Magic Quadrant for Endpoint Protection Platforms

22 December 2014 ID:G00262733

Analyst(s): Peter Firstbrook, John Girard, Neil MacDonald

VIEW SUMMARY

The endpoint protection platform provides a collection of security capabilities to protect PCs, smartphones and tablets. Buyers of endpoint protection should investigate the quality of protection capabilities, the depth and breadth of features, and the ease of administration.

Market Definition/Description

The enterprise endpoint protection platform (EPP) is an integrated solution that emerged in the 2006 time frame composed of previously separate capabilities. These include:

- Anti-malware
- Personal firewalls
- Host-based intrusion prevention
- Port and device control

EPP solutions also will often include:

- Vulnerability assessment
- Application control (see Note 1) and application sandboxing
- Mobile device management (MDM)
- Memory protection
- Behavioral monitoring
- Endpoint detection and remediation technology (see "Market Guide for Endpoint Detection and Response Solutions")
- Full-disk and file encryption, also known as mobile data protection
- Endpoint data loss prevention (DLP)

These products and features are typically centrally managed and ideally integrated by shared policies. Not all products in this analysis provide the same collection of features. Here, we focus primarily on anti-malware effectiveness and performance, management capability, protection for non-Windows platforms (such as VMware, Macintosh, Linux, Microsoft Exchange and Microsoft SharePoint), MDM capability, application control, vulnerability assessment, as well as emerging detection and response capabilities. See the Completeness of Vision section for more information.

DLP, MDM and vulnerability assessment are also evaluated in their own Magic Quadrant or MarketScope analyses (see the Gartner Recommended Reading section). In the longer term, portions of these markets will be subsumed by the EPP market, just as the personal firewall, host intrusion prevention, device control and anti-spyware markets have been subsumed by the EPP market in the past. EPP suites are a logical place for the convergence of these functions. In a recent Gartner survey,[1] 40% of organizations said they already use a single vendor for several of these functions, or are actively consolidating products. In particular, mobile data protection is the leading complement to EPP, and purchasing decisions for the two products are increasingly made together. For most organizations, selecting a mobile data protection system from their incumbent EPP vendors will meet their requirements. Application control and the features of vulnerability analysis are also rapidly integrating into EPP suites. Currently, MDM is largely a separate purchase for more demanding large enterprise buyers; however, small and midsize businesses (SMBs) are likely to be satisfied with EPP MDM capabilities.

The total EPP revenue of the Magic Quadrant participants at year-end 2013 was slightly more than $3 billion. However, most growth came from accounting issues versus real revenue growth. As a result, the market is up only 2% from 2012, even as the number of reported seat licenses sold increased by 6%. Essentially, this means that the license revenue per seat declined slightly. At the same time, EPP suites continue to grow in functionality. Consequently, some EPP revenue is inflow from other markets. We anticipate that growth will continue to be in the low single digits in 2014.

Magic Quadrant

Figure 1. Magic Quadrant for Endpoint Protection Platforms

STRATEGIC PLANNING ASSUMPTION

This document was revised on 22 December 2014. For more information, see the Corrections page on gartner.com

By 2018, more than 60% of EPP solutions will enable the restriction to only execute processes that have been preinspected for security and privacy risks — up from 22% today.

EVIDENCE

[1] Gartner conducted an online survey of 140 EPP reference customers in 3Q13.

[2] Good performance and malware detection testing information is available from AV-Comparatives and the AV-Test Institute.

NOTE 1
APPLICATION CONTROL

By Gartner's definition, "application control" solutions provide "policy"-based protection capabilities that can restrict application execution to the universe of known good (nonmalicious) applications. Application control solutions must provide a database of known and trusted applications, and allow changes by trusted sources. Policy must be able to range between limiting execution to the inventory of applications that are preinstalled on a machine, to running any application in the database of known good applications. More advanced application control solutions will be able to provide varying degrees of control over what an application can do once it is running, and as it interacts with system resources. Solutions that cannot enforce default-deny rules, and that do not have a database of known good applications, are considered "application lockdown" tools.

NOTE 2
DEFINITION OF "DWELL TIME"

Dwell time is the time in days that malware is on an endpoint before it is detected and quarantined or deleted.

EVALUATION CRITERIA DEFINITIONS

Ability to Execute

Product/Service: Core goods and services offered by the vendor for the defined market. This includes current product/service capabilities, quality, feature sets, skills and so on, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

Overall Viability: Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

Sales Execution/Pricing: The vendor's capabilities in all presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel.

Market Responsiveness/Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of

Source: Gartner (December 2014)

Vendor Strengths and Cautions

Bitdefender

Bitdefender (created by private software company Softwin) is primarily known for its consumer products, but is included in this analysis for its increasing enterprise market presence. Bitdefender is a consistently solid performer in anti-malware test results, and is noted by clients for ease of use and customer support. It is a good choice for SMBs in supported geographies that highly weight malware detection accuracy and performance.

Strengths

- Bitdefender provides very good malware detection capabilities, including a sandboxed application emulation environment, automatic unknown file analysis and continuous behavior monitoring, resulting in very good public test scores. The agent performance is very good with low overhead.
- The GravityZone management interface provides an easy-to-use single management console for physical, virtual and mobile endpoints, and provides a customizable dashboard. Cloud Security for Endpoints allows cloud-managed implementations, and enables managed security service providers (MSSPs) to co-brand or rebrand Bitdefender for their managed clients.
- A version of GravityZone offloads most of the antivirus functions being performed on a central server, with only a lightweight client on the endpoint.
- The Security for Mobile Devices service is available in the GravityZone Control Center. It provides anti-malware protection, Web access control, anti-phishing and encryption.
- Bitdefender was one of the first to integrate natively with VMware and offers good support for virtual servers with hypervisor-agnostic centralized scanning for virtual servers using the Security Virtual Appliance and vShield integrated agentless protection, as well as autoprotection of new virtual images.
- The company received high marks from reference customers for support and service.

Cautions

- Bitdefender's market share and mind share are very low. Its existing customer base is primarily in the SMB market. While the firm is growing very rapidly, it only has a very small base of business customers.
- The management console lacks a holistic security state assessment, vulnerability analysis or application control, forensic investigation or malware discovery capabilities. Role-based management is assigned to each individual administrator. In general, policy management is good, but some tasks require multiple windows to complete.
- Management of SharePoint and Microsoft Exchange Edge role clients is not yet included in the GravityZone central management console. Security for mobile endpoints is not yet available in the cloud management console.
- Reference customers commented on the need for improved device control (in beta now), reporting and new release testing.

Check Point Software Technologies

responsiveness.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional initiatives, thought leadership, word of mouth and sales activities.

Customer Experience: Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements and so on.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen to and understand buyers' wants and needs, and can shape or enhance those with their added vision.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.

Sales Strategy: The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service, and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements.

Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.

Check Point Software Technologies is a well-known network security company. Its venture into the EPP market, starting with the 2004 acquisition of ZoneAlarm, has suffered from poor marketing and channel execution. However, it may still appeal to organizations that value strong integration among remote access solutions, full-disk and media encryption, and malware protection, as well as for organizations seeking to consolidate network and endpoint security operations into one management and operational environment.

Strengths

- Check Point recently added forensics and investigation capabilities that record endpoint activities such as network communication, registry key changes, and file/processes manipulation in the Check Point log server for later analysis.
- Endpoint's URL filtering capability enables an off-LAN URL filtering security policy synchronized with a firewall blade policy.
- Endpoint Anti-Bot capability adds an effective postinfection solution that identifies and stops command and control (C&C)/bot traffic. Anti-Bot leverages Check Point's ThreatCloud for the latest threat indicators.
- Check Point offers selective activation of capabilities that are packaged as "software blades." These blades include a personal firewall, anti-malware (licensed from Kaspersky Lab), full-disk and media encryption, port protection, network access control (NAC), and an integrated VPN.
- Check Point's endpoint management console offers a clean interface with easy navigation and quick access to summary data. The dashboard can be customized for each administrator. Administrators may develop and view user-specific policies across multiple devices. The Endpoint Security Best Practice Report in the management console highlights the main configuration/vulnerability issues, such as vulnerable applications, misconfigurations, missing Windows service packs and potentially unwanted applications.
- Check Point offers a number of features for mobile devices, including integrated MDM and mobile app containment capabilities. Check Point's Mobile VPN supports iPhone, iPad and Android mobile devices, and also manages Exchange email synchronization.

