

Trend Micro

ENDPOINT SECURITY BUYERS GUIDE

There's a lot of noise in the security market. It's becoming harder to separate the hype from the true benefits of an effective endpoint security solution. In addition, security threats continue to become more advanced, making it more important than ever to choose a forward-looking solution that continually evolves with the changing threat landscape.

The Endpoint Security Buyers Guide is a navigational tool designed to define the various benefits needed in a security solution, helping you differentiate between the various threat detection, protection, and investigative capabilities currently flooding the market.



TABLE OF CONTENTS

[» CLICK ON A BENEFIT FOR FULL DESCRIPTION](#)

AUTOMATED DETECTION AND RESPONSE

Anti-Malware/Malware Scanning	8
Provides first-wave of protection against known threats.	
Application Control (Whitelisting and Blacklisting)	6
Determines if an application should be allowed or blocked.	
Automated Response Techniques	9
Immediately removes threats, isolates the endpoint, and prevents the threat from spreading.	
East-West/Lateral Movement	8
Detects movement that is typically indicative of a breach of data.	
Endpoint Isolation/Threat Quarantine	8
Isolates or quarantines infected endpoints.	
In-Memory Runtime Detection	6
Provides threat detection techniques for specialized threats.	
Packer Detection	7
Detects threats before they unpack and execute.	
Pre-Execution Machine Learning	4
Detects unknown threats found in executable style files.	
Rollback	9
Revert endpoint back to pre-infected state.	
Runtime Behavioral Analysis	5
Detects unseen threats before they execute.	
Runtime Machine Learning	5
Uses rule sets to analyze and discover unknown malware.	
Sandbox Submission (On-Premises and Cloud)	7
Determines whether files are malicious by executing or detonating files in a safe environment.	
Terminating a Process	9
Automatically terminates a malicious process	
URL and Web Reputation Filtering	7
Prevents access to unsafe sites before malicious activity can take place.	
Variant Protection	8
Deletes malware threats that are modifications of existing known threats.	
Virtual Patching (Intrusion Prevention)	6
Keeps machines protected even if they aren't up to date with the latest patches.	

DATA PROTECTION

Data Loss Prevention (DLP)	10
Secures sensitive data such as financial and customer information or intellectual property.	
Device Control	11
Prevents transfer of sensitive data to external devices such as USBs and external hard drives.	
Encryption	11
Ensures that data stored on a lost or stolen endpoint is protected from malicious action.	

INVESTIGATION AND CENTRALIZED VISIBILITY

Alerts, Timelines, and Threat Information Visibility	14
Provides users with centralized visibility across their entire environment.	
Metadata Collection (Server Side Sweep)	12
Provides a quick snapshot about the recorded telemetry stored on the endpoint.	
Recording Endpoint Events (Telemetry)	12
Records all actions that happen on the endpoint so threat researchers can retroactively query infected endpoints for certain suspicious actions.	
Root Cause Analysis (RCA)	13
Shows all the events that have occurred on an infected endpoint.	
Patient Zero Identification	13
Find the first endpoint or user affected by malware.	
Real-Time IOC Search and Sweeping	13
Queries an endpoint in real time to search for an indicator of attack (IOC).	
Support for Managed Detection and Response	14
Provides managed threat hunting and response services on behalf of customers.	
Unknown File Guidance	14
Provides users with a guided view to alerts, prioritizing threats that require immediate action.	

MANAGEMENT

API Capabilities	15
Connects third-party management and automation platforms.	
Compliance	17
Ensures employees and users adhere to corporate IT policies related to securing endpoints.	
Language Support	16
Provides multi-language care for end users.	
Open IOC Integration	16
Allows for easy identification and characterization of attack indicators.	
Role-Based Access Control for Administrative Features	15
Provides a reporting console to tailor reports and alerts to different functional groups.	
SIEM Integration	15
Sends security events from various controls.	
Support for PC and Mac Endpoints	17
Endpoint care for both operating systems.	
Threat Information Sharing and Distribution	16
Communicates threat information to other security layers.	

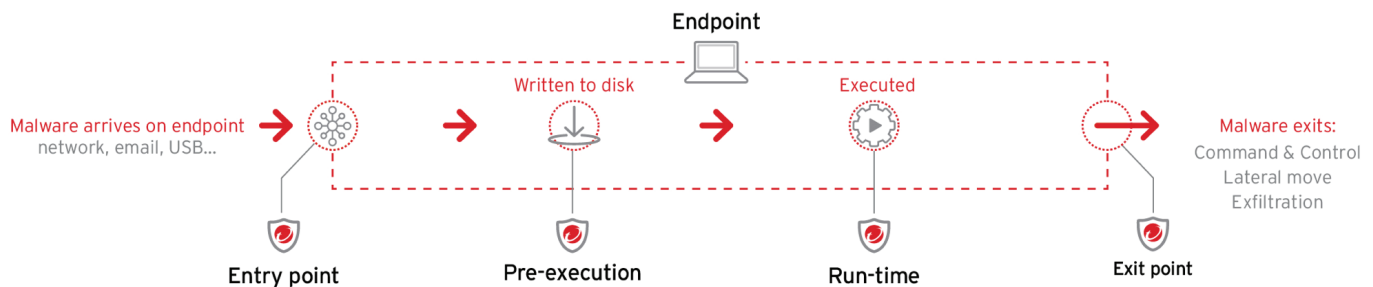
ARCHITECTURE

Easy Upgrade and Deployment Process	19
Provides multiple deployment options to meet existing organizational practices.	
Efficient System Architecture	20
Comprehensive feeds tailored towards active real-world threats.	
Geographic Availability (for SaaS and MDR)	19
Global coverage for both threat analysis and data storage.	
Global Support	20
Provides support to customers anywhere, anytime.	
Scalability	18
Allows security platform adapt and grow without adding complexity.	
Security as a Service (SaaS) and On-Premises Deployment Options	20
Provides flexibility of how to deploy security, with complete product parity between the two.	
Single Interface for Accessing Endpoint Protection Platform (EPP) Functions	18
Provides a common pane of glass to visualize both EPP and EDR functionality and alerts.	

