Magic Quadrant for Endpoint Protection Platforms

8 January 2014 ID:G00247705

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. Vendors in this market compete on the quality of their protection capabilities, the depth and breadth of features, and the ease of administration.

Market Definition/Description

(This document was revised on 14 January 2014. The document you are viewing is the corrected version. For more information, see the Corrections page on gartner.com.)

The enterprise endpoint protection platform (EPP) market is a composite that is primarily made up of collections of products. These include:

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

EPP solutions also will often include:

- Full-disk and file encryption, also known as mobile data protection
- Endpoint data loss prevention (DLP)
- Vulnerability assessment
- Application control (see Note 1)
- Mobile device management (MDM)

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. In this analysis, we focused 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, and vulnerability assessment. See the Completeness of Vision section below 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 or midsize businesses (SMBs) are likely to be satisfied with EPP MDM capabilities.

The total EPP revenue of the Magic Quadrant participants at year-end 2012 was slightly more than $2.8 billion — essentially flat from 2011 — even as the number of reported seat licenses sold increased by 8%. Essentially, this means that the license revenue per seat was declining slightly. At the same time, EPP suites continue to grow in functionality. Consequently, some EPP revenue is

STRATEGIC PLANNING ASSUMPTION

By 2017, more than 50% of end-user devices will be restricted to running only apps that have been preinspected for security and privacy risks — up from 20% 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.

inflow from other markets. We anticipate that growth will continue to be in the low single digits in 2014.

Return to Top

Magic Quadrant

Figure 1. Magic Quadrant for Endpoint Protection Platforms

Source: Gartner (January 2014)

Return to Top

Vendor Strengths and Cautions

Arkoon Network Security

Arkoon Network Security was acquired by Cassidian CyberSecurity, an aerospace and defense company. Arkoon'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 protection, tempered by a still-maturing management and a Windows-only focus. It is a reasonable shortlist solution for organizations in supported geographies that are seeking a 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 Arkoon'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 effectively uses policy-based restrictions to minimize the attack surface with

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 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.

object-oriented policies and configurations that are easy to set up. Policy-based application blacklisting/whitelisting is improved by a challenge response mechanism, which allows users to add software if they type in the justification for the installation in a pop-up window.

- Full-disk encryption as well as encryption for files and folders on fixed hard drives and removable devices is available. Recent improvements include support for fully encrypted logical containers in addition to per-file encryption.
- Arkoon has created a bundled mobile data protection product that includes SecurityBox and StormShield, but doesn't have any technical integration.

Cautions

- Although it continues to grow rapidly, StormShield has a very small market share in this Magic Quadrant. Neither SkyRecon Systems in France nor its parent company Arkoon have significant brand recognition or a significant enterprise client base outside Europe. Arkoon's acquisition by Cassidian, its second owner in two years, is unlikely to improve its near-term enterprise presence outside of defense and aerospace.
- Despite its focus on preventing advanced persistent threats (APTs) and more sophisticated malware, StormShield does not offer much help in detecting existing malware, or support for forensic or remediation actions.
- StormShield 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.
- StormShield supports Windows only, and provides no Mac, Linux, Unix, mobile or email server support. Although it works in a virtual machine (VM) environment, there are no 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.
- The only option for signature-based anti-malware protection is from Avira. Arkoon has a very small malware research team and is dependent on Avira for signature-based protections.
- The management interface is comprehensive, but not recommended for nontechnical users. The console lacks dashboards and context-sensitive help. 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.

▲ Return to Top

BeyondTrust

BeyondTrust continues to integrate reporting from eEye's vulnerability analysis and endpoint protection with its privileged management solutions. Current BeyondTrust and Retina Vulnerability Management customers and enterprises that value integrated vulnerability analysis should consider BeyondTrust's PowerBroker Endpoint Protection Platform (formerly named Blink).