Cautions

- Check Point did not respond to our survey or supply any reference customers, and did not disclose sufficient detail for us to adequately evaluate its progress in this market. However, based on Gartner client inquiry, it has failed to significantly impress prospective customers or improve its market share or mind share in the EPP market beyond the acquired installed base of customers.
- Check Point's dependence on Kaspersky Lab's engine and signature updates continues to challenge enterprise buyers to differentiate it from Kaspersky Lab, which is rapidly adding other competitive features.
- Check Point's application control capabilities (which it calls "program control"), augmented by its Program Advisor service, are suitable for blocking or allowing a specific set of applications, but they do not provide a manageable default-deny application execution environment.
- Check Point views MDM as a network manager's tool; consequently, MDM capabilities are in the SmartConsole dashboard, not the EPP dashboard. MDM capabilities are basic.
- Check Point protection is oriented to Windows endpoint PCs. Not all software blades are available for OS X, and Check Point doesn't offer protection for specialized servers, such as Microsoft Exchange, SharePoint or Lotus Notes.
- Although its agent will run in virtual machines (VMs), Check Point has no specific optimization for virtualized environments.

Eset

Eset has built a substantial installed base in EMEA, particularly in Eastern Europe, and it has a rapidly growing SMB presence in North America. Its Completeness of Vision score benefits from good malware effectiveness in a lightweight client, but it still suffers from a lack of investment in market-leading features, such as vulnerability detection and application control. Eset is a good shortlist option for organizations seeking an effective, lightweight anti-malware solution.

Strengths

- Its anti-malware engine is a consistently solid performer in test results. The engine benefits from virtual sandbox, which simulates executable files before execution in a virtual emulator, memory scanner, that monitors process behavior, and a vulnerability shield for widely exploited software.
- Eset Live Grid, Eset's cloud-based malware prevention system, automatically collects suspicious executable content from endpoints and analyzes it in the cloud using whitelist/blacklist, reputation, and sandbox analysis.
- SysInspector provides a point-in-time query tool to inspect system elements on demand, on event or at scheduled intervals.
- The new Eset Remote Administrator 6 now provides a Web-based user interface and significantly improved customized dashboards, reporting, workflow and policy creation.
- Eset offers an Android security and basic Android MDM capability.
- The low-performance impact of the Eset product has been noted by many customers.
- The vendor supports a broad range of Windows clients and servers. Eset Virtualization Security is a native centralized scanner for vShield-powered environments. Eset also provides a caching of clean files to reduce scanning impact in virtual environments.

Cautions

- Eset has generally been late to market with industry-leading functions, such as Web-based management consoles, MDM and virtualization support. It still does not offer application control or vulnerability scanning. Vulnerability shields do not report on Common Vulnerabilities and Exposures (CVEs) covered.
- Eset SysInspector can optionally store snapshot logs, but comparison of logs is done with Windows

Explorer, making it difficult to use for forensic investigations. The dashboards do not provide any vulnerability or configuration information that would aid in security state assessments. Although SysInspector offers vulnerability shields, it does not indicate which CVEs are covered.

- Eset Live Grid provides an automated malware sandbox. However, it only uploads files suspected by Eset and does not provide a report on malware detected. Manual submission is cumbersome and could be improved. Eset does not support VMware APIs for agentless anti-malware scanning (due in 2H15).
- MDM functions do not support iOS or Windows Phone.
- Device control is not available on OS X yet (due in 1H15).
- Eset does not yet offer a cloud-based management console, despite its focus on SMB customers.

F-Secure

F-Secure, a veteran of the anti-malware industry, has an excellent track record for malware testing results. F-Secure business solutions are targeted for SMBs seeking cost-effective solutions with low administration overhead. Its Completeness of Vision score is tempered by the slow development of advanced capabilities, such as dashboards, security state assessments, application control, MDM and virtualization protection. Its execution score is hampered by low growth and limited market presence. F-Secure is a good choice for SMB organizations in supported geographies that weight malware protection heavily.

Strengths

- F-Secure has consistently good malware test results and performance tests. It provides cloud-based lookups and a file reputation feature, which considers file metadata (such as prevalence, source and age) before allowing files to execute. We particularly like the sandbox environment, which tests unknown applications in a virtual sandbox for malicious behavior. Browsing Protection and DeepGuard exploit interception also aid detection accuracy. F-Secure client agents are lightweight with minimal performance impact.
- Software Updater provides automatic or manual updating of outdated software, including more than 2,800 versions of the most well-known endpoint and server applications.
- F-Secure Security for Virtual and Cloud Environments solution provides agent-based security that is optimized for virtual environments without tying the agent to a specific hypervisor architecture.
- The vendor offers BlackLight, one of the better rootkit detection and removal tools called.
- F-Secure has mobile security for Android. It also offers protection for a broad range of Linux variants and Mac platforms.
- F-Secure recently introduced mobile security and privacy solution called Freedome, which is a VPN, that provides safe browsing, and anti-tracking for iOS and Android.
- Younited is F-Secure's new online backup, collaboration, file sync and share solution.

Cautions

- F-Secure has very little presence or brand recognition in markets outside Northern Europe. It has a minor market share despite its long-term presence in the market.
- F-Secure's management interface is showing its age. It does not support any type of graphical dashboard, nor does it provide security state or asset information beyond anti-malware status. Autodiscovery of new, unmanaged agents and Active Directory syncing are partly a manual process and can't be scheduled, although automation exists for importing new agents and removing inactive agents. The reporting capability is very basic and does not allow for ad hoc reporting.
- The addition of Freedome and Younited is targeted for consumers and SMBs, and will have limited appeal to enterprise buyers that are looking for best-of-breed functions.
- While F-Secure has a healthy focus on malware detection effectiveness, it has not invested in more advanced protection techniques, such as security state assessments, application control, malware investigation and impact assessment capabilities or network-based malware sandboxing capability.
- F-Secure Security for Virtual and Cloud Environments does not natively support VMware NSX or vShield APIs.
- Although F-Secure develops its own signatures and behavioral detection techniques for advanced threats, its solution relies on Bitdefender as a reference engine of anti-malware signatures. Business disruptions at Bitdefender could impact F-Secure customers.

IBM

IBM's EPP offering is built on the foundation of its strong client management tool platform, the IBM Endpoint Manager (IEM). Trusteer Apex, which has some interesting application exploit protection technology, complements the Trend Micro core anti-malware engine. These tools are augmented by IBM's X-Force and Trusteer research labs. Large organizations that are considering IBM for client management tools should include IBM on their shortlists.

Strengths

- Trend Micro malware protection is augmented by Trusteer Apex, which provides memory exploit protection by limiting system calls of commonly exploited applications to known behaviors. Other notable protection mechanisms include credential protection and Java lockdown.
- IEM provides a converged endpoint management and security operations console that supports large enterprise needs across multiple endpoint types, including mobile devices and Mac devices. Tivoli Endpoint Manager (TEM) for Security and Compliance offers fully integrated patch, configuration and vulnerability management, as well as the ability to monitor other EPP agents, such as Intel Security, Symantec and Microsoft.
- IBM Endpoint Manager for Mobile Devices enables unified MDM within the same management console.
- IEM for Core Protection provides serialization of antivirus scans, and caching of files based on

virtual desktop image (VDI) golden image, while Virtual Server Protection exploits VMsafe network security APIs to provide non-agent-based virtual security.

- Add-on components include IEM for Data Protection, which provides port/device control and DLP. Application control is offered via the license of Bit9 technology.
- The security and compliance analytics Web interface can establish and monitor built-in and administrator-created key performance metrics, and show compliance over time.
- The IBM Global Services group offers mature managed security services for endpoints.

