



issue 1

The Broad Benefits of Connected Threat Defense

Greatly Enhancing Your IT Security with an Integrated Solution

2	The Broad Benefits of Connected Threat Defense
6	Research from Gartner: A Buyer's Guide to Endpoint Protection Platforms
17	About Trend Micro

The Broad Benefits of Connected Threat Defense

Enhancing Your IT Security with an Integrated Solution

As a savvy IT director, you know it's more challenging than ever to protect your enterprise against today's evolving, sophisticated threats. And you are probably now looking at your security with a critical eye and the knowledge that traditional, signature-based antivirus by itself is a weak defense against the latest threats and targeted attacks.

While many security vendors claim to have "the silver bullet" to solve all your security problems, the reality is that no single layer of security will protect against all the threats you face. You need a multi-layered security strategy, as outlined in Gartner Research's "[A Buyer's Guide to Endpoint Protection Platforms](#)". However, there's more to it than just having multiple layers of security. You need those layers to work together to provide an entire lifecycle of connected threat defense.

Connected Threat Defense

To adequately protect against the current threat landscape, you'll need a multi-layered endpoint protection platform that delivers a full lifecycle of a threat defense. As the diagram below shows, this lifecycle of threat defense consists of four stages: **Prevent, Detect, Analyze, and Respond**. Each of these stages uses a series of techniques to keep you protected.

Historically, most enterprises have focused on only the Prevent quadrant, and today there are many niche vendors delivering solutions that target only the Detect, Analyze, or Respond quadrants. But the reality is, in today's dynamic and sophisticated threat environment, no one quadrant of the lifecycle provides enough protection, especially in isolation. There are strengths and weaknesses to the many techniques available to you, and only by having multiple layers of interconnected security across the entire lifecycle can you achieve the strongest defense.

Trend Micro Inc.

225 E. John Carpenter Freeway,
Suite 1500
Irving, TX 75062
888.762.8736
<http://www.trendmicro.com/switch>

The Broad Benefits of Connected Threat Defense is published by "Client Name". Editorial supplied by "Client Name" is independent of Gartner analysis. All Gartner research is © 2011 by Gartner, Inc. All rights reserved. All Gartner materials are used with Gartner's permission. The use or publication of Gartner research does not indicate Gartner's endorsement of Client Name's products and/or strategies. Reproduction or distribution of this publication in any form without prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Gartner shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The opinions expressed herein are subject to change without notice. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "Guiding Principles on Independence and Objectivity" on its website, http://www.gartner.com/technology/about/ombudsman/omb_guide2.jsp.



figure 1. Connected Threat Defense Lifecycle

Connected Threat Defense



Source: Trend Micro

For the best possible security posture, you need connections between the quadrants of the lifecycle. This connected threat defense ensures that threat intelligence gained by techniques in one quadrant is automatically and rapidly shared with the other quadrants.

A connected threat defense delivered through a fully integrated solution also facilitates central visibility and control, giving you a connected threat defense with a complete view of your users and network security. Plus, it makes it simpler for you to investigate threats and to administer day-to-day management.

Below, we outline the strengths and weaknesses of the techniques found in each quadrant of a connected threat defense. Later, we'll introduce you to Trend Micro™ Smart Protection Suites, which provide you with a complete lifecycle of connected threat defense for all of your endpoints, regardless of device or location.

The Prevent Quadrant

The Prevent quadrant assesses vulnerabilities to potential threats and proactively protects endpoints, servers, and applications. There is no single technique that will prevent all threats, and multiple techniques, each with their own strengths and weaknesses, are needed to ensure the broadest range of threat prevention.

The Prevent quadrant includes:

Technique	Strengths	Weaknesses
Traditional, Signature-based Detection (antivirus; web and email reputation)	High-performance rejection of known malware: documents, applications, websites and email senders	Cannot block new, not previously known malware, which makes up the majority of today's attacks
Behavior Monitoring (memory inspection, browser exploit protection, social engineering attack protection)	Doesn't need to recognize specific malware, instead monitors application behavior to look for recognizable signs of suspicious activity	Can be CPU intensive and provides no definitive list of what will be caught or missed
Vulnerability Shielding	Protects against exploits of operating system and application vulnerabilities even before patches are available or deployed	Can't protect until a vulnerability is known
Application Whitelisting	Allows only known-good applications to be run and can be used for system lockdown	Can only stop executables, not malicious PDF's or other files that don't launch a process
Encryption and Data Loss Prevention (DLP)	Protects sensitive data from falling into the wrong hands and provides visibility and control of data to meet compliance requirements	Some dependencies on hardware for encryption, DLP requires application and channel specific integration
Isolation	Isolates an application in a container of sorts so malware can't easily access data or other applications	Not a highly recommended technique as it negatively impacts the user experience because it is resource intensive and makes inter-application data sharing difficult

Source: Trend Micro

The Detect Quadrant

Despite the strength of its techniques, the Prevent quadrant will not block 100% of malware or attacks. That's why you need the Detect quadrant to employ techniques that will help you to detect advanced malware, malicious behavior, and communications that are invisible to standard defenses. This quadrant is particularly strong at detecting zero-day attacks, command and control communications, and advanced persistent threats.

The Detect quadrant includes:

Malware Sandboxing. When one of the techniques from the Prevention quadrant finds something that is suspicious, the item in question is automatically deposited into a virtual sandbox. You can optimize detection if the sandbox precisely matches your own system configurations, so when the suspicious content is safely detonated, you'll be able to determine its potential impact and if it is in fact malicious.