AUTOMATED DETECTION AND RESPONSE

Given today's complex security landscape, it's important for organizations to use a combination of advanced threat protection techniques to eliminate security gaps across any user activity and any endpoint in the organization.

You can no longer rely on single threat detection techniques such as machine learning or AI to find all types of threats, you need to leverage a blend of advanced techniques, like pre-execution and run-time machine learning, behavioral analysis, application control, vulnerability protection, and more for comprehensive protection. It's also important to ensure your endpoint security solution is constantly learning, adapting, and automatically sharing threat intelligence across your entire environment.



It is important to secure your endpoint with complete protection, from the point where malware arrives to its exit point.

Pre-Execution Machine Learning

Detects unknown threats found in executable style files.

Why is this Important?

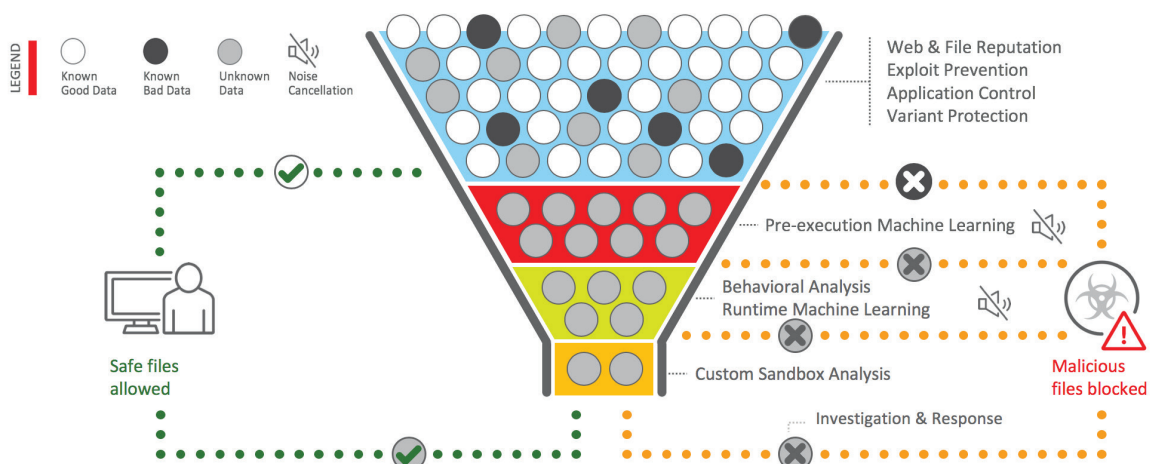
- It allows you to protect against new targeted attacks with no known patterns associated with it, but which still possess malware characteristics.
- Machine learning looks at the attributes of an executable file and determines if it has malware characteristics.
- Makes decisions based on attributes, not on if the engine has seen that pattern before.

What to Look For

- An endpoint solution that doesn't only rely on machine learning to avoid resource-intensive threat detection methods, which are prone to false positives.
- A multi-step approach to threat detection.
- Noise cancellation (census).

Trend Micro Approach

- Trend Micro Apex One™ predictive machine learning scores files against a cloud-based or local/offline model to detect previously unknown threats.
- Our cross-generational approach blends in other detection capabilities to drastically reduce false positives caused by machine learning engines.
- Filters out known threats using signature-based techniques, leaving only a small number of unknown files for use in resource-intensive techniques (that may slightly be more prone to false positives), like machine learning.
- Employs "noise-cancelling" techniques to further reduce false positives. This includes census checks (to look at the prevalence and maturity of files) and our global whitelist (which contains 1 billion known good files).



Runtime Machine Learning

Uses rule sets to analyze and discover unknown malware, and fileless threats that are not detected during pre-execution but as they are executed.

Why is this Important?

- Most malware doesn't have a traditional "signature" to identify it, so advanced rules examine malware attributes for detection.
- Combined with other detection techniques, this provides an advanced detection capability.
- Advanced malware can bypass certain types of machine learning as they often arrive inside scripts or attached to existing benign files which might get missed by pre-execution machine learning engines.
- Detecting "fileless malware" requires a separate run-time machine learning engine is required to identify malicious processes that are only visible during runtime.

Trend Micro Approach

- Uses advanced runtime machine learning capabilities to closely monitor files and programs that are being executed (like a program, a script, a document), comparing that behavior against a model to detect threats.
- This machine learning model is completely separate from the pre-execution machine learning model to give you two separate and very effective threat monitoring methods for fewer false positives.
- Develops new rules and updates on machine learning models more often than many in the industry to detect the latest in advanced malware.
- Machine learning engines benefit from continuous threat information being fed into it through multiple sources of data (sensors).
- Trend Micro's extensive database of threat intelligence and ongoing research give a superior view of new threats entering the landscape, feeding that knowledge and research into our detection engines, including machine learning models, for better accuracy.