Strengths

- With its flash-based management console, BeyondInsight combines vulnerability analysis and endpoint protection (formerly eEye Retina CS Threat Management Console and eEye Blink Professional/Server).
- BeyondTrust PowerBroker for Windows (a separate endpoint agent at this time) enables the removal of Windows administrator rights while still selectively escalating privileges for legacy applications. The PowerBroker solution suite also provides tools for database monitoring, Active Directory bridging, least privilege on Unix, Linux and OS X, and auditing of Active Directory, SQL and exchange.
- In addition to licensed anti-malware signature libraries from Norman, BeyondTrust now has a small team of malware experts that provide excellent technical support and malware information.
- The anti-malware techniques include process execution rules, registry protection and file integrity monitoring.
- BeyondTrust is one of the few providers in this Magic Quadrant analysis to offer a service-level agreement (within 48 hours) on new critical vulnerabilities, meaning that it will identify critical vulnerabilities within 48 hours based on its integrated vulnerabilities assessment engine (Retina).
- BeyondTrust offers Retina Mobile, which can provide a mobile vulnerability scan on Android, iOS, BlackBerry, and other devices through various technology and MDM connectors.

Cautions

- Beyond Trust continues to grow quite rapidly; however, it has a very small market share in the EPP market, and is rarely mentioned by Gartner clients. Most of its installed base is in North

America.

- The management dashboard cannot be customized. It has limited drill-down from the dashboard into actions or logs. Although it has the ability to collect custom information, it must be predefined and scheduled for collection, making it less useful for forensic investigation or remediation. There is no ability to pull information from clients; this data is only available as push from the clients to the management console.
- The solution has the capability to blacklist applications, but it is a manual process with no trusted sources of change. It is not a full application control solution.
- Although the PowerBroker team develops its own signature spyware database and cleanup routines, the solution relies on Norman for anti-malware signatures; therefore, business disruptions at Norman could impact PowerBroker customers. Although the Norman anti-malware engine is tested regularly, PowerBroker EPP does not participate in any industry tests to demonstrate the effectiveness of its collection of technologies. Automated malware damage cleanup capabilities are limited.
- PowerBroker EPP has limited device control capabilities, and no encryption capabilities.
- PowerBroker EPP supports only Windows OS desktop and server platforms (including Microsoft Internet Information Services [IIS] using an integrated Web Application Firewall based on BeyondTrust's own SecureIIS technology).
- The anti-malware agent works on a virtualized Windows host; however, it is not optimized for a virtualized environment.

Return to Top

Bitdefender

Bitdefender (created by private software company Softwin) is primarily known for its consumer products, but is now included in this analysis for its increasing enterprise market presence. Bitdefender is a consistently solid performer in anti-malware test results, and 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

- GravityZone, the recently updated 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.
- Bitdefender provides very good malware detection capabilities, including a sandbox application emulation environment and continuous behavior monitoring.
- The "GravityZone-in-a-Box" solution 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 GravityZone Control Center. It provides anti-malware protection, Web access control, anti-phishing and encryption.
- Bitdefender offers good support for virtual servers with both 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.

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 is only from a very small base of business customers.
- The management console lacks a holistic security state assessment, forensic investigation, and malware discovery capabilities. Role-based management is assigned to each individual administrator. In general, policy management was good, but some tasks require multiple windows to complete.
- Bitdefender does not offer policy-based protection mechanisms, such as vulnerability analysis or application control.
- Management of Mac, Exchange, SharePoint and Microsoft Exchange Edge role clients is not yet included in the GravityZone central management console. (However, management of Mac is expected in 1Q14, and management of Exchange is expected in 2H14.)
- Reference customers commented on the need for improved device control, reporting and new release testing.

Return to Top

Check Point Software Technologies

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 will still appeal to organizations that value strong integration among remote access solutions, full-disk and media encryption, and malware protection.

Strengths

- 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 does not disclose sufficient detail for us to adequately evaluate its progress in this market; however, based on Gartner client inquiry levels about Check Point's EPP solutions, it has failed to significantly 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 with 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 SmartDefense 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 VMs, Check Point has no specific optimization for virtualized environments.

Return to Top

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 weak enterprise management capabilities and lack of investment in market-leading features, such as application control and virtualization support. Eset is a good shortlist option for organizations seeking an effective, lightweight anti-malware solution.

Strengths

- The flagship enterprise product, Eset Endpoint Security, includes integrated anti-malware, anti-spam, HIPS, device control, Web content filtering and a personal firewall in a single-agent footprint. Installation can be tailored to specific needs by selecting only the modules that are desired.
- The low-performance impact of the Eset product has been noted by many customers.
- Its anti-malware engine is a consistently solid performer in test results. The engine has a strong reliance on heuristics and generic signatures, and includes client-based malicious URL filtering and sandbox heuristics, which run all executable files in a virtual emulator. The vendor recently introduced Eset Live Grid, a cloud-based lookup service.
- The vendor supports a broad range of Windows clients and servers, including Exchange, Lotus Notes/Domino, Linux, and Novell NetWare and Dell storage servers; mobile devices (Windows Mobile, Android); and Apple OS X and Linux desktop platforms.