Network Analysis. 360-degree monitoring of network traffic scans multiple protocols across the network to detect suspicious activity, command and control communications and lateral movement of inbound, outbound, and internal network communications.

The Analyze Quadrant

After threats have been prevented or detected, the analysis phase of the threat protection lifecycle occurs. Assessments of the risks and the full nature of attacks are made, along with a retrospective look to determine the impact of these threats.

The Analyze quadrant includes:

Endpoint Forensic Investigation. Endpoint sensors record and report detailed system-level activities on endpoints to assist in the discovery and remediation of attacks. This allows you to find and contain endpoints that have been affected by an infiltration and discover the full context, timeline, and extent of the attack.



Global Threat Intelligence Correlation. With the rapidly evolving threat landscape, massive amounts of threat-specific data are collected by enterprises and security vendors alike. The increasing volume, variety, and velocity of threats demand big data analytics in the cloud in order to effectively identify, correlate, and analyze new threats. This high-level data science produces actionable threat intelligence that must be automatically shared in a timely manner with all of the threat defense lifecycle quadrants.

The Respond Quadrant

Once you have prevented, detected, and analyzed a threat, you need to be able to respond. The Respond phase delivers real-time signatures and security updates to the other quadrants to prevent future attacks, to recover from past attacks, to provide remediation, and to deliver new signatures.

This quadrant relies on rapid response based on the findings in the Analyze quadrant. If a threat is discovered through sandboxing, or a file is found to be malicious, or command-and-control (C&C) traffic is detected, then your security needs to create a real-time signature for that file or C&C server and immediately share it with all endpoints and gateway security components. After this, the threat will automatically be blocked the next time it is encountered.

The Response quadrant includes:

Rapid Response. If an attack is detected in this quadrant, signatures for the attack objects, malicious files, IP addresses, and C&C sites are shared with the Prevention quadrant. The next time these objects are encountered they can automatically be blocked, delivering on the benefit of connected threat defense.

Damage Clean-up Service. To maximize productivity, you need the ability to automatically clean computers of file-based and network viruses, as well as virus and worm remnants.

In Summary: The Integration of the Entire Threat Defense Lifecycle

It is important to have techniques that cover the entire threat lifecycle. However, it is also a key requirement to have those techniques integrated into a single solution where all components work together with central management and reporting.

Integration allows the various security layers to share intelligence and gives you a consolidated view of what is happening. Central visibility across all security layers gives you a comprehensive view of the security of your users and network, and simplifies threat investigation and day-to-day management tasks.

User-centric visibility allows you to understand how threats are spreading for particular users across multiple threat vectors, devices, and applications. A visual dashboard provides a real-time display of key performance metrics and prioritization indicators for simpler, more effective security management.

Trend Micro Solutions

Trend Micro™ Smart Protection Suites along with Trend Micro™ Custom Defense deliver connected threat defense with a multi-layer security solution that covers the entire threat defense lifecycle.

Trend Micro will fortify your defenses to the highest levels with the broadest range of threat prevention, detection, analysis, and response capabilities. Our solutions include a spectrum of advanced threat detection techniques such as application whitelisting; behavior monitoring; vulnerability shielding; threat sandboxing; and endpoint sensors for threat investigation.

Our Smart Protection Suites provide strong security with user-centric visibility and central management across all layers for simpler threat investigation and day-to-day management. In addition, we make it easy for you to evolve your security by giving you a single user-based license that delivers multiple layers of protection for all of your users' devices. This streamlines installation and lets you easily deploy and fine tune your protection in the way that best fits your business: onsite, in the cloud, or as a hybrid solution.

Now, if things change and you need to move something to the cloud or back onsite, it's not a problem. We give you the flexibility to change the mix of on-premises and cloud components at any time, without requiring you to buy new licenses.

To learn more about the Smart Protection Suites, visit www.trendmicro.com/switch.

Continue on to read Gartner's "[A Buyer's Guide to Endpoint Protection Platforms](#)".



Gartner Research, G00274074, Peter Firstbrook
Neil MacDonald, 29 January 2015

A Buyer's Guide to Endpoint Protection Platforms

Endpoint protection platforms offer a diverse array of features. This guide lists the most advanced features to help buyers differentiate solutions.

Key Findings

- A wide array of endpoint protection platform (EPP) solutions are available with significant differentiation among vendors. No single vendor leads in all functional areas, so buyers need to prioritize their requirements to address the needs of their specific business, technical and regulatory environments.

Recommendations

- Give primary consideration to the malware effectiveness of a solution and the breadth and depth of non-signature-based techniques used, especially application control, malware sandboxing, vulnerability detection and full software attestation.
- Look for vendors that are investing in endpoint detection and remediation tools that have high value in detecting stealthy attacks and recovering from incidents.
- Seek out vendors that are expanding management capability and protection to alternative platforms such as Mac, Linux, virtual desktops/servers, tablets and mobile devices.
- Consider the needs of data protection when considering endpoint protection. Encryption and data loss prevention (DLP) are core functions for data protection and often provided by endpoint protection vendors. The ability to simplify client-side agents with a common management framework is an advantage, but broader enterprise DLP and encryption requirements could outweigh these advantages.
- Resist vendor packaging that includes gateway protection with endpoint protection unless there is a clear link between these products that improves overall security effectiveness. Focus on client and server as one domain and gateways as a separate domain. Resource-constrained small and midsize businesses (SMBs) may want to consider the advantages of centralized management of both domains, but must put a higher priority on the unique requirements of each domain.