What to Look For

- Runtime machine learning to detect fileless malware during execution.
- Frequent update of machine learning models using up-to-date threat information.

Runtime Behavioral Analysis

Detects unseen threats before they execute.

Why is This Important?

- While many threats are detected before runtime, there are some threats you just won't see until they execute, such as malware hidden in PowerShell scripts or other fileless attacks.

Trend Micro Approach

- Uses behavioral analysis to monitor harmful and suspicious behavior, such as rapidly encrypting files or the exfiltration of sensitive information.
- Our behavioral analysis engine provides a clear indicator if an attack (including ransomware and fileless malware) is taking place based on specific behaviors and suspicious indicators of attack (IOA).
- Adding new IOAs to continually boost rules set in the engine to detect new suspicious behavior.



What to Look For

- Behavioral analysis engines updated with the latest in global threat information.
- Continuous learning and adapting behavior models.
- Ability to detect advanced threats such as fileless malware and ransomware.

In-Memory Runtime Detection

- Provides threat detection techniques for specialized in-memory threats.

Why is This Important?

At times endpoints come across threats that execute only in memory and never in a file, certain traditional techniques cannot detect these types of threats.

Trend Micro Approach

- Apex One uses in-memory runtime detection to look for and stop malicious script behavior in memory and malicious code injections.
- Stops threats even after a script has started running, and can revert harmful actions.

What to Look For

- Ability to detect malicious script behavior in memory.

Application Control (Whitelisting and Blacklisting)

Determines if an application should be allowed or blocked from running on endpoints.

Why is This Important?

- To determine if an application should be allowed or blocked, endpoint solutions need to understand what that application is trying to do.
- Some organizations want to identify a set of approved applications and not allow any other executables to run outside of this approved configuration (whitelisting), while others would rather add to a list of apps not permitted (blacklisting).

Trend Micro Approach

- Trend Micro's application control policies and rules allow for granular and flexible whitelisting and blacklisting, so organizations can only allow select applications to run (whitelisting) or allow all applications to run except those that have been blocked (blacklist).
- Performs an inventory of the applications running on the endpoint and use that to inform a lockdown policy unique to every organization.
- Dynamic rules combined with Trend Micro app rating service enables administrators to automatically approve safe apps.
- Apex One provides users flexibility and granularity when it comes to what they want to allow and block to help with overhead administrative tasks.

What to Look For

- Both blacklisting and whitelisting capabilities.
- Flexible and granular controls over allowed and blocked lists.
- Offline mode with ability to update programs as needed.

Virtual Patching (Intrusion Prevention)

Keeps machines protected even if they aren't up to date with the latest patches.

Why is This Important?

- Keeping endpoints fully patched and protected is a challenge many organizations feel.
- Protects against new malicious threats by keeping machines stay up to date with security patches.
- Provides an effective defense against malware trying to exploit security vulnerabilities.

Trend Micro Approach

- Provides organizations with the industry's most-timely virtual patching.
- Trend Micro™ Vulnerability Protection™ virtually patches known and unknown vulnerabilities, for instant protection, often before a patch is available or deployable.
- Trend Micro endpoint, network, and cloud solutions have early access to new vulnerabilities through our work with the Zero Day Initiative (ZDI) and our acquisition of Telus Security Labs.
- Vulnerability Protection offers a flexible approach to virtual patches, giving full control over which vulnerability filters you turn on, cutting down on administrative overhead to help security teams stay one step ahead of new exploits.
- Anticipates the rise and fall of threats and dynamically adapts products to meet threats without any user interaction.

What to Look For

- Vulnerability patching, as opposed to simple vulnerability assessments, to ensure proactive protection.
- Data filtering across vulnerabilities.

URL and Web Reputation Filtering

Prevents access to unsafe sites before malicious activity can take place.

Why is This Important?

- Employees have no real way to know if a website is unsafe until they open it, and a good endpoint protection solution should prevent access before malicious activity can occur.
- Most malware attempts to reach out to particular web addresses that are known to be malicious, both within and outside of browsers.

Trend Micro Approach

- Apex One provides dynamically-updated reputation information on websites through integration with the Trend Micro™ Smart Protection Network™ to detect malicious URLs and filter them out.
- Because Trend Micro web reputation technology doesn't rely on a web browser plugin, it can protect HTTP communication at the kernel level, securing communication from applications, enhancing protection and mitigating any damage caused by malware.

Sandbox Submission (On-Premises and Cloud)

Determines whether files are malicious by executing or detonating files in a safe environment.

Why is This Important?

- Not all threats are known good or known bad, certain times your endpoint solution will come across a grey file that needs to be investigated further in a safe environment away from other endpoints.

Trend Micro Approach

- Offers two types of sandboxes; cloud sandboxing and on-premises custom sandboxing, to mimic a real endpoint to "trick" the malware into performing malicious behavior that can be detected and blocked, providing proof of a threat.
- Output from the sandbox can inform other products through APIs, bolstering the overall security posture.

Packer Detection

Detects threats as they unpack and execute.

Why is This Important?

- Certain threats can only be detected once they start to unpack and execute their actions.
- Many pre-execution techniques can't detect these threats, and other run-time capabilities can't impact these threats once they have already started running.

Trend Micro Approach

- Apex One identifies malware as it unpacks prior to execution and blocks threats immediately.
- Techniques such as behavioral analysis are also used to prevent these attacks. Many endpoint solutions only detect these threats without stopping them.