Cautions

- IBM is starting to show some traction in this market; however, mind share and market share for this solution remain very low, despite IBM's obvious size and channel advantages.
- The vendor has a large and somewhat confusing product portfolio in this market, and prospective customers must carefully match desired features with specific product offerings. The complete suite is expensive.
- The Win32 console is complicated and is not designed for nontechnical users. TEM has more reporting and management capabilities than most EPP security solutions; however, there are surprisingly few out-of-box reports for the security function, and it is still not fully optimized for the security workflow. For example, instead of searching a log for the presence of a file on a PC, administrators must create a script and push it out. IBM is investing in customized Web interfaces to improve its usability by non-operations-administrator roles as part of a broader initiative to move to a Web console.
- IEM does not offer malware detection and investigation capabilities or malware sandboxing capability, although IBM has a collection of solutions and services it calls the IBM Threat Protection System, which can aid in this function.
- Although its network host-based intrusion prevention system (HIPS) engine uses VMware's network APIs, the integrated Trend Micro anti-malware agent does not natively support VMware's vShield agentless anti-malware scanning capabilities.
- The Proventia HIPS and Virtual Server Protection products went end-of-market in April. They are being supported until April 2016, but are no longer available for new customers.
- Trusteer Apex is not integrated into the common IEM console yet.
- IEM for Core Protection does not provide antivirus protection for Exchange, SharePoint, Lotus Notes and other specialized servers.
- Reference customers noted that the signature distribution method could be improved.
- Although IBM has its X-Force and Trusteer security analysis teams, it is dependent on Trend Micro for its broad signature database. Disruptions affecting this critical partner could have an impact on IBM's customers. Integration of the latest Trend Micro engine into the TEM client can take 30 days.

Intel Security (McAfee)

Intel Security (formerly McAfee) holds the second-largest EPP market share worldwide, and offers a broad portfolio of information security solutions. Intel Security has integrated its core endpoint security components into a common endpoint agent (v.10), which should improve performance and efficacy. Intel Security's ePolicy Orchestrator (ePO) policy management and reporting framework provides a platform for addressing several aspects of the security life cycle. Intel Security is a very good choice for any organization, but especially a large, global enterprise that is seeking solid management and reporting capabilities across a number of disparate security controls.

Strengths

- Intel Security offers a broad array of protection mechanisms and has dramatically improved its malware test results. The new v.10 integrated agent combines the functions of a common communications layer, with firewall, Web controls and malware protection engine, including pretuned HIPS functionality, in a single agent deployment. The new agent is designed to be smaller, faster and more modular, with additional modules to be added later.
- The ePO management platform provides consistent management for Intel Security's security products. The "real time" query functionality allows search to detect specific client state information for incident investigation. It provides integration to over 120 third-party applications. Intel Security recently released an ePO Cloud version.
- Application Control is a full-featured solution that fully supports trusted sources of change, and integration with Intel Security's Global Threat Intelligence (GTI) provides file reputation services. Intel Security Risk Advisor provides good security risk analytics, identifying devices with vulnerabilities that need additional countermeasures or patching.
- Intel Security also added the Threat Intelligence Exchange (TIE) and Data Exchange Layer (DXL) to accelerate reputation information across both network and endpoint products, and to provide more context for threat decisions.
- Intel Security's Advanced Threat Defense (ATD) provides a centralized network-based sandbox for malware inspection. Intel v.10 clients can send suspect files to the sandbox for analysis.
- Intel Security's Management for Optimized Virtual Environments (MOVE) provides anti-malware scanning in virtualized environments. MOVE offers agentless anti-malware scanning in VMware environments using native vShield API integration, as well as hypervisor-neutral implementations to support OpenStack, Microsoft Azure and VMware vSphere.
- Intel Security Enterprise Mobility Management (EMM) 12 for mobile security and management is now fully ePO-integrated, and includes a secure container for Android, McAfee VirusScan for Android and mobile application control.

Cautions

- ePO is powerful, but at the cost of complexity. The key design strategy of the latest release is to simplify workflows, data presentation, and speed to install/use. However, smaller organizations may find it to be complex for their resources and requirements. As an alternative to ePO, Intel Security has provided a cloud-based EPO management console targeted at SMBs.

- Intel Security has the most security life cycle tools of any vendor in this analysis; however, the tools are not yet fully integrated at a policy and context layer, although the TIE and DXL will help. These security life cycle tools come at a significant premium cost compared to other solutions that are integrated out of the box into a single platform. For example, Vulnerability Manager comes at an extra cost, and does not exchange information with the HIPS vulnerability shields to show which CVEs have mitigations in place.
- ePO Real Time allows administrators to query endpoints for specific properties, but it does not maintain a database of events to aid in forensic investigations. Scalable discovery capabilities to detect indicators of compromise are also absent.
- Organizations must upgrade to the latest versions of Intel Security EPO and endpoint agent to take advantage of detection performance and administration improvements.
- A common customer complaint has been the agent size, complexity and performance impact; this should be addressed by the new v.10 client. However, at the time of this writing, it had not been demonstrated in independent tests.

- Intel's strategy is to integrate MDM into the EPP suite and, as such, it is not competing against dedicated vendors in the Magic Quadrant for Enterprise Mobility Management Suites.

Kaspersky Lab

Kaspersky Lab's global market share is growing rapidly along with its brand recognition. The company continues to augment its malware detection with internally developed, "policy"-based protection features such as application control and vulnerability management. Kaspersky Lab's Completeness of Vision score benefits from very good malware detection effectiveness as measured by test results, as well as its virtual server support, MDM, integrated application control and vulnerability analysis, tampered by an aging management interface. It is a good candidate as a solution for any organization.

Strengths

- The malware research team has a well-earned reputation for rapid and accurate malware detection. The vendor offers advanced HIPS features, including an isolated virtual environment for behavior detection, vulnerability shields, application and Windows registry integrity control, real-time inspection of code at launch, and integrated malicious URL filtering. On PCs, the endpoint agent (Kaspersky System Watcher) can perform a system rollback.
- Kaspersky offers an impressive array of integrated client management tools, including vulnerability analysis, patch management and application control. Application control includes a fully categorized application database and trusted sources of change.
- Kaspersky Security for Virtualization provides a light-agent approach combined with the use of VMware's vShield APIs for virtual guests with a shared cache, as well as agentless intrusion prevention systems/intrusion detection systems (IPSs/IDSs) and URL filtering using VMware NetX APIs. Kaspersky Endpoint Security provides life cycle maintenance for nonpersistent virtual machines, automated installation agents to nonpersistent virtual machines, and automatic load optimization.
- Kaspersky Mobile Security provides MDM capability and security agents for mobile clients. Advanced functionality includes containerization wrappers for business apps on BYOD devices.
- Centrally managed file-level and full-disk encryption, with preboot authentication for hard drives and removable devices, is integrated with endpoint security policies and application and device controls.

Cautions

- Kaspersky Lab's client management tool features (such as vulnerability and patch management) are not replacements for broader enterprise solutions. However, they are good for the enterprise endpoint security practitioner to validate operations, or to replace or augment SMB tools.
- The Microsoft Management Console (MMC) is showing its age, especially as most other vendors have migrated to Web interfaces. It is significantly more complex for less-technical small business users; however, it is possible to hide unused functionality in the Kaspersky Security Center management console. The optional Web console offers an improved experience, but it is not a replacement for the MMC console. Kaspersky does not offer a cloud-based management console. The security-state assessment capability would be improved with more predefined reports and dashboards to prioritize tasks and provide key performance metrics.
- Some customers have commented that internally developed features are of uneven quality upon general availability, although Kaspersky has improved its testing process for the next release.
- Kaspersky does not offer malware investigation and impact assessment capabilities or malware sandboxing capability.
- Security products for Exchange and Microsoft Forefront Threat Management Gateway have separate management servers and are not integrated with other Kaspersky Lab products.

Landesk

Landesk is a pioneer in the integration of client management tools, MDM and security. Landesk has its own firewall, vulnerability, patch and application control solution, and uses Kaspersky's antivirus engine for malware detection. A focus on development of IT workspaces customized for the needs of different administrator personas including security should improve the value of the suite to security operators out of the box. The Landesk Security Suite is an excellent choice for the vendor's current customers, and a good shortlist candidate for enterprises seeking integrated security and operations.

Strengths

- The base Landesk Security Suite includes an anti-spyware signature engine (from Lavasoft), a personal firewall, HIPS, device control and file/folder encryption, vulnerability and configuration management, patch management, and limited network access control (NAC) capabilities. Customers can use Landesk to manage Intel Security, Symantec, Sophos, Total Defense and Trend Micro solutions, or they may choose to pay extra for Landesk Antivirus, which leverages an integrated Kaspersky Lab malware scan engine. Landesk can also manage the Windows firewall.