Analysis

The most fundamental component of EPP suites is a collection of technical features to prevent malware infection. These tools typically include antivirus, anti-spyware, rootkit detection, host-based intrusion prevention, memory protection, behavior monitoring, port/device protection and a personal firewall. Advanced EPP suites may also include application control, and malware sandboxing capability to restrict applications to known or tested applications. The demanding management needs of large enterprises and the desire to proactively reduce the attack surface are also forcing EPP suites to replicate some PC operations infrastructure, such as security configuration management, patching and vulnerability management. Advanced solutions are starting to add capabilities to perform more ad hoc investigations. EPP vendors also offer data protection technologies, such as DLP and encryption.

As the form factor of endpoints expands beyond the traditional Wintel machines to virtual servers and desktops, tablets, Mac and mobile devices, the need to provide appropriate security utilities for these diverse operating systems is expanding.

By combining multiple technologies into a single management framework, EPPs have the promise of increasing security, while lowering complexity, cost and administrative overhead. More Integrated systems will also enable the conveyance of context from between different elements in the suite providing better security.

Organizations should initially evaluate their needs across five critical capabilities:

- 1 Malware effectiveness – Does the solution have full security life cycle capabilities from hardening and isolation techniques to detecting and recovering from malware incidents?
- 2 Manageability – How adequate is the management capability for the organization? Smaller organizations may be looking for simple set-and-forget functionality with limited options, while larger organizations may be looking for more complete capability that will be more agile.

- 3 Solution completeness – Does the candidate solution have the appropriate components and endpoint and server platform coverage to satisfy current and future needs?
- 4 Support and service – What is the ability of the vendor to provide the adequate level of support?
- 5 Strategic vendor status – What is the vendor's ability to service other security needs to reduce vendor management and provide future opportunities for integration and cost savings?

The major functionality components of EPP suites are listed below, with a review of the advanced capabilities of each. Organizations should use these features to build RFPs and/or scorecards to differentiate products under evaluation. No product will have all these features, so buyers must focus on features they deem valuable for their enterprise. This list is not intended to be comprehensive. It is intended to be representative of advanced functions which, when investigated, will help identify more-sophisticated solutions.

Malware Detection

As the anchor solution in EPP suites, the quality of the malware scan engine should be a major consideration in any RFP. The ability of most organizations to accurately test malware engines in real-world situations is limited at best. Moreover, none of the signature-based malware engines are ever 100% effective at detecting known threats, and accuracy at detecting new threats is only 30%. Low distribution/targeted threats are even more elusive to signature techniques:

- Test results from organizations such as AV-Comparatives.org, and AV-Test Institute are useful guides on malware detection accuracy, false positives rates and scanning speeds. In the absence of other information, good test scores are better than poor results, but buyers should beware that sample malware used in tests may not accurately reflect malware encountered in the real world, and do not test all proactive techniques for blocking malware. Such application control, vulnerability detection and configuration management and solutions are tested with out-of-the-box configurations.
- Traditional antivirus systems only classify “known bad.” An emerging technique we call “full software attestation” provides a classification of the entire process inventory. That is, it classifies all running processes as “good” or “bad” and provides metadata about the applications such as author, function, malware traits and prevalence. This is

a valuable service because it removes the lingering doubt that an unknown malicious file is lurking on the system, by inspecting and reporting on all executable files.

- Real-time, cloud-based look-up mechanisms should provide extensive two-way communications that share computing objects, such as files and URLs, and include metadata about these objects to improve the ability to detect and respond to new events. Vendors that offer real-time cloud-based interactions are better positioned to spot new trends and respond quicker than vendors that rely on traditional one-way database synchronization schemes.
- The capability to detect rootkits and other low-level malware once they are resident is a significant consideration. Some solutions are limited to catching only known rootkits as they install, while others have the ability to inspect raw PC resources seeking discrepancies that will indicate the presence of rootkits.
- As more malware shifts to Web distribution methods, EPP solutions should include client-based URL filtering to block clients from visiting websites that are security risks.

Advanced Malware Protection

As previously mentioned, antivirus/anti-spyware databases are 90% to 99% effective at detecting well-known, widely circulating threats. However, they are only 20% to 50% effective at detecting new or low-volume threats. Security effectiveness is significantly enhanced by non-signature-based techniques, collectively categorized as host-based intrusion prevention systems (HIPSs), but there is no generally accepted method of testing the HIPS effectiveness of different solutions:

- HIPS techniques have no standard terminology. Consequently, it is essential for buyers to ask vendors to list and describe HIPS techniques so they can normalize the list of techniques and compare the breadth and depth of HIPS techniques across vendors. Buyers should also understand which techniques are included in the base client and those that are optional, and what, if any, additional charges are required for additional HIPS techniques. Vendors are adept at spinning minor HIPS techniques into invincible solutions. Buyers must pressure vendors to provide statistical information to illustrate the frequency at which these techniques detect unknown malware.