What to Look For

- Continuous update of reputation information backed by extensive threat intelligence.
- Automatic filtering of malicious sites.
- Kernel level detection and blocking across all browsers and applications.

What to Look For

- Customizable sandboxes to mimic actual endpoints.
- Ability to send known grey files to sandbox regardless of on-premises or cloud deployments.
- Sharing threat information across multiple security solutions.

What to Look For

- Automatic identification and blocking of threats during the unpacking stage.

East-West/Lateral Movement

Being able to see later movement of files is important to track and detect data breaches.

Why is This Important?

- The ability to identify data breaches early reduces remediation and prevents spread of threats across the network.

Trend Micro Approach

- Apex One Endpoint Sensor provides a detailed view of lateral movement across endpoints, while Trend Micro™ Deep Discovery™ provides lateral movement detection on the network.
- Apex One with endpoint detection and response (EDR) and/or Trend Micro Deep Discovery Inspector™ will provide a complete picture of the movement of an attack throughout your network.
- Trend Micro managed detection and response (MDR) service can also be tasked with identifying lateral movement and subsequent infections along with providing specific instructions for removal of these threats.

Variant Protection

Detects malware threats that are modifications of existing known threats.

Why is This Important?

- Many new malware threats are modifications of existing known threats, which have been altered in ways to try and avoid detection.

Trend Micro Approach

- Employs variant protection as a standard automated detection technique, and is designed to detect small mutations for a known-bad file.
- Detects entire malware families, even when key sections of a known malware file has been changed to avoid detection.

Anti-Malware/Malware Scanning

Provides a low-overhead, first-wave of protection against known threats.

Why is This Important?

- While this traditional technique will not detect all threats, it is a vital step to efficiently and automatically remove all known malware from the endpoints before they can cause damage.

Trend Micro Approach

- Apex One uses a blend of malware detection techniques, including static analysis, signatures, and file and web databases, to detect and remove known malware.
- Uses non-signature-based detection methods in conjunction with these techniques to detect more advanced and unknown malware threats.
- Frees up more resource-intensive techniques to focus on detecting unknown threats by applying anti-malware techniques first.

Endpoint Isolation/Threat Quarantine

Isolate or quarantines infected endpoints.

Why is This Important?

- Ensures malware or threats do not spread throughout the organization.

Trend Micro Approach

- Apex One can isolate the machine without having to rely on network routers or other third-party infrastructure.

What to Look For

- Detailed view of threat movement between endpoints and across network and servers.

What to Look For

- Automatic removal of known bad files, including malware variants.
- Ability to detect malware families and modified threats.

What to Look For

- Ability to quickly apply malware scanning to remove majority of bad files.

What to Look For

- An endpoint solution that can quarantine and delete harmful files off endpoints without administrative input.

Terminating a Process

Automatically terminates a malicious process.

Why is This Important?

- Ensures threats are immediately and automatically removed before they can spread across endpoints.

Trend Micro Approach

- In addition to isolating and quarantining infected endpoints, Apex One automatically kills harmful processes.
- Can terminate a process for single or multiple users.



What to Look For

- Ability to automatically kill processes without administrative task.
- Can kill processes across multiple endpoints/users simultaneously.

Rollback

Revert endpoint back to pre-infected state.

Why is This Important?

- Ransomware can cause thousands of dollars' worth of damage in the form of lost revenue, ransom payouts, and irreparable endpoint and system damage.

Trend Micro Approach

- Apex One can rollback any damage that has already been done (in the case of ransomware) and revert the machine back to a clean state without having to reimage every infected endpoint, saving administrators time and money.



What to Look For

- The ability to clean infected files and revert machines back to pre-infection state.
- Automated remediation without administrative tasks.

Automated Response Techniques

Immediately removes threats, isolates the endpoint, and prevents the threat from spreading.

Why is This Important?

- Security teams have too many other pressing issues to be constantly dealing with each individual endpoint threat that is discovered and manually implementing remediation actions.

Trend Micro Approach

- Apex One allows our customers to respond to threats in an automated way, without relying on specialized security operations center (SOC) teams or manual intervention.
- Apex One can mitigate damage that has been caused by malware, clean up endpoints and return them to a pre-infected state, saving time lost data, infrastructure or ransom fees.



What to Look For

- Ability to automatically quarantine, isolate endpoints, and kill malicious processes.
- The cleanup of infected endpoints and return to its pre-infected state.

DATA PROTECTION

Whether it is important trade secrets, confidential customer information, or medical records—keeping data secured and protected is a key requirement for endpoint protection solutions. Below are some key capabilities integral to a comprehensive and effective data protection strategy.

Data Loss Prevention (DLP)

Secures sensitive data such as financial and customer information or intellectual property.

Why is This Important?



















- The introduction of the mobile workforce, the use personal devices and consumer applications for work, and the increasing frequency of advanced persistent threats (APTs) have contributed to the rise in data breach incidents.
- Data protection on the endpoint can help protect sensitive data from leaving the endpoint.

Trend Micro Approach

- Apex One applies easy-to-define and easy-to-modify rules to prevent specific types of data from leaving the organization, like credit card information, customer information, and medical records.
- Apex One DLP can take one of several remediation actions; reporting, notifying, logging, asking for justification, or blocking.
- DLP templates can be used to help comply with regulatory regulations such as PCI, HIPAA, and GDPR.
- Apex One DLP has integrated the most commonly-used data loss prevention capabilities to offer protection of sensitive data without the expense and management of a separate solution.

