competitive Sell Sheet on Sales Library)

							Comments
Independent testing (i.e. not sponsored by vendor)	★★★	Missing	Missing	Missing	Missing	Missing	Trend performing best on 0-day & performance with independent labs (i.e. AV-Test, NSS Labs).
High Fidelity Machine Learning (pre-execution & runtime, with noise cancellation)	★★★	★	Missing	Missing	Missing	Missing	CrowdStrike claims machine learning but no proof points. Trend Micro noise cancellation with Census & whitelisting checks.
Exploit Prevention + HIPS	★★★	★	Missing	Missing	★	Patching	Only Trend provides host-based intrusion prevention (HIPS).
Application Control	★★★	Missing	★★★	Missing	Missing	Missing	Carbon Black missing dynamic rules based on prevalence, maturity, regional usage for user environments.
Sandboxing	★★★	Missing	Missing	★★	Missing	Missing	Trend a leader according to NSS Labs. Palo Alto has cloud sandboxing only.
File reputation, variant protection, behavioral analysis	★★★	Missing	★	★	★	Missing	Hard to tell if Palo Alto has anything here, Carbon Black made a recent acquisition but still separate product & unproven.
Web reputation & browser exploit protection	★★★	Missing	Missing	Missing	Missing	Missing	Only Trend providing web specific protections.
Encryption, Device control & DLP	★★★	Missing	Missing	Missing	Missing	Missing	Only Trend has data protection for compliance.
Investigation & Forensics (EDR)	★★	★★	★★★	Missing	★★	★★	Palo Alto missing.
Mobile & Mac platforms	★★★	★	★	Missing	★	Missing	Carbon Black has Mac support for app control only.
Scalability, Central Visibility & Management, Cloud deployment	★★★	★	Missing	Missing	Missing	Missing	Trend has strong central management, user-based visibility and reporting.

CONFIDENTIAL – NOT FOR GENERAL DISTRIBUTION

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.

CrowdStrike

- **What is it?:** Cloud-based deployment & management . They come out of the EDR market with investigation and hunting capabilities but this technology is highly reactive in nature (i.e. finds things after they have executed or been in on your endpoint for a long time. They claim to have machine learning as well which is pro-active in nature but no testing claims to see if it works effectively or not.
- **Poor detection beyond Executables:** Machine learning is usually only good at detection on Windows PE (Executable) type files but doesn't work as well on scripts and macros which Trend would catch.
- **High false positive rates:** Machine learning is known for having higher false positives (false positives are huge head-ache for users and for the administrators who have to take the help desk calls and try to fix the problems).
- **"Independent" 3rd Party Test Results:** No independent 3rd party testing exists showing their ability to protect against malware or threats.
- **Gartner EPP Magic Quadrant:** CrowdStrike did not meet the criteria that 20 other vendors met to be included in the Gartner endpoint MQ. Trend Micro is in the top right position of the leader's quadrant.
- **No on-premises offering:** CrowdStrike is a cloud only option so customers have to trust their endpoint & network info and security policies to the CrowdStrike cloud environment.
- **Multiple agents & management consoles:** CrowdStrike like other next gen vendors will usually recommend that you deploy their agent on top of your existing antimalware solution, so now you have at least 2 agents and 2 management consoles. Trend does all of the same protection from one agent and one management console.
- **No vulnerability, exploit shielding and virtual patching:** CrowdStrike does not provide host-based intrusion prevention (HIPS) & lateral movement detection like Trend.
- **No data protection (device control, DLP, encryption), no mobile protection**
- **No Web reputation & browser exploit protection:** CrowdStrike doesn't have these technologies that prevent users from downloading and executing malware via email, web browsing or other social media activities and applications.

Bit9 & Carbon Black

- **What is it?:** Carbon Black has 3 separate products 1. application control / whitelisting 2. Investigation and forensics (EDR) solution 3. File reputation for antimalware. The file reputation is their recent acquisition of Confer.
- **Poor detection beyond Executables:** Application Control only stops executables, misses malicious PDFs, macros in files, etc. Can't detect a good file trying to do malicious activity or privilege elevations within existing legitimate applications.