- Memory protection to prevent malicious code injection to common process is a critical HIPS technique. Buyers must press vendors to explain which types of memory injection attack are blocked and what application are protected from such attacks.
- Malware engines should also continuously monitor file objects and system resources for changes that might indicate the presence of suspicious code. Increasingly, malware solutions will store this history to perform retrospective malware encounter analysis and for malware investigations and remediation. There is an emerging endpoint detection and remediation market delivered by specialized providers. However, this technology is being adopted by leading EPP vendors.
- Journaling changes (that is backing up files) that are generated from a low reputation or unknown process is a critical capability for recovering from damaging malware such as cryptolocking malware.
- One very effective HIPS technique is “vulnerability shielding” (also known as “virtual patching”) – that is, the ability to inspect and drop attacks based on knowledge of specific vulnerabilities they are exploiting. This technique allows protection against attacks against known vulnerabilities before the vendor releases a patch, and to buy time for patches to propagate out to all endpoints. Of particular value is a list of the actual common vulnerabilities and exposure IDs that are shielded, such that administrators know when a patch can be safely delayed.
- The simulation of unknown code before the code is executed to determine malicious intent without requiring end-user interaction with the unknown code (e.g., using static analysis, simulation or reverse compilation techniques) is another deterministic technique, but can be very resource-intensive and should be selectively used for suspicious or unknown code (see Malware Sandbox section for off-endpoint techniques).
- Behavior-based protection is a useful tool, but can be prone to false positive unless known applications are excluded. The integration of an application control (see Application Control section) database of known good applications with HIPS can help automatically tune HIPS features to avoid false positives and to reserve more intense inspection to unknown code.

- A core principle is that the HIPS solution must enable the administrator to choose and tune the styles of protection he or she needs based on the requirements and resources of the endpoint, and configure protection to reflect the organization's overall tolerance for risk and administrative overhead.
- Notwithstanding the previous point, the best solutions will provide preconfigured out-of-the-box templates for common application and system configurations, as well as a learning mode for enterprise environments and the ability to test policy in a log-only mode.
- Some vendors only offer binary control over HIPSs, allowing administrators to turn them on or off only. Although we do not expect IT organizations to agonize over each setting, it is important to have granular control that enables them to turn off certain rules for specific applications to accommodate false positives.

Malware Removal

Modern malware is significantly more complex than that of previous generations, often involving multiple components with sophisticated keep-alive routines. Malware removal services and support assistance can be beneficial. However, the wisest course is often to simply reimage machines. Increasingly, the use of event recording will enable better event investigation and improved malware removal.

Cryptolocker and other ransom or destructive malware (for example BKDR_WIPALL used in the Sony hack) represent a unique new form of malware that is not recoverable from. Some solutions offer journaling and file backup capabilities to prevent malware from performing unrecoverable changes.

Application Control

Application control describes the ability to restrict application execution to a list of known and trusted applications. The “trusted application” list can be as restrictive as the applications already installed (aka lockdown) or as loose as the known universe of cataloged trusted applications or anything in between. Application control shifts the paradigm from “default allow” (allow any applications as long as it is not a known malware) to “default deny” (do not allow any application unless its providence and reputation are known) thereby automatically blocking new or targeted malware. Even in “monitor only” mode, application control provides excellent early detection of potential malware. For more information on application control.



Application control features to investigate include:

- The size and quality of the catalog of known “good” applications.
- How applications are identified and how they are prevented from executing (e.g., whether they block the installation of applications or just the execution).
- The ability to automatically allow sources of trusted applications (i.e., certificates, locations, processes or administrators), so that even applications not yet cataloged by the vendor can be allowed if they come from a trusted source.
- Application control should extend to the execution of browser helper objects/controls within the context of Internet Explorer or other browsers and Java applets and other scriptable objects.
- Application control should be integrated with malware signature and HIPS engines such that the verdict of each system can be relayed to others. For example, applications that are known good or trusted should not be blocked by HIPS, while applications that are not known may execute but with elevated HIPS protection.
- Unknown applications should be able to be automatically submitted to a cloud or local malware sandboxes for malware analysis.
- The workflow for users requesting the use of an unknown application should be integrated into the help desk ticketing system and provide sufficient context for the help desk to make an educated decision.
- Support for Windows endpoints at a minimum including XP and 2002 as well as optional support for Macintosh and Linux.
- Centralized deployment or cloud-based deployment is preferable to deployments that must be in tap mode on specific network segments
- Ability to store multiple customizable virtual images to match enterprise gold image and the ability to maintain images in synch with enterprise patch activities
- Ability to inspect multiple executable file types including documents and interpreted code such as Java
- Automated and manual methods to submit code to the malware sandbox, that is the ability for endpoints or network agents to automatically submit unknown code to the sandbox, and administrators to manually submit code
- Evasion detection techniques are important to detect malicious code that does not exhibit malicious behaviors if it suspects it is running in a sandbox
- Integration with object reputation databases (that is a “good” application and malware databases) help conserve resource by eliminating known good or known malicious programs from the behavior analysis system
- Comprehensive reporting that describes the actions and metadata of sample and why it reached the verdict
- Queue management functions that enable administrators to set wait times before allowing local endpoint execution and user display functions that help users understand what is happening while they wait for local execution

Malware Sandbox

A malware sandbox is a centralized resource that can execute suspect code in a virtual environment and make an automatic determination of whether it is malicious. Sandboxes are an early stage optional component of an EPP, but are rapidly gaining mainstream adoption. Features to look for in a malware sandbox include:

Vulnerability Management

We know that unpatched vulnerabilities are the most common attack technique. Detecting and patching known vulnerabilities is the most effective method of blocking known malware. Larger organizations often use dedicated vulnerability assessment tools.