What to Look For

- Templates for common DLP policies.
- Flexible and easy-to-define DLP policies that can be implemented across users, groups, and organization.
- The ability to detect sensitive data like credit card numbers and health and financial information.
- Remediation actions including reporting, notifications, logging, and blocking.
- Ability to prevent data from being copied to external sources, or emailed outside the organization.

	Approach	Channels					
Data in motion (DIM)	 Network	 Email	 Web	 IM	 File sharing	 Cloud Apps	
Data in use (DIU)	 Endpoint	 USB sticks	 CDs & DVDs	 Mobile devices	 External hard drives	 Printouts	
Data at rest (DAR)	 Discovery	 Mobile Devices	 Databases	 Mail archives	 File Shares	 Content Mngt.	

Device Control

Prevents transfer of sensitive data to external devices such as USBs and external hard drives.

Why is This Important?

- Controlling and monitoring what external devices can be used with your endpoints is vital to keeping sensitive information safe.

Trend Micro Approach

- Apex One device control allows users to implement policies to determine which devices can be plugged in and used with protected endpoints.
- Trend Micro™ Data Loss Prevention™ (DLP) allows you to specify manufacturers or serial numbers of specific USBs, providing granular control over devices.



What to Look For

- Granular control over which devices can be used with secured endpoints.
- Control of external devices such as USBs and hard drives.
- Policies to control which types of data storage options can be used.

Encryption

Ensures that data stored on a lost or stolen endpoint is protected.

Why is This Important?

- Many regulatory and industry-specific security frameworks mandate encryption as a “safe harbor” from data breach fines and notification requirements.

Trend Micro Approach

- Apex One employs both full-disk encryption as well as file/folder and removable media encryption so users can encrypt entire hard drives or can select certain sensitive files or folders for added levels of encryption.
- Apex One can also be used as an encryption key manager for organizations that rely on Microsoft® Windows® Bitlocker encryption or Mac File Vault encryption.
- Apex One's full disk encryption product encryption is integrated into DLP policies, so they can work in tandem.



What to Look For

- Full disk encryption.
- File/folder encryption.
- Encryption key management.
- Integration with other data protection capabilities, allowing for the creation of strong and unique policies.

INVESTIGATION AND CENTRALIZED VISIBILITY

Investigation, detection, and response is becoming an important add-on to any endpoint security solution. Organizations are increasingly looking for endpoint detection and response (EDR), as well as augmenting their current security operations center (SOC) with managed detection and response (MDR).

While EDR is very important, it provides a limited scope of view. Commonly organizations are leveraging multiple solutions in order to gain the additional visibility of threats outside of the endpoint. For the most effective investigation results, solutions need to provide a holistic picture of the entire environment including telemetry from the network, cloud workloads, containers, servers, workstations, and the most prolific threat vector, email.

Recording Threat Events (Telemetry)

Records all actions and system behavior on the endpoint, as well as threats across email and servers, allowing threat researchers to retroactively query infected endpoints, servers, and inboxes for suspicious actions.

Why is This Important?

- Recording endpoint activity is an important part of any endpoint detection and response solution as it allows users to look back in time and see what happened on the endpoints before and after a detection. Additional enrichment through recorded email activity allows for greater visibility into the source and additional recipients.
- The length of time data is stored directly impacts how far back researchers can investigate endpoint attacks.

Trend Micro Approach

- Trend Micro Endpoint Sensor (EDR)—offered both as an on-premises solution and available as a service—records end user telemetry (network events, processes, system and user behaviors, alerts, commands).
- Information is stored on endpoints and “meta data” is sent to the Trend Micro Apex Central™ server so threat investigators can query or “sweep” for indicators of compromise (IOCs).
- Threat investigators can then isolate endpoints with an IOC and perform a Root Cause Analysis (RCA) to determine the cause and spread of the malware. Once identified, a number of response options are available.
- Trend Micro™ Endpoint Sensor, XDR Edition provides detection and response across endpoint, email, and servers, allowing investigators to explore detections and hunt for new threats across multiple security layers. This cross-layer detection and response is available as a service only.

What to Look For

- Security as a service (SaaS) and on-premises deployment options.
- Flexible data storage options for SaaS options.
- Efficient recording of user telemetry, network events, processes, system events, and more.
- Integrated workflow with one console for EDR and endpoint protection platform (EPP).
- Flexible searching across multiple parameters.
- Added vendor intelligence and threat information.
- Immediate response options.
- Advanced threat hunting using IOAs.
- Cross-layer detection and response across endpoint, email, and servers.

Metadata Collection (Server Side Sweep)

Provides a quick snapshot about the recorded telemetry stored on the endpoint.

Why is This Important?

- If the need for an investigation occurs, any threat researcher who wants to look for a specific hash key or a certain behavior can look through the metadata and get an instantaneous response.

Trend Micro Approach

- Trend Micro Endpoint Sensor performs a server-side metadata sweep so researchers can search the metadata for indicators of compromise (IOCs) on all endpoints, online or offline.
- Dramatically lessens the data that needs to be centrally stored and managed.

What to Look For

- Efficient collection of endpoint information.
- Ability to perform a server-side metadata sweep.