Cautions

- The management interface is adequate, but it is still a Win32 application. Management is generally complicated by pop-up windows and a policy that requires multiple windows.
- Eset has a great point-in-time system inspector function, Eset SysInspector, but it cannot store historical asset information, nor does it provide any vulnerability or configuration information that would aid in security state assessments, forensic investigations or APT detection capabilities.
- A separate Web-based dashboard provides a flexible, customizable reporting interface, but it does not allow for direct drill-down into the management console for rapid remediation.
- ESET has not integrated competitive uninstall functionality into the product; however, ESET does offer uninstall tools on its Web properties that are free to its clients. It also provides a

paid professional service option.

- Eset doesn't yet offer application control.
- MDM functions are very basic.
- The Mac client does not have full functional parity with the Windows agent.
- Although Eset Endpoint Security operates in virtual environments and has a low system impact, it has not been optimized for virtual environments.

Return to Top

F-Secure

F-Secure, a veteran of the anti-malware industry for more than 20 years, has a very good track record for malware testing results. 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. F-Secure is a good choice for 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 look-ups 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 sandbox for malicious behavior.
- 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 recently released its Security for Virtual and Cloud Environments solution, which provides agent-based security that is optimized for virtual environments.
- The vendor offers one of the better rootkit detection and removal tools.
- F-Secure client agents are lightweight with minimal performance impact.
- It provides basic device control functionality.
- F-Secure has mobile clients for Android, BlackBerry, Symbian and Windows Mobile, as well as a cloud-based MDM capability that is primarily aimed at SMBs. It also offers protection for a broad range of Linux variants and Mac platforms.

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, and it is growing much slower than the overall market.
- 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 or application control.
- At the time of this writing, F-Secure Security for Virtual and Cloud Environments is very new and does not provide centralized ageless security.
- Although F-Secure develops its own signatures and behavioral detection techniques for advanced threats, its solution relies heavily on Bitdefender for the majority of anti-malware signatures. Business disruptions at Bitdefender could impact F-Secure customers.
- 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.
- MDM and Mac device protection are not integrated into the endpoint management console.
- Mac clients are not managed in the same console as Windows clients.
- F-Secure does not provide any protection for SharePoint servers (this was due in 1H13, but has been postponed).

Return to Top

IBM

IBM's EPP offering is built on the foundation of its strong client management tool platform, the Tivoli Endpoint Manager (TEM). IBM recently acquired Trusteer, which has some interesting application exploit protection technology. TEM for Core Protection is provided by Trend Micro, and advanced HIPS capability is provided by Proventia. These tools are augmented by IBM's X-Force research labs. Large organizations that are considering IBM for client management tools, or those looking at Trend Micro, should include IBM on their shortlists.

Strengths

- TEM provides a converged endpoint management and security operations console that supports large enterprise needs across multiple endpoint types, including mobile devices and Mac

devices, which received significant development attention in 2013.

- 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 McAfee, Symantec and Microsoft.
- IBM Endpoint Manager for Mobile Devices enables unified MDM of iOS, Android, Windows Phone, Windows Mobile and Symbian devices with the same management infrastructure. Services include inventory profile management, remote locate and wipe, and app deployment. IBM is rated as a Visionary in the "Magic Quadrant for Mobile Device Management Software."
- Add-on components include TEM for Data Protection, which provides port/device control and DLP. Application control is offered via 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.
- IBM server protection products boast very broad server support for Windows, Linux, HP-UX, Solaris and AIX, including 64-bit support for Windows and Linux, as well as new AIX 6.1 support.

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.
- IBM received low satisfaction scores from reference customers and channel partners.
- 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.
- TEM 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.
- IBM received low customer satisfaction scores from reference customers and channel partners contacted for this report.
- Although IBM has its X-Force and now Trusteer security analysis teams, it is dependent on Trend Micro for its broad signature database. Disruptions at 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.

Return to Top

Kaspersky Lab

Kaspersky Lab's global brand awareness is growing rapidly as it continues to broaden its offering with internally developed, "policy"-based protection features. Kaspersky Lab's Completeness of Vision score benefits from malware effectiveness, virtual server support, MDM, integrated application control and vulnerability analysis. It is a good candidate solution for most organizations.