However, EPP features that provide insight into known vulnerable applications, particularly those that are frequently exploited by malware, is a useful tool to understand the security state of the endpoints and overseeing operations teams that may have a different agenda than security. Organizations that do not have a dedicated vulnerability assessment tool will find EPP solutions to be adequate for the purpose of deflecting endpoint malware. Vulnerability assessment features should:



- Address, at a minimum, the most commonly exploited applications and not just Microsoft patches
- Provide insight into the number and the severity of vulnerabilities as well as provide a prioritized list of software to patch to provide the maximum impact on security
- Be combined with patch capability to remediate endpoints or at a minimum a link to the appropriate patch
- Cross-reference unpatched vulnerabilities with shields (for those that include vulnerability shields) so administrators know which vulnerabilities are actually shielded

Manageability and Scalability

Reduced administration overhead is one of the top concerns of EPP administrators. An effective task-oriented graphical user interface (GUI) and comprehensive management interface will offer lower total cost of ownership. Gartner recommends creating a list of the top 10 to 20 most common or critical tasks (see Note 1), and using this list as a guideline for comparison testing and demonstration of solutions. Required management capabilities will depend heavily on the enterprise's specific needs and available technical skill sets. Advanced capabilities will include:

- Level of integration between components, which is of critical consideration when selecting suites: Integration at a reporting layer is easy to achieve, integration of policy is harder but most important is the ability to share context between components. Look for concrete examples of components enhancing the security state by operating together rather than independently. For example, the integration of an application control database with HIPS behavior monitoring enables more restrictive behavior-based policies for unknown applications.
- Varied degrees of management and reporting integration into a common centralized management console: Consider the look and feel of management pages and the ability to transition from dashboards to the configuration or remediation of indicated problems.
- A home page dashboard of real-time events and trending information that enables rapid troubleshooting of event or server issues: Ideally, dashboard elements should be actionable so that clicking on an event or graph will initiate steps to better understanding the issues. More-advanced

management interfaces allow for easily clicking through from the dashboard to more detail and problem resolution options (see below for more dashboard features).

- Range of client information, which can be collected and reported to the management server and is a growing differentiator: Most EPP suites will collect information only about the status of the EPP suite. However, as endpoint hygiene becomes more critical, the status of patch levels, configuration information software inventory and vulnerability information is becoming more important. Event information storage that enables better investigation and remediation capabilities will be a critical differentiator as EPP vendors integrate endpoint detection and remediation capabilities.
- Reporting that enables multiple devices to be linked to a particular user: This is a good indication of the degree of integration of mobile device management (MDM)/enterprise mobility management (EMM) functionality.
- Multiple directory integration options (i.e., Microsoft active directory [AD], Lightweight Directory Access Protocol [LDAP]) and the ability to integrate with multiple directories and traverse directories to find users groups and authentication information.
- Methods to combine directory, device and event information to create dynamic groups are very useful for creating flexible policy: Dynamic tags allow for alert prioritization and automatic policy implementation when event thresholds are exceeded.
- A “wizard”-type installation mechanism that provides optimal default settings for different-sized environments and different types of endpoints as well as those that automatically add licensed entitlements is very useful for reducing the implementation overhead.
- Ability to automatically and natively distribute the full client agent and remove competing products is a differentiator: Some solutions simply provide an .msi file for manual distribution by other software distribution tools.
- Task-based (not feature-based) management GUI that simplifies management by hiding complexity, but also gives more technically skilled users the ability to drill down into granular detail for more-technical users (see Note 2).

- Solutions that provide native management server redundancy: For example, load-balancing, active/active clustering within and across LANs, or automatic active/standby failover – without a single point of failure.
- Centralized management with automatic configuration and policy synchronization among management servers in large deployments.
- Threshold alerting capabilities – including email, SMS and Simple Network Management Protocol (SNMP) – and threshold alerts for dashboard statistics and policy thresholds alerts: Ideally threshold alerts should be proportional as well as deterministic, that is alert when a parameter exceeds normal by X percentage rather than when it reaches a numeric value of X.
- Granular, role-based administration, ideally with both predefined roles and the capability to customize and add and remove options: It should be possible to limit data visibility to only groups that the role is managing.
- Ability to create different management GUI workspace views (for example, administrator or help desk view), with the ability for users to adjust their default views a plus.
- A task/context-based help function, with recommendation settings for Web configuration options.
- Configuration backup and configuration preservation between version upgrades.
- Policy (see Note 3) in a single view with intelligent drop-down pick lists and fields that change based on previous optional selections: Avoid solutions that have multiple popup windows or require visiting several tabs to create a single policy.
- Policy creation that is object-oriented so that policy elements can be created once and used in multiple policy instances (see Note 4): For example, the definition of off-LAN can be created once and reused in multiple policies such as firewall/Wi-Fi policy and update server location. Policies should also be able to inherit the attributes of higher-level policy without recreating the higher-level policy, as well as the ability to break this inheritance when necessary. This makes exceptions easier to create and manage.
- Solutions that offer a human-readable printable policy summary for audit and troubleshooting purposes.
- EPP solutions with a complete audit log of policy changes, especially those with extensive role-based administration and delegated end-user administration.
- A customizable toolbox element that allows the consolidation of common tasks into a single user-defined menu.
- Globalization: In addition to global support and centralized management and reporting, look for local language support for the management interface and end-user interface.
- Management server that can collect client status information in real time, rather than in scheduled delta updates: The ability to collect information from mobile endpoints that are not connected to the network that hosts the management server is a significant differentiator.
- Management system that can automatically detect new/rogue endpoints that do not have an EPP client installed: This function may be integrated into network access control (NAC). However, it should not be dependent on NAC and should be able to detect clients that have already joined the domain.
- Some solutions that offer a software-as-a-service (SaaS)-based managed console to eliminate the need for a dedicated server for managing endpoints: This feature is more useful for SMBs and regional offices. Ensure that vendors are clear on the level of integration between the SaaS management and on-premises management servers. Also, insist on a list of the functional difference between SaaS-based consoles and on-premises-based ones. For example, SaaS consoles cannot typically find rogue machines that do not have the client installed.
- The typical ratio of management servers to clients in practice and the factors that affect this ratio are important considerations for large enterprise and will impact the total cost of ownership (TCO): For smaller organizations, the management server should work on a shared server or a virtualized server.
- Ability to stage and phase the rollout of signatures or policies and to roll back changes quickly is important: Fewer users test signatures before deploying them.