Root Cause Analysis (RCA)

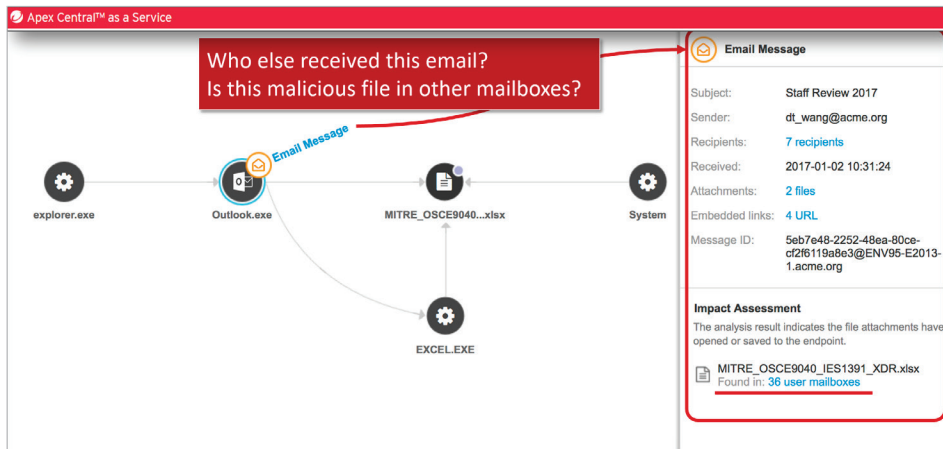
Shows all the events that have occurred on an infected endpoint leading up to a detection.

Why is This Important?

- Gives threat investigators visibility to the source, spread, and remediation required.

Trend Micro Approach

- Apex One Endpoint Sensor provides a graphical or tabular representation of infected endpoints and servers, allowing threat researchers to determine how a malicious threat got on the endpoint, including tracking it down to the originating email and tracing where the malware spread.
- The Root Cause Analysis shows lateral movement of the threat across your network, and other endpoints that may have been infected.



What to Look For

- Graphical representation of malware infections across email, endpoints, and servers.
- Ability to push immediate response to individual endpoints.
- A detailed investigation into a specific infection.

Patient Zero Identification

Find the first endpoint or user affected by malware.

Why is This Important?

- Patient zero needs to be identified quickly and accurately to ensure no further spread of threats.

Trend Micro Approach

- Sweeping for the IOCs of a detection can determine the number of endpoints that were compromised before the particular item was deemed suspicious or harmful.

What to Look For

- Quick and accurate patient zero identification.

Real-Time IOC Search and Sweeping

Queries an endpoint in real time to search for an indicator of compromise (IOC).

Why is This Important?

- Threat researchers need to determine if an IOC is present on their endpoints, which generally indicates a high chance of attack.

Trend Micro Approach

- Endpoint Sensor can perform “live investigation” and provides the ability to search for particular IOCs or various other criteria when scanning endpoints.

What to Look For

- Real-time scanning for IOCs.
- Ability to search across various criteria.

Support for Managed Detection and Response (MDR)

Provides managed threat hunting and response services on behalf of customers.

Why is This Important?

- Many organizations lack the required skill set or dedicated teams to perform full-time threat hunting and analysis of threats impacting their organization.

Trend Micro Approach

- Trend Micro offers Managed XDR (managed cross-layer detection and response) for endpoints (Apex One), servers and cloud workloads (Trend Micro™ Deep Security™), networks (Trend Micro™ Deep Discovery™) and email (Trend Micro™ Cloud App Security), separately or together, correlating multiple vectors to provide enhanced detection of advanced threats.
- Collects user, network, and server telemetry, as well as alerts, correlating information through advanced AI techniques to determine if customers have been compromised.
- Offers regular IOC sweeping and IOA hunting to find attacks, building out a full root cause analysis while working with the customer to deliver a robust response to the incident.
- Access to Trend Micro experts who will determine the full root cause analysis and develop a response plan with the enterprise.

Unknown File Guidance

Provides users with a guided view to alerts, prioritizing threats that require immediate action.

Why is This Important?

- When threat investigators come across suspicious unknown objects, they need to know if those objects have been securely signed, are present elsewhere, or have attributes that may be risky.

Trend Micro Approach

- Endpoint Sensor separates threats that require immediate action against less dangerous threats that can be handled at a later date.
- Trend Micro layers in its extensive threat research and provides access to Threat Connect, a service that correlates discovered objects with data from our Smart Protection Network.
- Endpoint Sensor also provides information on unknown events, to provide users with a better understanding of the threat.

Alerts, Timelines, and Threat Information Visibility

Provides users with centralized visibility across their entire environment.

Why is This Important?

- Endpoint security solutions need a centralized and detailed view of the organization's security posture showing information not just on threats and alerts but the overall security posture of the organization.

Trend Micro Approach

- Apex One provides users with centralized visibility across their entire environment through Trend Micro Apex Central™ to see endpoint and EDR alerts, timelines, threat information and more. This extends to all Trend Micro products, including network security, gateway security, and email security.
- Apex Central also provides a detailed active directory heat map of your organization, telling you which organization groups have been associated with threats and alerts and which groups are out of compliance with security policies.

What to Look For

- 24/7 event monitoring and alerting.
- Advanced correlation of data from multiple sources such as emails, endpoints, servers, and networks.
- Detailed reporting of investigated events, monthly summary reports.
- Ability to provide details recommended mitigation options to resolve and recover infected endpoints.

What to Look For

- Prioritized list of threats.
- Guidance on all file types to advise which are suspicious and which are benign.

What to Look For

- Centralized visibility across all endpoints and EDR sensors.
- Detailed mapping of threats and endpoints to organizational groups.

MANAGEMENT

Management of complex endpoint solutions plays a key role in the purchasing decision—having a state-of-the-art security platform is impractical if IT and security operations teams can't manage the platform day-to-day.