- Application management functions such as patch, vulnerability management and application control capabilities enable proactive protection from malware.
- Landesk can connect and assess a machine via the VMware Virtual Desk Development Kit (VDDK) to scan and patch offline virtual machines and templates residing on ESXi Hypervisors.
- The Landesk console is comprehensive, and "IT workspaces" enable separate dashboards and workflows for personas like security administrators.
- Automated provisioning and state management are particularly useful to easily reimage PCs in the case of pervasive malware.
- Integrated MDM capability includes geofencing and location-aware policies.
- Pricing for the Landesk Total User Management suite, which also includes Client Management, MDM, IT Service Management and Asset Lifecycle Management is user-based, rather than device-based.

Cautions

- Despite several years in the security market, Landesk's market share and mind share remain very low.
- Despite the wealth of information in the Landesk solution, security state assessment and support for forensic investigation is weak. "IT workspaces" should help consolidate security information; however, Landesk still needs to prove it can adequately address the security practitioner's needs.
- Landesk doesn't conduct its own malware research; instead, it relies on Kaspersky Lab. Business disruptions between Kaspersky and Landesk could have an impact on customers. Landesk does not offer a malware sandbox.
- Not all Landesk Security Suite features are available on all managed platforms. There's no malware support for Linux, SharePoint, Lotus Notes and Android, or for Windows Mobile clients.
- Landesk needs to expand its application control capabilities with better workflow and an application database, which is due in 2015.
- While Landesk can discover, patch and inventory VMs, and its agent will run within a VM, it has no specific optimization for anti-malware protection in virtualized environments.

Lumension Security

The Lumension Endpoint Management and Security Suite (LEMSS) provides for the integration of client management tools, MDM and security. It is delivered as a single-server, single-console, single-agent architecture that includes antivirus, application control, encryption, device control, patch management and remediation. Current Lumension customers, or those seeking integrated solutions for security, operations and compliance, should add this vendor to their shortlists.

Strengths

- The anti-malware engine was switched from Norman to Bitdefender, with a linkage to VirusTotal. Advanced Memory Protection includes capabilities to detect advanced malware like memory scrapers or remote memory injection attacks. LEMSS provides a generic framework for the management of third-party security agents, such as Windows firewalls. Lumension resells Sophos SafeGuard Easy for full-disk encryption.
- The combination of vulnerability detection, patch management and application control provides a strong framework for hardening and isolating endpoints from malware. Application control capabilities benefit from a cloud-based file reputation service and a recently added memory protection capability.
- The Web-based console manages all client management tools with similar task-based orientation and consistent navigation. The full capability is delivered by a single-agent footprint, and individual modules can be licensed and delivered as pluggable services in the agent. Basic MDM capability is now fully integrated.
- Lumension Device Control is a very granular solution for managing and restricting USB and other ports, and the only solution with shadow copy capability.

Cautions

- Lumension has limited brand awareness in the EPP market outside of its patch management installed base, and the majority of its EPP customers have fewer than 500 seats. While it is growing, its EPP market share remains very low.
- Lumension has no anti-malware labs of its own; rather, it relies on an anti-malware partner to review suspicious code samples and prepare custom signatures. Disruptions to this relationship could have consequences for Lumension's customers.
- Despite the wealth of information in the LEMSS solution, security state assessment and support for forensic investigation is weak.
- There is no personal firewall component; Lumension relies on the native OS firewalls, such as the Windows firewall.
- Lumension does not provide antivirus for specialized servers (for example, Exchange and SharePoint). Although its agent will run in VMs, Lumension has no specific optimization for anti-malware protection in virtualized environments.

Microsoft

Microsoft's System Center Endpoint Protection (SCEP, formerly Forefront) is intimately integrated into the popular System Center Configuration Manager console. Microsoft licensing often includes SCEP, making it an attractive shortlist candidate. We view SCEP as a reasonable solution for Windows-centric organizations licensed under the Core Client Access License (Core CAL) that have already deployed Microsoft System Center Configuration Manager, and that have additional mitigating security controls such as application control or additional HIPS protection in place.

Strengths

- Microsoft's malware lab also benefits from a vast installation of the consumer version of the SCEP engine and its online system check utilities, which provide a petri dish of common malware samples.
- SCEP relies on the software distribution capability of System Center Configuration Manager for deployment and updates. Existing System Center Configuration Manager shops only need to deploy the SCEP agent. System Center Configuration Manager supports a dedicated endpoint protection role configuration. SCEP also allows on-demand signature updates from the cloud for suspicious files and previously unknown malware.
- Microsoft Intune is a lightweight management solution that can manage the deployment of Endpoint Protection clients and manage security policies and patch management for nondomain joined Windows PCs. Intune can also manage and enforce security policies for Windows RT, Windows Phone, Android or Apple iOS devices and integrate with SCCM.
- Organizations that are licensed under Microsoft's Enterprise CAL or Core CAL programs receive SCEP at no additional cost, leading many organizations to consider Microsoft as a "good enough" way to reduce EPP budget expenses.
- Microsoft offers advanced system file cleaning, which replaces infected system files with clean versions from a trusted Microsoft cloud.
- Microsoft's Enhanced Mitigation Experience Toolkit (EMET) provides supplemental memory and OS protection for all Windows systems and is offered to all Windows users, independent of SCEP.
- Microsoft introduces several new security features in Windows 10 (due in 2H15), including a hardware-enabled application control method to restrict execution to only signed code (see "Windows 10 for PCs Will Let Organizations Choose How Often They Update").

Cautions

- Test results of the effectiveness of SCEP are very low. Microsoft is focused on reducing the impact of prevalent malware in the Windows installed base with very low false-positive rates. It does not focus exclusively on rare or targeted threats whose impact is minimal to the entire Microsoft ecosystem.
- SCEP still lacks numerous capabilities that are common in other security solutions, including advanced device control network-based sandbox and application control. Windows features such as Firewall, BitLocker, and AppLocker are not as full-featured as comparable solutions from leading vendors, and the management of these components is not integrated into a single policy interface.
- Microsoft delivers its most important security improvements in the OS. While every Microsoft customer benefits when the OS is more secure, including those that use alternative EPP solutions, most enterprise cannot upgrade OS as fast as EPP versions.
- Microsoft System Center Configuration Manager is a prerequisite to SCEP. System Center Configuration Manager is not as easy to deploy and maintain as purpose-built EPP management platforms, and it is overkill for organizations that use other PC management solutions. System Center Configuration Manager is not designed for the unique needs of the security practitioner. Dashboard indicators are minimal and not customizable. There are only six preconfigured reports, although the offering includes a custom reporting capability.
- Despite the integration with system and configuration management, SCEP does not provide a security state assessment that combines the various security indicators into a single prioritized task list or score. SCEP also does not provide preconfigured forensic investigation or malware detection capabilities.
- SCEP provides support for virtual environments by enabling the randomization of signature updates and scans, and by offline scanning. It does not integrate with VMware's vShield or provide similar agentless solutions for Microsoft's Hyper-V environments.
- Intune MDM comes at an additional cost.
- Microsoft does not offer antivirus for SharePoint and other specialized application platforms. Mac and Linux servers are supported with clients licensed from Eset, but they do not report to the administration console.

Panda Security

Panda Security is rapidly advancing the state of the art in cloud-based EPP, with numerous advanced features that provide customers with tools for all stages of the security life cycle. Panda is the first EPP vendor to deliver a full process inventory attestation service. As a result, it can advise customers of the providence and reputation of all executed files. This is a significant innovation versus traditional malware detection services. It offers EPP, email, Web gateways and PC management capabilities — all delivered within a cloud-based management console. SMBs that are seeking easy-to-manage cloud-based solutions should consider Panda as a good shortlist entry in supported geographies (primarily Spain, Germany, Sweden, Portugal, the Benelux countries and North America).