- Number of required clients, the client disk and memory footprint are good indicators of the level of integration between EPP components, as well as the efficiency of the client: Ideal solutions will provide a single consolidated agent that has component parts that can be remotely enabled and disabled.
- Client interface that is adaptable to enable a full range of delegated control for end users: Advanced solutions allow administrators to delegate or restrict any client option.
- Options to limit the client impact of scheduled scans are a significant differentiator: Scheduled scans are one of the most annoying aspects of signature-based anti-malware. Advanced features include the ability to delay scans based on battery life or running process or CPU utilization. More rare is the ability to “wake and scan” PCs in off hours. Scheduled memory scans should be independent of disk scans.
- Administration that is simplified when solutions include protection for a broad range of platforms, including Macintosh, Android and Linux, and specialized servers, such as SharePoint, Exchange and virtual servers from a single management console.

Dashboard and Reporting Capabilities

Real-time dashboard and analytics capabilities are a key differentiator of current EPP solutions and will become increasingly important in the shift to continuous monitoring and long-term data retention. For example:

- Dashboards should provide a real-time prioritized list of actions and alerts that need attention of security and operations administration – what we like to call the “cup of coffee” screen. At its most basic, it should provide a list of suggested actions and graphical views of anomalies worthy of investigation.
- Management dashboards should provide continuous display of key performance metrics, such as dwell time, vulnerabilities outstanding, time to containment, remediated infections, most dangerous users/groups, and threat type distribution as well as summary info of operations dashboard. Comparisons to global local and vertical industry norms would be beneficial.
- Dashboards should offer data feeds with relevant external news, such as global malware activity, Or additional context, such as malware family, relevant URLs and IP addresses, etc.
- vulnerability information or other events, are desirable. External trending information enables administrators to better understand internal activity levels and compare them to global events.
- Dashboards should be administrator-customizable, so that information that is most relevant can move up to the top of the page, and display options (such as pie charts, bar charts and tables) should be configurable so that information can be displayed in the format that specific administrators need.
- Reports and dashboards should include trending information against customizable parameters. For example, create a dashboard view or report that shows percentage compliance against a specific configuration policy over time.
- Dashboard information should always offer one-click detail to enable administrators to quickly drill down into detail, rather than forcing them to switch to the reporting application and manually select the appropriate report and recreate the parameters that include the condition they are interested in investigating.
- Dashboards should also offer quick links to remediation actions (i.e., clean, quarantine, patch or distribute software), as well as quick links to other resources, such as malware wikis, to resolve alerts.
- Solutions should include the ability to import or export data and alerts with security information management systems or other reporting systems.
- Reporting engines should be capable of running on-box for smaller solutions or moving to a centralized reporting server for consolidation and storage of multiple management servers’ log information without changing the look and feel of the reports.
- Dashboards should have the ability to create custom reports – in HTML, XML, CSV and PDF output types – save them and schedule them for distribution via email or FTP, or move them to the network directory. The ability to put multiple reports together in a report package and schedule for distribution is a more advanced feature.
- Databases must enable rapid report queries and the ability to store historical data for long-term storage in a standard format. Bonus points for natural language queries capabilities.



- Latency of the data should be customizable (i.e., faster refresh rate) with minimal network impact. Real-time queries against live data will be increasingly critical.
- Reporting engines should include a facility for creation of completely ad hoc reports similar to SQL queries, rather than just modification of the parameters of predeveloped reports.
- More-advanced solution will include analytics cubes that enable very complex queries that answer specific questions – for example; “show number of users in active directory group ‘finance’ that have an unencrypted laptop that have had more than three infections in the last two years.”

Virtualization Support

Virtualization has become ubiquitous in modern data centers (desktop and server) and nearly every EPP vendor offers some form of support for running their solution in a virtualized environment. However, there are some key differences and before looking at vendor solutions, buyers must understand their organization's approach and use of virtual servers.

The first consideration is whether it is a full virtualization solution, where each system gets its own virtual machine (VM) and its own copy of an OS, or is it the older terminal services model, where a single copy of Windows is used in a multitenant fashion to support multiple simultaneous sessions. The distinction is important because while most vendors support their EPP agents running in a full VM, they may or may not have redesigned their offering to run in a terminal services environment.

Most new virtualization deployments today use a model where server or desktop has its own full copy of an OS. Because the guest is essentially identical to the OS that runs on a physical device, most vendors will state they support running their agent in a VM. However, the reality is that there are substantial differences between different EPP vendor's supports of virtual environments. Simply running unmodified EPP agents in virtual machines can create significant resource contention issues. For example, if all the signature files of an agent are updated at once across hundreds of VMs, or if anti-malware scanning of the file system kicks in all at the same time. The impact on network bandwidth, CPU utilization and storage input/output can be significant. Because of this, a poorly implemented EPP solution can reduce VM density and negatively affect the overall TCO of the virtualization project.