Having one integrated platform to provide advanced threat detection and response, comprehensive visibility, control, and investigation can help streamline IT and security team resources and cut back on operational costs.

Role-Based Access Control for Administrative Features

Provides a reporting console to tailor reports and alerts to different functional groups.

Why is This Important?

- It's often important for key pieces of information and data to be presented to stakeholders in an organizations.

Trend Micro Approach

- Offers customizable dashboards to fit different administration responsibilities, so various groups can assess the information vital to their job role.
- Apex One offers full Active Directory Integration with role-based access control, allowing administrators to view security settings and compliance across groups of users.
- Trend Micro offers several pre-configured roles with differing levels of access and views. Or customers can choose to create their own roles.

What to Look For

- Active Directory Integration.
- Customizable dashboards.
- Fine-grained role-based access control.
- Customizable roles.

API Capabilities

Connects third-party management and automation platforms to endpoint security solutions.

Why is This Important?

- Endpoints solutions rarely function in complete isolation.
- It's critical for these solutions to have built-in APIs that can connect to external systems, allowing for automation across the enterprise network.

Trend Micro Approach

- Apex One has expanded API sets, enabling third-party programs to communicate and automate actions.
- Share threat intelligence through APIs provided by third-party vendors.

What to Look For

- Open RESTful APIs.
- Extensive third-party API sets.
- Threat information sharing across multiple programs.

SIEM Integration

Sends security events to various controls.

Why is This Important?

- A SIEM is the central location where users can view all security events from various security controls across the organization.
- SEIMs integrate multiple security solutions in one to provide a comprehensive view across the organization.

Trend Micro Approach

- Apex One provides the ability to send security events to a SIEM via syslog or other integrations.

What to Look For

- SIEM integration via syslog.

Open IOC Integration

Allows for easy identification and characterization of attack indicators.

Why is This Important?

- Despite the differences in products from vendor to vendor, the ability to communicate via an extensible XML schema provides an organization with invaluable cross-product coverage.

Trend Micro Approach

- Utilizes OpenIOC communication to enable far more integration with other security products.
- Sharing threat intelligence to improve the entire security posture of an organization significantly.



What to Look For

- Integration to third-party security systems.
- Threat information sharing.

Language Support

Provides multi-language care for end users.

Why is This Important?

- Organizations today are global, and security solutions need support for multiple languages.

Trend Micro Approach

- Trend Micro products are available in over a dozen languages across the globe to support any customer with multinational locations.



What to Look For

- Multi-Language support.

Threat Information Sharing and Distribution

Communicates threat information to other security layers.

Why is This Important?

- Having endpoints share threat information ensures comprehensive protection across the entire organization.

Trend Micro Approach

- Instantly shares suspicious network activity and files with other security layers to stop subsequent attacks in other areas of the network.
- Support for STIX and TAXII industry standards for enhanced threat prevention.
- YARA integration for advanced malware searches.
- Trend Micro™ Connected Threat Defense™ provides improved visibility, automated identification of new threats, and rapid response across multiple security layers.



What to Look For

- Automatic sharing of threat information and suspicious files across security layers.
- Support for STIX, TAXII and YARA.

Support for PC and Mac Endpoints

Endpoint care for both operating systems.

Why is This Important?

- Organizations today have a mix of both Windows and Mac endpoints, each with differing security requirements.

Trend Micro Approach

- Apex One provides Mac support for a number of effective detection techniques, including device control, machine learning, encryption, threat investigation, and more.

Compliance

Ensures employees and users adhere to corporate IT policies related to securing endpoints.

Why is This Important?

- Organizations are faced with a growing number of regulations and mandates they must follow, especially when it comes to storing and maintaining sensitive customer and financial and health data.

Trend Micro Approach

- Apex One supports regulatory frameworks like PCI, HIPAA, and GDPR with ready-to-deploy policy templates and guides for regional compliance.
- Easily modifiable templates to meet unique requirements of specific organizations.
- IT rules to provide administrators a view into which endpoints are compliant or out of date.
- Views compliance by department by mapping compliance against the active directory.

What to Look For

- Support for Mac endpoints and operating systems.

What to Look For

- Ready-to-deploy policy templates based on industry regulations.
- Flexible policy templates.
- Compliance view by organization

ARCHITECTURE

How an endpoint solution is architected and developed plays a large role in its ongoing effectiveness, scalability, and usefulness over time.

As organizations grow and evolve, it's important for endpoint security to adapt, while constantly providing the best possible protection without impacting performance, usability or day-to-day management.

Single Interface for Accessing Endpoint Protection Platform (EPP) Functions

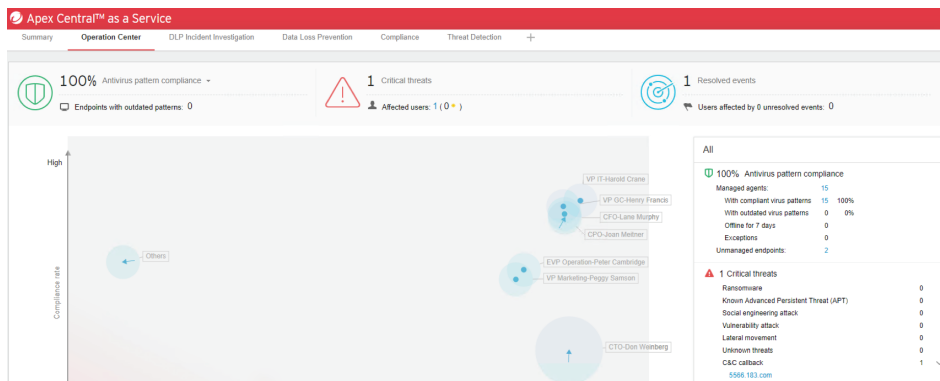
Provides a common pane of glass to visualize both EPP and EDR functionality and alerts.