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.
- The Microsoft Management Console (MMC) dashboards can be customized with predefined graphs and are task-oriented. The security status dashboard rolls up warnings of vulnerability, antivirus client status, infection information, network events and OS error reports.
- Kaspersky is building out an impressive array of integrated client management tools, including vulnerability analysis, patch management, application inventory, application control and MDM. These proactive tools help organizations reduce the attack surface.
- Kaspersky Mobile Security provides MDM capability and security agents for mobile clients. Advanced functionality includes Web threat protection, application control and jailbreak detection.
- Application control capabilities provide a fully categorized application database and trusted sources of change; they also offer client-level Web filtering for managing websites and Web applications.
- 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.

- Kaspersky Lab offers broad endpoint platform support, including an agentless VMware vShield solution with an intrusion prevention system/intrusion detection system using VMware Network Extensibility (NetX) technology — all managed by Kaspersky Security Center. (Citrix and Hyper-V is planned for release in 1H14.)

Cautions

- Kaspersky Lab's client management tool features (such as vulnerability and patch management) are still maturing and are not replacements for enterprise solutions. However, they are good for the enterprise security practitioner to validate operations, or to replace or augment SMB tools.
- The vendor has added numerous new capabilities to its MMC management console, making it 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.
- Some customers have commented that internally developed features need longer beta testing before general availability.
- The security state assessment capability would be improved with more predefined reports and dashboards to prioritize tasks and provide key performance metrics. Kaspersky now needs to expand its capabilities in malware detection and forensic investigations to reduce the dwell time (see Note 2) of APTs and improve incident response.
- Security products for Exchange and Forefront Threat Management Gateway have their separate management servers and are not integrated with other Kaspersky Lab products.

Return to Top

LANDesk

LANDesk is a pioneer in the integration of client management tools, MDM and security. In 2013, LANDesk added several native security features, but it is largely reliant on partner Kaspersky Lab for anti-malware. 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 LANDesk console is comprehensive and provides the ability to view IT operational dashboards, alongside security-related dashboards, in a browser or native iOS app.
- The LANDesk agent has a single, modular architecture so that security functionality (such as anti-malware) can be activated as needed. Policy is very object-oriented, and reuse is common.
- Automated provisioning and state management are particularly useful to easily reimage PCs in the case of pervasive malware.
- MDM capability has been a focus of recent development work, including the addition of geofencing and location-aware policies.
- 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 NAC capabilities. Customers can use LANDesk to manage McAfee, 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 Antivirus can also manage the Windows firewall. In 2013, the solution was extended to Mac clients.
- The LANDesk Security Suite includes an integrated full-drive encryption option, licensed from Dell (formerly Credant Technologies), and it can also centrally manage Microsoft BitLocker through the LANDesk console.
- LANDesk Configuration Manager provides extensive port and device control, including encryption capabilities for removable media.
- Pricing for the LANDesk 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. Its focus on the security operator's information requirement and workflow remains underdeveloped. Customer feedback indicates that the LANDesk console dashboard and reporting are designed from an operations perspective, as opposed to having a security-oriented focus. Security state assessment, forensic investigation and APT detection capabilities are incomplete.
- LANDesk doesn't perform its own malware research; instead, it relies on Kaspersky Labs. Business disruptions between Kaspersky and LANDesk could have an impact on customers.
- Not all LANDesk Security Suite features are available on all managed platforms. There's no malware support for Unix, 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.
- 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.

Return to Top

Lumension Security

The Lumension Endpoint Management and Security Suite (LEMSS) 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 the vendor to their shortlists.

Strengths

- 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.
- The anti-malware engine is licensed from Norman, and includes a sandbox capability that intercepts and prevents changes to host files and registry settings, as well as other malicious changes.
- Application control capabilities benefit from a cloud-based file reputation service and a recently added memory protection capability.
- Lumension Device Control is a complete solution for managing and restricting USB and other ports.
- Lumension resells Sophos SafeGuard Easy for full-disk encryption.
- LEMSS provides a generic framework for the management of third-party security agents, such as Windows firewalls.
- Lumension received high Net Promoter scores from reference customers that were contacted for this Magic Quadrant.