At an absolute minimum, EPP solutions should support:

- Randomized scanning in which the scheduled scanning is “randomized” so that all scans do not kick off at the same time.
- Signature files (commonly referred to as DAT files), which should not all update at the same time; ideally, these can be delivered once and shared either directly or copied in a peer-to-peer fashion among VMs, reducing bandwidth requirements during updates.
- Gold image files, which ideally should be cached so they are not rescanned if unchanged.
- Configuration testing for organizations implementing “thin provisioning” where the VM images are reset back to known good state on each reboot. The configuration should be tested to understand how the signature files will be updated on each machine reboot and subsequent regeneration. This process can create issues if all users login at the same time in the morning and a new session is generated, requiring an update of the DAT file if it is provisioned from an out-of-date source.

More advanced solutions will offer centralized scanning by exploiting the hypervisor-level application programming interfaces (APIs) opened up by VMware to perform “agentless” scanning (the term agentless is somewhat of a misnomer as there is stub code placed into each VM by VMware's tools). Using this approach, the file-based anti-malware scanning can be offloaded to a “security VM” that coordinates the anti-malware scanning on all virtual hosts.

Additional features to look for in agentless scanning include:

- Support for agentless anti-malware scanning using the VMware hypervisor APIs
- Agentless file integrity monitoring and agentless access to network streams for firewalling and IPS exploiting VMware APIs

In a Microsoft Hyper-V environment, Microsoft has not delivered equivalent APIs for agentless malware scanning, but one of Microsoft's partners, 5nine Software, has implemented this using licensed signatures.

Using hypervisor-specific APIs has its pros and cons. On the positive side, resource contention can be greatly reduced. However, on the negative side you are creating lock-in to the vendor's hypervisor platform. Another negative is that your capabilities are limited as to what is exposed by the APIs. For example, behavioral and memory protection as well as application control aren't yet exposed via the VMware APIs, so the EPP solution loses these capabilities unless an additional agent is introduced.

For this reason, some of the EPP vendors have implemented "Hybrid" architectures where a small agent in each VM coordinates with a master "security VM" running separately. This combination can centralize anti-malware scanning, but keep a small local agent for behavioral and memory protection. This hybrid approach has several benefits:

- The small local agent can perform inspection not possible using the hypervisor APIs
- The EPP solution can be architected to be hypervisor-neutral and therefore run in VMware, Hyper-V, KVM and other virtualization environments. Likewise, the EPP solution can be run in public clouds where VMs are used, but where none of the leading infrastructure-as-a-service (IaaS) providers offer hypervisor-level API access due to security concerns.

Even if hypervisor-specific APIs are used locally and agent-based protection is used in public clouds, the agent and management infrastructure should be architected to provide a single pane of glass for managing agents seamlessly across hybrid physical, virtual and cloud-based infrastructure without requiring different consoles for configuring policy and viewing security events.

Finally, licensing models should favor simplicity. In most cases, the EPP provider will charge the same amount for all endpoints, physical or virtual, easing the complexity of licensing for enterprises. Cloud virtual deployments that auto scale should be capable of accounting for utilization bursts without excessive auditing requirements or over capacity buying (see Note 5 for additional checklist for virtualization protection solutions).

Data Encryption and DLP

As organizations become increasingly concerned about data loss, EPP vendors are advancing data protection through endpoint data encryption and DLP capability. Many EPP vendors are selling encryption in the related mobile data protection market and are successful in selling both stand-

alone and suite installations. Some EPP DLP solutions are components of broader enterprise DLP solutions, while others are stand-alone endpoint-only solutions. Endpoint DLP that is integrated into the EPP suite offers the promise of more content-aware port/firewall and encryption policies, simplified agent management and distribution, and lower cost. Stand-alone EPP DLP will likely satisfy many businesses' early needs but may not be suitable for more-ambitious future data protection plans. Buyers should certainly evaluate prospective EPP DLP capabilities and the vendor's longer-term road maps to determine how well it aligns with business needs. Mobile data protection (encryption solutions) does not need to be tightly integrated with EPP solutions. However, there are administrative and cost savings when they are integrated. Moreover integration of port control to selectively enable removable storage with DLP and encryption enable policies based on the content of the files in use – for example, forcing encryption on a file transferred to a USB drive if it contains sensitive information.

Enterprise Mobility Management and Mobile Malware Protection

As more endpoints in organizations take the form of mobile devices and mobile operating systems, EPP vendors are responding with protection and management features for these platforms. Since the mobile OS (primarily Android and iOS) are more secure out of the box, protection typically takes the form of managing the protection features built into mobile OS, which is generally referred to as "mobile device management" and now "enterprise mobility management." EMM functionality is not well-integrated into EPP suites, although several vendors have made investments in solutions with plans to integrate this functionality. Consider the following when looking at EMM functionality:

- Proactive auditing and upward reporting of status of system encryption policies
- Policy support that takes advantage of all management capabilities in a given platform
- Proactive detection and countermeasures for "jailbreaking," rooting and data leakage prevention
- Support for three major mobile platforms (Android, iOS, Windows), realizing that this is not a monolithic challenge

In addition to EMM, EPP suites also offer antivirus protection for these platforms. The traditional approach of only identifying malicious applications is tempting at this early stage of the market; however, an application control approach that catalogs all aspects of both good and bad apps will have more long-term business value. Security risks will extend to applications that leak sensitive or private information, create back doors to corporate resources, have no business value or may increase legal risk. Vendors like Appthority have created the mobile application catalog; however, few EPP vendors have made the investment in creating a mobile application catalog or licensing one yet – but that is the desired direction.