Strengths

- Panda Advanced Protection Service (PAPS) provides for the classification of all running executable files. This service is an intelligent blend of application control and traditional malware-based analysis to provide a high degree of confidence that no malware has been missed.
- In addition to PAPS, Panda's traditional malware detection includes several proactive HIPS techniques, including policy-based rules, vulnerability shielding anti-exploit protection against commonly attacked software such as Java, and behavior-based detections. Trusted Boot ensures that all boot elements are trustable on restart, and administrators have granular control to modify policies or add exclusions. Panda uses a cloud database lookup to detect the latest threats.
- The cloud-based management interface provides granular role-based management and group-level configurations — but, at the same time, simple and frequent tasks are easy to perform. Status updates for problem resolutions are effectively summarized on the main screen. The solution provides an easy-to-use report scheduler that delivers reports in PDF. A large selection of template policies is provided, as well as many standard reports.
- An integrated cloud-based endpoint system management solution, which includes audit, configuration, patch and software distribution capabilities, remote control and MDM capabilities, is a useful optional component for maintaining endpoints in a clean state and repairing endpoints.

Mobile device management is included.

- Panda's pricing is very competitive, and there are no upfront license costs — only an annual subscription.

Cautions

- The Spain-based vendor is slowly expanding beyond its EMEA presence. However, more than 70% of its business remains in Europe, and mind share is still weak in other geographies. Panda's revenue is transitioning from a declining legacy software to a growing cloud service revenue.
- Numerous changes to Panda Cloud Systems Management are promising. However, it is still evolving from an asset inventory and remediation tool to a tool that can provide better security state assessments, vulnerability detection and forensic investigation capabilities. It provides only Microsoft patches.
- Although Panda has several large customers, the cloud-based solutions are primarily designed for SMBs that favor ease of use over depth of functionality.
- There's only one option to minimize the impact of scheduled scanning (CPU load limitation), although end users can delay scanning if they're authorized.
- The vendor is more focused on the endpoint than the server. Panda does not have any specific optimization or integration for virtualization platforms or for Microsoft SharePoint.

Qihoo 360

Qihoo 360 offers the most popular consumer anti-malware in China, with more than 400 million users. It has recently started to branch out into the enterprise EPP market in China with global expansion plans. Qihoo is good shortlist candidate for the Chinese market.

Strengths

- Qihoo has a massive installed base, which provides huge numbers of samples for data mining to create signatures and to monitor the spread of viruses/malwares. It also offers vulnerability detection and patch management for Microsoft and third-party product patches, and provides a basic application control option delivered via an app-store-type "software manager" product module.
- Qihoo uses peer-to peer technology to upgrade software, signature files and patches to save network bandwidth.
- Reference customers commented on the low resource requirement for clients.
- 360 Safeguard Enterprise for SMBs is a free, cloud-managed EPP offering for very small organizations (less than 200 seats).
- 360 SkyKey provides MDM solutions, including an antivirus engine for Android.
- 360XP Shield Enterprise Edition provides specific protection for Windows XP platforms.

Cautions

- Qihoo 360 has a dominant market share in China, but it is still in the early stages of expanding to a global market.
- Malware protection methods are based on rapid sample collection and signature distribution, rather than advanced techniques for detection malicious programs. A lack of global sample collection methods will hinder effectiveness at detecting regional threats.
- Qihoo leverages the Bitdefender Antivirus engine; disruptions in this relationship can affect results.
- Security state assessment and application inventory capabilities are very limited.
- Qihoo's enterprise product is still relatively immature. Reference customers had a long list of needed improvements, including hierarchical policy management, improved reporting, more streamlined installation packages, firewall features and more granular policy controls. Qihoo has made some progress in addressing these issues.
- Virtualization support is limited to centralized local caching of hash signature files. A VMware NSX-enabled agentless virtualization solution is scheduled for a 2Q15 release.
- All product modules are not integrated into a common management console.
- Qihoo 360 enterprise security customers are only in China. The Qihoo 360 enterprise security team supports large customers directly. Smaller organizations are only supported by a value-added reseller.
- 360 Safeguard Enterprise is currently only offered in a Chinese language version. An English version is due in 2015.

Sophos

Sophos is one of a few companies in this Magic Quadrant that sells exclusively to business markets. It has expanded into the SMB network security market, with a longer-term goal to provide a consolidated network and endpoint security solution that offers a unified, context-aware approach to threat prevention and detection and response. Sophos is good fit for buyers that value simplified administration and for SMB organizations that are interested in a unified endpoint and network approach to security.

Strengths

- Sophos recently introduced a framework ("Next-generation end-user protection strategy") to identify threats by correlating across inbound and outbound data and live and recorded events. The new Sophos Advanced System Protector coordinates among Sophos components and enables detection rules based on multiple data points such as combining URL information with file analysis and Web exploit detections. Sophos recently added Malicious Traffic Detection to identify command and control traffic from malicious or infected processes. In-agent HIPS and buffer overflow protection also aid in detecting and blocking previously unseen files.
- Sophos' management interface is, by design, very easy to use and highly capable out of the box, without the need for excessive fine-tuning. It provides consolidated management of endpoint

protection and encryption for Windows, Mac and Linux, as well as mobile device protection. Sophos Cloud, which includes endpoint protection (for Windows and Mac), mobile device management and Web content filtering, is an alternative. Integration provides user-based policies that work across devices and platforms.

- Sophos also provides a vulnerability monitoring solution to reduce the attack surface of PCs.
- Sophos Antivirus for vShield provides agentless antivirus for VMware environments. Sophos clients also support memory sharing, staggered scheduled scans and updated randomization for other virtual platforms. It recently added vShield cleanup functionality.
- Client-based URL filtering blocks known malicious sites. Sophos integrated its EPP with its Web and firewall gateway products to apply Web policy and reporting on mobile devices.
- Data protection is enhanced with an increasing range of DLP features and context-driven encryption policies, which can be applied to data that is written to removable media. A new optional feature in SafeGuard Enterprise extends Sophos encryption to file servers and cloud storage at no additional charge.
- Sophos offers user-based pricing rather than device-based prices.

Cautions

- Sophos suffers from a weak marketing presence, particularly in North America. Sophos Antivirus for Mac, a free consumer tool offering Mac security, should help drive more brand awareness.
- The simplicity of Sophos' management console becomes a liability in larger enterprises that need more granular control and reporting. The security state assessment capabilities are buried and should be moved to the main dashboard. The cloud management interface is still maturing and does not include all product or all capabilities of the on-premises management server.
- Sophos' malware test results are average and could be improved. Reference customers commented on the need for better malware remediation tools from Sophos.
- Sophos does not provide application control suitable for a default-deny execution environment for endpoints (a server-based product was recently introduced).
- Sophos' acquisition of unified threat management gateway vendor Astaro and more recently Cyberoam may create new opportunities to compete with companies in the unified threat management market, but it does not improve Sophos' competitive standing in the EPP market yet.

Stormshield

Stormshield targets organizations looking for protection from advanced persistent threat (APT) attacks. Stormshield's Ability to Execute score is hampered by its relatively small market share and limited geographic presence. Its Completeness of Vision score benefits from its design as a seamless, integrated EPP with a focus on behavioral memory protection, tempered by a still-maturing management console and a Windows-only focus. It is a reasonable shortlist solution for organizations in supported geographies that are seeking a supplemental behavior-based approach to malware detection.

Strengths

- The Stormshield security suite is designed to address system and data protection via an extensible EPP capability that integrates multiple layers of security. These include a host-based intrusion prevention system (HIPS), a personal firewall, device control, encryption, and an optional, fully integrated, signature-based anti-malware engine licensed from Avira. The suite boasts a single lightweight agent (15MB, including anti-malware protection) that is extensible to support multiple functions and runs at the kernel level.
- We particularly like Stormshield's focus on advanced behavioral-based HIPS techniques, such as memory overflow protection, anti-keylogging, application control, rootkit detection, honey pots, privilege escalation, reboot protection and driver management. Remediation and status assessment are enabled with administrator-generated scripts.
- Stormshield Endpoint Security effectively uses policy-based restrictions to minimize the attack surface with object-oriented policies and configurations that are easy to set up. The Stormshield Device Control module permits granular data usage controls. Policy-based application restriction policies include a challenge response mechanism, which allows self-authorization.
- A specific protection solution for Windows XP has received interest from customers using XP-based systems after Microsoft officially ended support in early 2014.
- For better integration on virtualized servers, Stormshield Endpoint Security supports the deployment and management of the agent on a pool of virtual machines and templating with VMware Horizon.
- Stormshield has created a bundled mobile data protection product that includes Stormshield data and endpoint security but doesn't have any technical integration.