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 anti-malware partner Norman to review suspicious code samples and prepare custom signatures. Disruptions to this relationship could have consequences for Lumension's customers. Norman's performance in key anti-malware test results is average.
- 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.
- The vendor does not yet offer MDM capability, although a natively developed solution is due in 1Q14.

Return to Top

McAfee

McAfee, a wholly owned subsidiary of Intel, holds the second-largest EPP market share worldwide, and offers a broad portfolio of information security solutions. Its acquisition by Intel in 2011 appears to be working well, and, as a result, McAfee has expanded its R&D efforts and extended its security product road maps for several years. McAfee's ePolicy Orchestrator (ePO) policy management and reporting framework provides a platform for addressing several aspects of the security life cycle. The vendor should be considered by any large, global enterprise that is seeking solid management and reporting capabilities across a number of disparate security controls.

Strengths

- McAfee's ePO management platform provides consistent management, deployment, reporting, workflow and alerting for McAfee's security products portfolio. The latest version, v5.1, includes "real time" query functionality that allows administrators to find detailed client state information very rapidly, aiding in forensic investigation. McAfee ePO 5 also introduced a streamlined interface to reduce complex tasks. It is also an open platform, with integration to over 120 third-party applications.
- McAfee Complete Endpoint Protection — Enterprise Suite provides a broad array of EPP tools that include integrated firewall, device control, URL block list, Deep Defender anti-rootkit, application control, HIPS capabilities, MDM, Risk Advisor, and antivirus for Windows, Linux,

Unix, Mac and email servers, all manageable within ePO.

- McAfee Application Control is a full-featured, market-leading solution for PCs and servers that fully support trusted sources of change. McAfee Risk Advisor provides good security risk analytics, identifying devices with vulnerabilities that need additional countermeasures or patching. These tools are valuable in satisfying proactive policy-based controls to reduce the attack surface.
- McAfee's optional Enterprise Security Manager (security information and event management [SIEM]) will increasingly provide better malware detection capability as it becomes more integrated.
- The acquisition of ValidEdge (malware execution sandbox) provides customers with a sandbox execution environment that can analyze suspect files from endpoints.
- McAfee's Management for Optimized Virtual Environments (MOVE) has offered optimized anti-malware scanning in virtualized environments for two years, and now MOVE 2.5 offers agentless anti-malware scanning in VMware environments using native vShield API integration.

Cautions

- ePO is powerful, but at the cost of complexity. Smaller organizations will likely find it to be too complex for their resources and requirements. As an alternative to ePO, McAfee has provided a SaaS-based management console targeted at SMBs.
- Although McAfee has integrated the management experiences, agents have not been consolidated. This creates "footprint bloat" and agent management issues. Moreover, multiple agents are less efficient and effective than a consolidated agent, which enables context passing between the different anti-malware systems.
- McAfee has the most security life cycle tools of any vendor in this analysis; however, the tools are not yet highly integrated into a consistent workflow and reporting structure. For example, there is no single metric that would allow administrators to track progress in policy-based controls.
- 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. Discovery capabilities to detect indicators of compromise are also absent. For example, there are no dwell time indicators or change control monitoring, although these features are supported by McAfee's SIEM tool.
- McAfee Host Intrusion Prevention for Desktops is not widely deployed on desktops due to technical and administrative resource requirements; it is more applicable to servers, where it overlaps significantly with McAfee's Application Control technology.

Return to Top

Microsoft

Microsoft's System Center 2012 Endpoint Protection (SCEP, formerly Forefront) is intimately integrated into the popular System Center management console, and Microsoft licensing often includes SCEP, thereby making it an attractive shortlist candidate. We view SCEP as a reasonable solution for Windows-centric organizations licensed under Core Client Access License (CAL) that have already deployed Microsoft System Center Configuration Manager, and that have additional mitigating security controls in place.

Strengths

- Microsoft has made gradual improvements in malware effectiveness testing as a result of its investment in better lab processes and proactive detection methods (such as Internet Explorer exploit protection, system monitors, hidden system drivers, anti-emulation detection, JavaScript emulators, generic signatures and vulnerability-shielding capabilities). 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 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.
- Organizations that are licensed under Microsoft's Enterprise CAL or Core CAL program 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.