Why is This Important?

- Less time is spent searching for information across multiple consoles, increasing efficiency and providing a holistic view of the overall security posture.

Trend Micro Approach

- Apex Central provides a detailed view of alerts, policy information, and timelines across all endpoints in your environment.
- Provides a per-user view, allowing administrators to see the user's security posture across email, web, encryption, data protection, and more.
- Administrators can manage and configure their EPP policies and rules without having to use the management console.



What to Look For

- Centralized console for accessing and managing endpoint and EDR functions.

Scalability

Allows security platform to adapt and grow without adding complexity.

Why is This Important?

- Wholesale changes in security products are often large undertakings, therefore scalability in an endpoint solution is imperative, allowing the solution to evolve over time as the organization grows.

Trend Micro Approach

- Apex One is capable of supporting organizations with any number of users, with SaaS deployments equipped with auto-scaling capabilities to fit the changing nature of organizations.
- On-premises deployments of Apex One benefit from clustering and hot-backup capabilities.
- Consistently delivers timely features and updates to meet and exceed customer requirements.

What to Look For

- Horizontal scaling approach.
- Dedicated research and development resources with continuous feature roadmap development.

Easy Upgrade and Deployment Process

Provides multiple deployment options to meet existing organizational practices.

Why is This Important?

- Users today are more likely to work remotely and to have more than one device (e.g. desktop, laptop, tablet, mobile), so ensuring their systems can easily be upgraded as new versions of security software become available is a key requirement needed for effective endpoint protection.

Trend Micro Approach

- Trend Micro SaaS solution deployment can be managed via self-service link or pre-configured agent download.
- On-premises installations can deploy via pre-packaged agents, self-service links, or credentialed push from the console and can be configured to remove existing AV products before installation.
- Apex One agents have the ability communicate with their management infrastructure regardless of where they are or how they are connected to the internet—whether it's making a policy configuration change, updating agents with the latest threat intelligence, and/or updating the agents to the latest software version.
- Offers flexible agent deployment options where organizations can use their existing processes and/or tools to deploy the Apex One security agent via an MSI package, web browser, etc.

What to Look For

- SaaS and on-premises deployment options.
- Automatic uninstall of old versions or replaced security products.
- Ability to make policy configuration changes and upgrade agents and endpoints remotely.
- Flexible agent deployment options.

Geographic Availability (for SaaS and MDR)

Global coverage for both threat analysis and response.

Why is This Important?

- Global follow-the-sun coverage helps to ensure continuous protection and compliance.

Trend Micro Approach

- Multiple data centers and SOCs located in multiple time zones and continents.
- Rigorous security policies and documented data collection procedures to ensure highest standards of data protection and security.

What to Look For

- Ability to store customer data in accordance with regional regulatory rules.
- 24/7 follow-the-sun coverage.
- SaaS ISO 27001:2013 certification.
- GDPR compliance.



Efficient Agent Architecture

Comprehensive feeds tailored towards active real-world threats.

Why is This Important?

- Resource heavy solutions and multiple agents running on an endpoint present increased risk of unfavorable performance and software interactions.
- If poorly designed security prevents a user from accomplishing their core business tasks, the user may attempt to circumvent these measures.

Trend Micro Approach

- Utilizes threat intelligence as a first step in detection and prevention.
- Checks encountered files and processes against a known bad/good list first to block threats with a virtually real-time list lookup.
- Utilizes global cloud network to maintain an advanced machine learning model that supports both pre and post execution and full behavior monitoring.

Security as a Service (SaaS) and On-Premises Deployment Options

Provides flexibility of how to deploy security, with complete product parity between the two.

Why is This Important?

- Many organizations prefer on-premises endpoint deployments, others want to adopt a more cloud-friendly software-as-a-service approach, while some want to take a hybrid approach, it's important your security solution can adjust to fit your organizations unique deployment mix.

Trend Micro Approach

- Apex One provides customers with ultimate control over their deployment scenarios, both on-premises and SaaS options are available.
- Allows customers grow and change their on-premises/SaaS deployment mix over time as their organization evolves and their needs change.



Global Support

Provides support to customers anywhere, anytime.

Why is This Important?

- Attacks can happen at any time, anywhere in the world.
- It is important for your security solution to provide global support and coverage across different time zones.

Trend Micro Approach

- Provides 24/7 support as a standard with all solutions.
- Support centers located globally around the world to provide support when customers need it.
- Provides local language support in most regions.

What to Look For

- Up-to-date global threat information that is incorporated into endpoint security.
- A blend of threat detection approaches that filters out all known bad files before using more resource intensive capabilities.

What to Look For

- Both on-premises and SaaS deployment options.
- Full product parity between SaaS and on-premises.
- Flexible licensing between deployment options.
- Option to change deployment mix in future.

What to Look For

- 24/7 support.
- Global support centers with around-the-sun coverage.
- Local language support.



Securing Your Connected World

©2019 by Trend Micro Incorporated. All rights reserved. Trend Micro, and the Trend Micro t-ball logo, Apex One(TM), and Trend Micro Control Manager are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice. [BG02_Endpoint_Security_Buyers_Guide_190828US]