Cautions

- Stormshield has a very small market share in this Magic Quadrant and does not have significant brand recognition (multiple name changes have not helped) or a significant enterprise client base outside Europe. Increased focus on the network appliance channel is unlikely to reach enterprise endpoint buyers.
- Despite its focus on preventing advanced persistent threats (APTs) and more sophisticated malware, Stormshield Endpoint Security does not offer much help for investigating forensic or remediation actions. Improvements in this area are expected in 2015.
- Stormshield Endpoint Security does not participate in any of the prominent endpoint protection malware tests, so it is difficult to compare its malware detection performance against other solutions in the market.
- More than 75% of Stormshield Endpoint Security customers use it to augment existing EPP, rather than as a replacement.
- Stormshield supports Windows only, and provides no Mac, Linux, Unix, mobile or email server support. Although it works in a VM environment, there are few features specific to virtualization.
- Application control is suitable for allowing or blocking specific applications, or for completely

locking down clients, but it does not have workflow features or an application database that would allow a flexible application control environment. Dedicated application control solutions providing improvements are due in 2015.

- The only option for signature-based anti-malware protection is from Avira. Stormshield has a very small malware research team and is dependent on Avira for signature-based protections. Business disruptions at Avira could impact Stormshield Endpoint Security customers.
- The management interface is comprehensive but not intuitive, and is not recommended for nontechnical users. The console lacks dashboards and context-sensitive help. It is not Web based. Much of the advanced capability is achieved by administrators creating their own scripts.
- Ad hoc reporting is not supported. Reports can be filtered, but not changed, and it is not possible to drill down into details.
- There is no out-of-the-box security state assessment beyond the EPP agent status, and no significant integration with operations tools such as vulnerability assessment.

Symantec

In October 2014, Symantec announced yet another new strategy to reinvigorate company growth by splitting the information management business unit and the security products groups into separate companies (see "Symantec Split Provides Opportunity to Focus, but No Immediate Customer Benefit"). Symantec's Completeness of Vision score is affected by the lack of application control, malware sandboxing, vulnerability analysis and forensic investigation capabilities. Its Ability to Execute score is impacted by nearly two years of corporate strategy disagreements, resulting in a slower growth rate moderated by the fact that Symantec is still the market share leader. Symantec remains a good tactical choice for solid anti-malware endpoint protection.

Strengths

- Symantec Endpoint Protection (SEP) 12 has an extensive set of layered defense capabilities, such as Symantec Online Network for Advanced Response (SONAR), Symantec Insight and its network protect technologies, which go beyond traditional signatures for protection from advanced targeted attacks. Most recent improvements were in components of SONAR. Symantec also integrated an advanced repair tool, Power Eraser, into the Symantec Endpoint Protection client.
- Symantec Insight provides a file reputation service that can restrict executable file download based on prevalence, source and age.
- Symantec Data Center Security leverages VMware's vShield APIs and NSX to offer "agentless" antivirus and reputation security features on a VMware ESX hypervisor. On other platforms such as Hyper-V or Kernel-based Virtual Machine (KVM), SEP provides I/O sensitive scan, virtual image exception and file cache, offline image scanner, and randomized scanning.
- For server-based HIPS, Symantec Data Center Security: Server Advanced (formerly Critical System Protection) has broad platform support compared with competitors.
- Symantec has solid MDM capabilities from its acquisitions of Odyssey Software and Nukona, which were integrated into a single console, Mobility: Suite 5.0.
- Not until 2014 did Symantec add agentless anti-malware scanning support leveraging the native VMware vShield APIs. It was the last leading EPP provider to do so.

Cautions

- Symantec has been in a nearly continuous rebuilding mode since 2012, with few customer benefits to show for its efforts. In the longer term, it is easy to imagine that a more focused security company may be better for security customers; however, in the short term, it has more significant potential for disruptions. Moreover, real product improvements will only result from a durable corporate strategy, regardless of the company size.
- Symantec's security products portfolio is not integrated at a meaningful level.
- SEP 12 remains weak in proactive security state assessments as well as forensic and discovery capabilities, and promised products addressing these weaknesses are still not available.
- Symantec lacks a network-based sandbox product that can analyze suspect code and report on its behavior (it is due in 1H15).
- Symantec does not offer any application control capability beyond administrator-defined lockdown capability. The Insight file reputation technology only works on file downloads.
- Symantec's server protection offerings center around Symantec Data Center Security and its Control Compliance Suite, but they use a different management console and reporting framework.
- Although Symantec has mobile security capabilities, they are not integrated into the SEP management console.
- Removable media encryption requires adhering to a confusing set of policies across Symantec's encryption products and SEP 12's device control functionality.

ThreatTrack Security

ThreatTrack Security's VIPRE (Virus Intrusion Prevention Remediation Engine) EPP solution is squarely aimed at the small business market, where ease of use and "set and forget" functionality are sought-after attributes; however, ThreatTrack is now attempting to move VIPRE into the midsize and large enterprise business. The vendor should be considered by SMBs that are looking for straightforward anti-malware protection with a low performance impact.

Strengths

- The VIPRE console provides consistent management across Windows and Mac clients, as well as email anti-malware scanning. MDM capabilities for Android and iOS are available in the same integrated console.
- The latest version of VIPRE Business Premium includes integrated PC application patch management capabilities, which will appeal to organizations that have no other solution for patch management.
- VIPRE for Hyper-V installs on the host server and can scan guest machines through the hypervisor,

so no agent is required on the guest operating systems. It leverages workload management to prevent overutilization of resources on the host so that the scans do not interfere with the availability of the host or guests.

- Roaming service allows VIPRE clients outside the network to contact the management server.

Cautions

- ThreatTrack is one of the smallest vendors in this report, and has a very low mind share and market share in the enterprise market. The majority of its customers are SMBs.
- Scores in the latest AV-Test are below average.
- The management console is not Web-based, and it is more complicated than expected given the target market. It does not offer much in advanced enterprise capability. Exchange anti-malware agents are managed in a separate console (integration is due in 1H15). Despite the target market, it does not offer a cloud-based management console.
- ThreatTrack's patch management capabilities are limited to 40 common Windows applications. Mac OS is on its road map.
- ThreatTrack does not sell a device control solution (it is due in 1Q15).
- ThreatTrack has no application control capabilities. Its MDM capability is limited.
- It has no specific integration with VMware's vShield APIs, although scanning can be randomized to reduce loading.

Trend Micro

Trend Micro is the third-largest enterprise EPP vendor, with a large worldwide installed base. Trend Micro offers a distinct focus on the needs of data center protection with Deep Security for servers, and has made significant visionary investments in the areas of application control, malware sandboxing, incident response investigation and forensics, and integrated MDM and mobile app reputation service. Trend Micro is a good shortlist candidate for all types of buyers.

Strengths

- OfficeScan provides a range of malware protection options including malicious URL filtering, critical resource and process protection, browser-exploit protection, vulnerability shielding, and behavioral monitoring. Trend Micro has also invested in leading-edge security products including a malware sandbox, application control and an incident response investigation tool. The endpoint sensor investigation tool has an excellent graphical representation of the threat event chain.
- Trend Micro's application control solution is complete with trusted sources of change and an application catalog. It is bundled in the Smart Protection suites.
- The Trend Micro Deep Discovery network-based malware detection sandbox can be centralized to receive files from Trend Micro Web gateway and email security products. It received top scores from NSS Labs in a malware sandbox test.
- Trend provides vulnerability assessment and vulnerability shields (virtual patches). Reports show vulnerability, severity and applicable virtual patches helping to prioritize patch availability.
- Worry-Free Business Security Services provides protection for Windows, Mac, iOS and Android devices delivered as a cloud service.
- Deep Security and its "agentless" anti-malware scanning, intrusion prevention and file integrity monitoring capabilities for VMware have benefited greatly from Trend Micro's close relationship with VMware. Further, Deep Security has been optimized to support the protection of multitenant environments and cloud-based workloads, such as Amazon Web Services. Capabilities include encrypting these workloads with its SecureCloud offering and an optional SaaS version of its Deep Security management console.
- Trend Micro integrates mobile device management capabilities in Trend Micro Control Manager (TMCM), with support for Android, iOS, Windows Phone, Symbian and BlackBerry.