Service and Support

Service and support are essential concerns for secure endpoint protection suites, as they are for any business-critical technology. Capabilities to consider include:

- Dedicated product engineers' resources or direct access to Level 2 support
- Global support presence with local language support engineers in necessary geographies
- Evidence of extended tenure of support staff
- Vendor willingness to agree to high service-level agreements for callback responses
- SLAs for the production of signatures for unique malware discovered in the enterprise network.
- Support resources, including user forums, best-practice guidance and white papers
- Installation assistance and training
- Clear and consistent escalation policies

Note 1

Sample Critical Tasks

Common tasks might include:

- Review home page dashboard, paying particular attention to the placement of indicators that illustrate negative changes in the security posture of endpoints. Look for direct links to more information, recommendations and action steps to resolve events.

- Identify patterns of noncompliance. Some users, workgroups or tasks may cause repeat occurrences of policy violations that can be recognized by historical event analysis.
- Tour the report center, create a custom report and schedule it for delivery to an email box or Web server/portal.
- Show alert configuration capability, and integrate an alert with an external subscriber identity module.
- Show real-time data that lists clients on a network that do not have an EPP agent installed.
- Create or edit the policy elements that can be delegated (or restricted) to end users.
- Create or edit the policy configuration for client update distribution and step-through policy creation.
- Create or edit the policy to automatically push the EPP client to an endpoint that does not have it installed.
- Configure scheduled scans for endpoints. Focus on the ability to limit CPU utilization, and delegate the ability for end users to delay scan execution.
- Create or edit the port (i.e., USB, CDs, infrared) control configuration. Pay particular attention to the granularity of the restrictions and the linkage to file types and encryption, if any.
- Create or edit VPN policy (i.e., deny split tunneling) for a specific active directory group.
- Create or edit location-based policy, and pay attention to the level of automation in selecting when a policy should be invoked.
- Create or edit a Wi-Fi-specific policy.
- Create or edit a whitelisting and/or lockdown configuration for a certain group of PCs. Add a new executable program to the whitelist. Autogenerate a whitelist from the installed applications on a PC. Authorize a software distribution method and directory as a whitelisted source of applications.



- Show a single-page summary of client configuration information, and print it for review.
- Review HIPS policy configuration and step through the false-positive-handling process, including deactivating a specific HIPS rule for a specific application.
- Edit role-based administration and hierarchical administration to add a new role.

Note 2

Evaluating a Task-Based System

A task-based system can be evaluated by creating a list of common tasks and comparing the number of steps required to complete each task.

Note 3

Choosing an Enterprise's Policy Interface

An enterprise's policy interface – like its policies – should be chosen fundamentally to address the needs of the business. Excessively complex and technical policy interfaces and reporting will force IT to interpret and implement business policy, increasing both workload and the potential for errors and miscommunication. A policy interface should be intuitive and usable by nontechnical business personnel – for example, HR and legal staff. A good way to test the usability of an interface is to give such personnel an opportunity to test it.

Note 4

Reusable Policy Objects

Reusable policy objects are critical to the creation of a scalable policy environment. Objects such as dictionaries should be separate referenced databases, files or subroutines, so that they can be reused in multiple policies but updated centrally. Policies that use hard-coded objects require administrators to update multiple policies to make a simple change.

Note 5

Checklist for Virtual System Support

- Which terminal services and virtualized environments are explicitly supported by the vendor?
- Does the support go beyond staggered scanning?
- How are DAT files updated across VMs?
- Is the agent architecture different than the one used for physical endpoints?
- Are hypervisor-specific APIs used and have you considered the pros/cons of this approach, including vendor lock-in?
- Does the EPP offer less functionality when running virtualized? What functionality is lost?
- Does the vendor offer a hypervisor-neutral option?
- Does the vendor offer a hybrid light agent/coordinating security VM option?
- Is the same management console used across physical/virtual?
- What is the EPP vendor's strategy for protecting workloads in public cloud IaaS?
- What public cloud IaaS providers are explicitly supported?
- For highly variable public cloud IaaS models, does the vendor offer usage-based licensing- per month or per hour?

About Trend Micro

Trend Micro, a global leader in security software and solutions, strives to make the world safe for exchanging digital information. For the past 25 years, its employees have been inspired to protect individuals, families, businesses and governments as they look to harness the potential of emerging technologies and new ways of sharing information.

In today's organizations, information has become the most strategic asset; embodying competitive advantage and powering operational excellence. With the explosion of mobile, social and cloud technologies, protecting this information has become more challenging than ever. Organizations need smart protection of information, with technology that is simple to deploy and manage, and security that fits an evolving ecosystem. Trend Micro solutions enable a smart protection strategy for organizations. Smart. Simple. Security that fits.



Trend Micro provides layered content security for mobile devices, endpoints, gateways, servers and the cloud. Leveraging these solutions, organizations can protect their end users, their evolving data center and cloud resources, and their information threatened by sophisticated targeted attacks.

All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe.

For additional information, visit www.trendmicro.com.