- **No intrusion prevention or virtual patching:** Can't protect against network-based application or vulnerability exploits. Requires IPS or virtual patching that Trend provides.
- **Adding applications is a head-ache:** Every time you want to add a new application (which happens frequently particularly in dynamic user environments), the user must file a help desk ticket and the admin must perform a forensic investigation to find out if that application is a good application or is in fact malicious. Antimalware threat research and the associated technologies (i.e. Trend Micro and not Carbon Black) reduce this tremendous time burden to only the items that are truly unknown to threat researchers. Because of this, they have recommended that customers use Microsoft antivirus (but per AV-Test.org this is the most ineffective antimalware solution with catch rates only around 70%), they may recommend the Confer file reputation now but it is also unproven.
- **No web reputation or browser exploit prevention:** no ability to block based on web reputation or to proactively prevent malicious web sites from leveraging Java or ActiveX vulnerabilities in the browser.
- **No DLP or encryption for data protection.**
- **Investigation & Forensics (EDR):** The Carbon Black technology is similar to Trend Micro's Endpoint Sensor which performs the investigation & forensics capabilities. However, this investigation technology also has limitations as it doesn't proactively protect the organization from threats & malware. Analysts have told us that it demonstrates many false positives.
- **Central visibility, cloud deployment do not exist**

Palo Alto Networks (Traps)

- **What is it?:** Palo Alto Networks acquired an endpoint company called Cyvera
- **Complementary to antimalware?:** Perhaps but much less comprehensive and no independent 3rd party testing to prove that it actually stops anything that Trend otherwise would.
- **Zero Trust?:** They talk about this notion of zero trust, which is essentially looking at malicious behavior that might be occurring within an application or between processes and then they send it to the cloud sandbox. Trend has machine learning behavioral techniques to block unknown malware.
- **No signatures:** Traps has no signatures to detect known malicious documents and executables so if their behavior engine detects a file as suspicious it must go to the cloud sandbox and if it doesn't detect it then it passes.
- **Palo Alto's WildFire cloud:** is sandboxing only and far less robust than the Trend Micro Smart Protection Network (SPN) cloud. We have file, web, email reputation, census data, and application whitelisting in our cloud ensuring more accurate & better protection.

- **Dynamic Analysis (Sandboxing):** is done in the WildFire cloud but due to sandbox evasion techniques it cannot completely replace threat researcher expert judgment (that Trend provides via SPN).
- **No vulnerability shielding, DLP, encryption, forensics:** Trend provides broad endpoint coverage that Palo Alto does not like device control, DLP, vulnerability protection, incident investigation, and encryption.
- **Application Control?:** For application whitelisting the Traps administrator has to add applications manually. This does not meet the basic definition and compares poorly to our full application whitelisting, which has a massive catalog of safe applications to choose from + dynamic rules to allow applications with a good reputation (prevalence, maturity, regional usage), and lastly the ability for trusted sources of updates.

SentinelOne

- **What is It?:** Cloud-based deployment & management . They also came out of the EDR market with investigation and hunting capabilities but this technology is highly reactive in nature (i.e. finds things after they have executed or been in on your endpoint for a long time. SentinelOne has behavioral analysis only which can lead to more infections and they lack any whitelisting or Census checks to reduce false positives that are common with behavioral based technologies.
- **VirusTotal file information:** VirusTotal is the largest and best source of malware and bad file information that multiple vendors share in to as a community of malware researchers. SentinelOne have been removed from using this information because they do not share in to the community and instead have been using the research of others to build their product. SentinelOne have tried to say that they do not need the VirusTotal information but because VirusTotal is the best and most definitive source of known bad files, it can't help but affect their ability to train the machine learning algorithms (see more on this in the Trend Responds document but machine learning requires constant training from files that are 100% confirmed as "bad" and "good" files).
- **High false positive rates:** Behavioral analysis is known for having higher false positives (false positives are huge head-ache for users and for the administrators who have to take the help desk calls and try to fix the problems).
- **"Independent" 3rd Party Test Results:** SentinelOne have only participated one time in May/June 2015 in AV-Test and their detection rates were average and significantly below Trend Micro.
- **Gartner EPP Magic Quadrant:** Trend Micro is in the top right position of the leader's quadrant for 2016 and cautions that SentinelOne do not have key EPP (endpoint protection platform) functionality is missing.

- **No on-premises offering:** SentinelOne is a cloud only option so customers have to trust their endpoint & network info and security policies to the SentinelOne cloud environment.
- **Multiple agents & management consoles:** SentinelOne like other next gen vendors will usually recommend that you deploy their agent on top of your existing antimalware solution, so know you have at least 2 agents and 2 management consoles. Trend does all of the same protection from one agent and one management console.
- **No vulnerability, exploit shielding and virtual patching:** SentinelOne does not provide host-based intrusion prevention (HIPS) & lateral movement detection like Trend.
- **No data protection (device control, DLP, encryption), no mobile protection**
- **No Web reputation:** SentinelOne does not have this technology that prevents users from downloading and executing malware via emails, web browsing or other social media activities and applications.