Cautions

- Management interface could be improved. Dashboards would be improved with more at-a-glance visual information versus list-based information. Multiple management consoles create some dead ends in workflow; for example, administrators cannot pivot from investigate function from the TMCM management console. Application control is a separate management console from Office Scan and TMCM, although both report to Control Manager for reporting.
- Trend Micro has not brought the "agentless" anti-malware scanning capabilities to OfficeScan; rather, it has left customers that want to do this for VDI to adopt Deep Security for hosted virtual desktop protection. OfficeScan and Deep Security are two separate products from separate teams with separate consoles, although both report up to the Trend Micro Control Manager for reporting.
- Some capabilities (like encryption and application control) have been integrated into TMCM, but still require their native consoles to be deployed, although from that point forward, they can be managed within TMCM.
- The Deep Discovery malware sandbox needs to be better integrated into the OfficeScan and deep security clients. The endpoint sensor client agent is required to automatically send unknown files to the sandbox, and Deep Discovery is not integrated into application control workflow for approving new unknown applications.
- Application control does not include self-updating applications and software deployment tools as trusted sources (due in 1H15). It also does not provide an out-of-the box inventory report; however, customers can create their own customized report and do their own inventory search and export in both Trend Micro Control Manager and Application Control.
- Asset tagging is limited to static information, making it hard to create dynamic groups.

Webroot

Webroot SecureAnywhere Business — Endpoint Protection takes a behavior-based approach that uses cloud databases to keep its EPP client small and fast. The cloud lookup classifies all files as good, bad or unknown, providing a higher degree of confidence in detection accuracy. Webroot SecureAnywhere is a

reasonable shortlist inclusion for organizations in supported geographies that are seeking a lightweight, behavior-based approach to malware detection. It can also be a good additional tool for high-security organizations.

Strengths

- Webroot SecureAnywhere is one of the few products to focus primarily on behavioral rules to identify threats. Webroot SecureAnywhere works by monitoring all new or highly changed files or processes, and checks file metadata and behavior against the cloud database of known files and behaviors. The cloud lookup results in a very small and fast EPP client. Webroot is the only vendor in this analysis that reports on malware dwell time.
- By journaling changes undertaken by unknown files, Webroot provides rapid remediation once malware behavior is detected. Consequently, remediation of ransomware such as Cryptolocker is possible by restoring data files from journaled versions, even if the initial infection evades detection.
- Webroot SecureAnywhere provides a remote management tool, built-in application process monitoring, a change log and rollback functionality to ease remediation. It also features remote application management controls using its override function, as well as a built-in identity and privacy shield to minimize the loss of sensitive data from unknown malware.
- Both the Endpoint Security consoles and the new Global Site Manager management consoles are cloud-based, with no on-premises server requirement.
- Administrators can build policies around the actions to be taken on files introduced onto the endpoint, including those via USB or CD/DVD.
- The vendor also offers security and basic MDM capability, including a mobile app reputation service for Android and iOS devices from within the same management console.
- Webroot again received the highest satisfaction scores from reference customers that were contacted for this Magic Quadrant.

Cautions

- Due to Webroot's emphasis on a behavior-based malware detection approach, existing malware testing does not accurately reflect capabilities, making it hard to compare efficacy to other solutions.
- SecureAnywhere is strictly an anti-malware utility. It does not provide port/device control, application control, malware event investigation capability or endpoint management utilities, such as vulnerability or patch management.
- High-level event data for all endpoints is provided via the Web-based management console; however, the dashboard is not customizable and does not allow for drill-down into log data. More granular data must be obtained through log files, accessible on a per-agent basis.
- Webroot does not protect the workload of specialized servers, such as Exchange and SharePoint.
- MDM is currently a separate management console.

Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants and MarketScopes as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant or MarketScope may change over time. A vendor's appearance in a Magic Quadrant or MarketScope one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. It may be a reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

Added

Intel Security is the new brand name for McAfee. Qihoo is a new participant this year. Stormshield is the new name of Arkoon Network Security after its merger with Netasq.

Dropped

BeyondTrust no longer qualifies for inclusion due to a prioritization of focus on privileged account management and vulnerability management rather than EPP-style protection.

Inclusion and Exclusion Criteria

Inclusion in this Magic Quadrant was limited to vendors that met these minimum criteria:

- Detection and cleaning of malware (for example, viruses, spyware, rootkits, trojans, worms), a personal firewall, and an HIPS for servers and PCs
- Centralized management, configuration and reporting capabilities for all products evaluated in this research, sufficient to support companies of at least 5,000 geographically dispersed endpoints
- Global service and support organizations to support products

Evaluation Criteria

Ability to Execute

The key Ability to Execute criteria that were used to evaluate vendors were Overall Viability and Market Responsiveness/Record. The following criteria were evaluated for their contributions to the vertical dimension of the Magic Quadrant:

- **Overall Viability:** This includes an assessment of the financial resources of the company as a whole, moderated by how strategic the EPP business is to the overall company.
- **Sales Execution/Pricing:** We ranked vendors based on whether reseller references reported satisfaction with their technical training, sales incentives, marketing and product quality, and on overall vendor satisfaction scores accumulated over the past three years.

- **Market Responsiveness/Record:** We ranked vendors by their market share in total customer seats under license.
- **Marketing Execution:** We ranked vendors based on self-reported growth rates in seats under license as a percentage of overall new seat growth for the market.
- **Customer Experience:** We ranked vendors based on reference customers' satisfaction scores as reported to us in an online survey, averaged over the past three years.
- **Operations:** We evaluated vendors' resources dedicated to malware research and product R&D, as well as the experience and focus of the executive team.

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product or Service	Not Rated
Overall Viability	High
Sales Execution/Pricing	Medium
Market Responsiveness/Record	High
Marketing Execution	Medium
Customer Experience	High
Operations	Medium

Source: Gartner (December 2014)

Completeness of Vision

The key Completeness of Vision criteria in this analysis were Market Understanding and the sum of the weighted Offering (Product) Strategy scores:

- **Market Understanding:** This describes the degree to which vendors understand current and future customer requirements, and have a timely road map to provide this functionality.
- **Offering (Product) Strategy:** When evaluating vendors' product offerings, we looked at the following product differentiators:
  - **Anti-Malware Detection and Prevention Capabilities:** This is the speed, accuracy, transparency, and completeness of signature-based defenses, as well as the quality, quantity, accuracy, and ease of administration of non-signature-based defenses and removal capabilities for installed malware. We looked at test results from various independent testing organizations, and used Gartner inquiries as guides to the effectiveness of these techniques on modern malware.
  - **Management and Reporting Capabilities:** This is comprehensive, centralized reporting that enhances the real-time visibility of end-node security state and administration capabilities, and eases the management burden of policy and configuration development. Vendors that have embarked on endpoint management operation integration have shown considerable leadership, and were given extra credit for registering as "positive" on this criterion.
  - **Application Management Capability:** We looked for the ability to provide a holistic-state assessment of an endpoint security posture, and for prioritized guidance and tools to remediate and reduce the potential attack surface. This capability includes configuration management, vulnerability management and integration with patch management tools. We also looked for the capability to apply a flexible default-deny application control policy that allows for trusted sources of change, and can handle requirements ranging from full lockdown to allowing any trusted application to run.
  - **Supported Platforms:** Several vendors focus solely on Windows endpoints, but the leading vendors can support the broad range of endpoint and server platforms that are typically found in a large enterprise environment. In particular, we looked for support for virtualized environments as well as Mac and mobile devices; we also looked for specialized servers, such as email and collaboration servers.
- **Innovation:** We evaluated vendor responses to the changing nature of customer demands. We accounted for how vendors reacted to new malicious code threats (such as spyware and APTs), how they invested in R&D and/or how they pursued a targeted acquisition strategy.
- **Geographic Strategy:** We evaluated each vendor's ability to support global customers, as well as the number of languages supported.

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	High
Marketing Strategy	Not Rated
Sales Strategy	Not Rated
Offering (Product) Strategy	High
Business Model	Not Rated

Vertical/Industry Strategy	Not Rated
Innovation	Medium
Geographic Strategy	Low

Source: Gartner (December 2014)

Quadrant Descriptions

Leaders

Leaders demonstrate balanced progress and effort in all execution and vision categories. Their capabilities in advanced malware protection, data protection and/or management features raise the competitive bar for all products in the market, and they can change the course of the industry. However, a leading vendor isn't a default choice for every buyer, and clients should not assume that they must buy only from vendors in the Leaders quadrant. Some clients believe that Leaders are spreading their efforts too thinly and aren't pursuing clients' special needs.

Challengers

Challengers have solid anti-malware products that address the foundational security needs of the mass market, and they have stronger sales, visibility and/or security lab clout, which add up to a higher execution than Niche Players offer. Challengers are good at competing on basic functions rather than on advanced features. They are efficient and expedient choices for narrowly defined problems.

Visionaries

Visionaries invest in the leading-edge (aka "bleeding edge") features — such as advanced malware protection, data protection and/or management capabilities — that will be significant in the next generation of products, and will give buyers early access to improved security and management. Visionaries can affect the course of technological developments in the market, but they haven't yet demonstrated execution. Clients pick Visionaries for best-of-breed features, and, in the case of small vendors, clients may enjoy more personal attention.

Niche Players

Niche Players offer viable, uncomplicated anti-malware solutions that meet the basic needs of buyers, or that focus on a specific protection capability. Niche Players are less likely to appear on shortlists, but fare well when given a chance. They typically address the low-overhead, basic anti-malware needs of the broader market. Clients tend to pick Niche Players when the focus is on a few specific functions and features that are important to them.

Context

Protection from common malware, as well as more APTs, is the top critical consideration for EPP buyers. There is significant variation in the quality of attack prevention, as illustrated by multiple malware testing organizations.[2] Buyers should look for solutions that offer a broad portfolio of protection techniques and high efficacy as determined by multiple public test results.

Solutions should provide a holistic security state assessment and a prioritized action plan to remediate potential security gaps. This not only enables administrators to proactively lower the attack surface on endpoints, but also can provide a performance metric that can be tracked over time to demonstrate the effectiveness of security operations.

Protection from highly targeted, new and low-volume attacks requires a more proactive approach that is grounded in solid operations management processes, such as vulnerability analysis, patch management and application control capabilities. In particular, application control, which restricts execution to known good applications, is proving to be effective in demanding security environments, and is especially effective when combined with support for trusted change and supplemented with cloud-based file reputation services.

Full application attestation — that is, classifying the entire application and process inventory into bad good or unknown classifications and rapidly classifying the unknown — will provide higher degrees of confidence that endpoints are malware-free. Traditional approaches using malware-detection-only approaches can leave unknown process lurking for long dwell times. Integration with cloud-based or private malware sandboxes will improve the speed of classification of unknown objects.

In theory, any security solution can be bypassed. Enterprise buyers should look for malware infection detection tools. These tools provide the capability to alert administrators about threats that may have had a longer dwell time (see Note 2) or more virulent infections. Malware investigation information should be sufficient to enable administrators to perform their own manual inspections for missed components of more complex infections, and to ascertain when, where and how the initial infection occurred, what happened after the infection started, as well as what other systems have handled the malicious content (see "Market Guide for Endpoint Detection and Response Solutions").

Solutions should include MDM capabilities and data protection for mobile and employee-owned devices. Buyers should favor solutions that have a short-term integration road map of the MDM capability into the broader suite.

Performance on virtual servers and hosted virtual desktops/the virtual desktop infrastructure is an increasingly important critical capability. Consider the level of optimization and integration for virtual servers, but do not assume that solutions must be "agentless" to provide the best performance. There are other ways to optimize performance in virtualized environments — for example, with the coordinated sharing of caches between VMs.

Server platforms are commonly supported by EPP vendors; however, optimal server protection may require additional features and protection mechanisms, such as file integrity monitoring or Web application firewalls. Enterprise buyers should consider specialized server solutions.

Solutions that take a more operational tool approach will be more flexible and provide more security state information, more forensic information and better remediation capability. IT organizations that cannot handle the increased complexity should outsource EPP management to MSSPs.

Market Overview

The rise of the targeted attack is shredding what is left of the anti-malware market's stubborn commitment to reactive protection techniques. Improving the malware signature distribution system or adapting behavior detection to account for the latest attack styles will not improve the effectiveness rates against targeted attacks. When 47% of reference customers for EPP solutions[1] have been successfully compromised, it is clear that the industry is failing in its primary goal of keeping malicious code off PCs. The sad reality is that any targeted attacker will code and test his or her payload to evade the target's anti-malware system. To be successful going forward, EPP solutions must be more proactive and focus on the entire security life cycle.

There are essentially four stages in the security life cycle:

1. **Setting policy:** In this stage, organizations need to proactively configure the endpoint to reduce the potential attack surface. Technical solutions that help at this stage include configuration and vulnerability assessment, patching and application control.
2. **Prevention:** This stage describes the implementation of real-time protection techniques to identify and filter malware. The techniques used include file, IP and URL reputation; real-time code analysis; behavioral monitoring; and virtual code execution (sandboxing).
3. **Detection:** The aim of this stage is to detect anomalies that indicate the presence of threats already resident on the endpoint. The key goal of this stage is rapid detection, thus reducing the dwell time of threats when they have successfully evaded the protection stage. An ancillary benefit is that detection techniques often provide information for remediation and forensic investigation.
4. **Remediation:** This stage focuses on repairing damage and implementing lessons learned.

In this Magic Quadrant analysis, we have evaluated vendors based on the features they provide to aid in all stages of the security life cycle.

Proactive policy-setting work — like patching Web-facing applications and utilities, reducing the number of applications to manage, removing administrator rights, and potentially exploiting application control — will, by itself, defeat 85% to 90% of malware. When we reference "security state assessments" in this analysis, we are describing the vendor's ability to quickly show the current posture of the device and its susceptibility to malware infection, and to provide prioritized remediation actions.

Despite the need to focus on the security life cycle going forward, we must acknowledge that EPP buyers put the highest value on *prevention,* hoping to avoid the additional work of proactively setting policy or tracking down anomalies that may turn out to be false positives. Consequently, in this Magic Quadrant, we continue to weigh prevention and performance heavily in our Completeness of Vision analysis.

Concurrently, long dwell times are a hallmark of successful advanced attacks. Gartner clients are searching for tools that can help reduce these long dwell times. When we discuss "detection" or "forensic" capability, we are addressing the vendor's ability to identify clients that may already be compromised, as well as tools that aid in incident response and forensic investigation (see "Market Guide for Endpoint Detection and Response Solutions"). Most enterprise buyers are starting to look for EPP products that can address not only Windows PCs, but also a broad array of servers and clients. We evaluated a vendor's ability to protect and manage new endpoints (such as Mac, iOS and Android devices), which are integrated into the management console. Today, many large enterprise buyers are selecting a best-of-breed MDM capability; however, within the next two years, we expect the EPP market to subsume this function (which is already happening at the SMB end of the market).

We also considered specialized features for virtualized servers, as well as the breadth of protection for specialized servers such as Exchange, SharePoint, Linux and Unix.

The large enterprise EPP market is still dominated by Symantec, Intel Security and Trend Micro, which represent approximately 65% of the total revenue of Magic Quadrant participants. Sophos and Kaspersky Lab are the two other global Leaders that are competitive across multiple functions and geographies. The combined Leaders quadrant market share is 81%. While still dominant, the combined market share of the Leaders is down 4% from the 2013 analysis. The displacement of incumbents is still a significant challenge in the large enterprise market; however, in the less demanding small and midsize market, competition is more intense, and the Niche Players and Visionaries collectively are slowly eroding the market share of the Leaders with a dedicated focus on specific features or geographic regions.

In the longer term, we believe that the increased displacement of Windows endpoints by application-controlled OSs (such as Windows 10, Microsoft Windows Runtime, and Apple's iOS and OS X Mountain Lion) is the biggest market threat. These solutions shift the value proposition of EPP solutions from traditional anti-malware to MDM and data and privacy protection capabilities. Concurrently, there are numerous startups responding to the market demand for better protection and detection capacities looking to displace or augment incumbents. Vendors such as Bit9, Cylance, CrowdStrike, RSA (The Security Division of EMC) and Bromium are primarily focused on the protect phase of the market. Vendors such as AccessData, Guidance Software, Promisec, Tanium, Triumfant, Carbon Black, RSA (ECAT) and FireEye are aimed mostly at the detect and remediate side of the market. We believe these new entrants will force EPP incumbents into a new phase of innovation and acquisition. Enterprises that are a frequent target for persistent attackers should experiment with these new vendors and pressure incumbent vendors to step up innovation.