Tanium

- **What is it?:** They focus on incident detection & non-protection techniques. They claim to be an additional layer for endpoint security with their focus on incident detection, configuration compliance, vulnerability assessment, asset inventory, patch management, software distribution and a bit of endpoint investigation. This is usually competition for people like Microsoft System Center Configuration Manager (SCCM), BigFix (now IBM), LANDesk/Shavlik and would complement Trend Micro endpoint protection.
- **Vulnerability Assessments & Patching:** On the vulnerability assessment piece they have, you can talk about how our vulnerability shielding and virtual patching technology offers much quicker time-to-protection over patch management. That we also offer IPS signatures to detect lateral movement which is critical to detecting & decreasing the dwell time of malware that has gotten on to your network.
- **Query machines in seconds:** They claim to be able to query the machine in seconds to look for vulnerabilities and threats but you have to know what to query for (i.e., you need an IOC feed from someone else). So this would compete on some level with our Trend Micro Endpoint Sensor but without the valuable detecting of new threats via the Deep Discovery sandboxing.
- **Not pro-actively protecting from threats & malware:** What they aren't doing and is so critical to any endpoint protection is actually provide anti-malware or threat protection. So keep that in mind and make sure you talk about not just responding to threats but actually protecting from threats, malware, etc.

Questions to Ask Customers:

- **What kind of independent, 3rd party testing or analyst reports have they participated in?**
There are very few truly independent 3rd party labs for testing endpoint security technology (AV-Test.org, AV-Comparatives and NSS Labs are the only ones). Other “3rd party” tests are paid for by the vendor and therefore they dictate the terms of the testing and what specific features to look at versus the competitor(s). Most of these next gen endpoint players are not participating in the independent testing. The analysts like Gartner do not recognize most of these players as meeting the criteria for the endpoint (EPP) magic quadrant whereas Trend has been in the “leaders” quadrant for 13 years now.
- **Will you need to learn and use security products from multiple different vendors with multiple management consoles to get the security coverage you need?**
How will the management for those different products work? Will you have visibility across a user’s devices and multiple platforms for rapid response? How will you manage cloud and on-premises security? Do the products talk to each other and when one detects a threat notifies and blocks it with other technologies on the network?
- **How are you tackling patch management or zero-day protection against vulnerabilities?**
How did you respond at the endpoint to vulnerabilities in your applications? How are you ensuring that network-based vulnerabilities that exploit a specific application are protected? Are legacy operating systems like Windows XP in your environment, for which no patches are being made available?
- **How are you detecting threats and malware that get inside your network?**
Does your endpoint product look for Command & Control traffic or detect lateral movement from one system to another? Does your endpoint integrate with internal network breach detection technology and investigation and forensic capabilities?
- **How is the vendor providing machine learning with high fidelity?**
Does the vendor provide machine learning for both pre-execution and runtime analysis? What if anything are they doing to cancel the noise of false positives with whitelisting or other?
- **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 operating systems (Windows, Mac, Linux), web-based applications, cloud storage — as well as mobile devices (iOS, Android, Blackberry)?
- **What are you doing to protect point-of-sale devices, financial, or healthcare endpoints?**
Are you considering application whitelisting technology to prevent any unknown software from executing? Protecting against MalumPOS, memory scrapers, and other specialized malware on these critical POS endpoints in your environment.
- **How are you providing data protection for your organization?**
How do you protect against laptops being stolen or lost with encryption? How are you protecting against users sharing confidential information with DLP (via all the channels today like email, cloud storage, IM, USB, mobile devices, and web)? Are there compliance regulations to enforce?
- **What is their customer service & support coverage model?**
Does the vendor have 24 x 7 coverage and local people in your region to provide the best account and technical support for your critical security infrastructure?

The 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 2.5 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: Trend Micro has 25+ years of continuous innovation. Gartner “Leader,” and highest vision score, InfoTech “Champion,” Ovum “Leader,” SC Magazine 5-Star Rating with comprehensive protection for advanced threat protection.

Remember to?

- **Use the Gartner Endpoint Magic Quadrant on sales library to demonstrate our extensive advanced protection capabilities.**
- **Talk about our central visibility and management across endpoints, servers, breach detection & sandboxing, etc.**
- **Show the latest AV-TEST (independent testing) that demonstrates that we are the best at stopping new zero-day.**
- **Tell our Connected Threat Defense story: how they can use and connect breach detection & sandboxing, email & web gateways with the endpoint to automatically protect with real-time local signatures for zero-day threats.**