Cautions

- Consideration of Microsoft is primarily due to attractive pricing in its enterprise agreements. Approximately one-third of enterprise buyers[1] have indicated that they are actively considering Microsoft, or plan to do so during their next renewal periods.
- Microsoft could be disruptive if it were to adopt an application control approach to the market, similar to the Apple iOS and Windows RT operating systems, for the traditional Windows

desktop; however, delivering this type of a solution within the next two years would require a major effort by Microsoft.

- Test results of the effectiveness of SCEP are low. Microsoft's approach to and priority of client anti-malware protection is focused on reducing the impact of prevalent malware in the Windows installed base with very low false-positive rates; therefore, the approach does not generally focus exclusively on rare or targeted threats whose impact is minimal to the entire Microsoft ecosystem.
- 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. System Center Configuration Manager is too heavy for users of Microsoft Windows Small Business Server Essentials.
- 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 clients use Windows user/administrator rights management for tamper protection. Users and applications with administrator rights can disable the client.
- SCEP still lacks numerous capabilities that are common in other security solutions, including advanced device control, integrated full-disk encryption, DLP and application control. Windows features such as Firewall, BitLocker, AppLocker and Group Policy Objects 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.
- SCEP provides support for virtual environments by enabling the randomization of signature updates and scans, and by offline scanning. It does not integrate with vShield or provide agentless solutions.
- Microsoft does not offer integrated MDM capability or antivirus for SharePoint and other specialized application platforms (except Exchange). Mac and Linux servers are supported with clients licensed from Eset, but they do not report to the administration console.

Return to Top

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. However, at the time of this writing, these features have only recently launched, and have not been widely field-tested.

Panda is also the first EPP vendor to fully embrace cloud delivery of security 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 region and North America).

Strengths

- The Windows-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.
- Malware detection includes several proactive HIPS techniques. Panda's HIPS capability includes policy-based rules, vulnerability shielding 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 look-up to catch the latest threats.
- Panda recently added a remote endpoint system management solution, which includes audit, configuration, patch and software distribution capabilities, as well as remote control.
- Panda also recently launched an advanced threat protection service that monitors and classifies all executables running on endpoints (PCs and servers).
- Panda pricing is very competitive, and there are no upfront license costs — only an annual subscription.

Cautions

- The vendor is slowly expanding from its EMEA presence, radiating outward from its Spain headquarters. However, more than 70% of its business remains in Europe, and mind share is still weak in other geographies.
- Numerous changes to Panda Cloud Systems Management are promising, but still not widely

field-tested. In general, it is still evolving from an asset inventory and remediation tool to provide better security state assessments, vulnerability detection, and forensic investigation capabilities. Also, it only provides 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.
- Panda still lacks advanced firewall features, such as location-based policies, wireless-specific firewall options and VPN integration options.
- 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.

Return to Top

Sophos

Sophos is one of a few companies in this Magic Quadrant that sells exclusively to enterprise markets. It is currently branching out into the network security market, with a longer-term goal to provide a consolidated network and endpoint security solution that is differentiated by ease of use and out-of-the-box integration, and is primarily aimed at the SMB market. We de-emphasized data protection in this year's analysis, which had a detrimental effect of Sophos' Completeness of Vision score. However, Sophos, remains a good fit for buyers that value simplified administration with solid support, and do not require complex policies.

Strengths

- Sophos' management interface is, by design, very easy to use and highly capable out of the box, without excessive fine-tuning. It provides consolidated management of endpoint protection and encryption for Windows, Mac and Linux, as well as mobile device protection. Sophos also recently launched a cloud-based management console, and has an aggressive road map on cloud management (and will eventually have one for cloud-based security services).
- Sophos also provides a vulnerability monitoring solution to reduce the attack surface of PCs.
- Sophos has added Sophos Antivirus for vShield to provide agentless antivirus for VMware environments. This is included as standard in Sophos Server Protection, as well as in select endpoint protection suite licenses.
- Sophos made several significant releases of Sophos Mobile Control, the MDM solution. It is rated a Niche Player in the "Magic Quadrant for Mobile Device Management Software."
- 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 an additional charge.
- Sophos offers user-based pricing, rather than device-based prices.

Cautions

- Sophos suffers from a weak marketing presence, particularly in North America, which is compounded by the lack of a consumer market Presence, outside of a free MAC product. .
- The simplicity of Sophos' management console becomes a liability in larger enterprises that need more granular control and reporting. In particular, reference customers wanted flexibility in deploying new engines. The security state assessment capabilities are buried and should be moved to the main dashboard.
- 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. However, it can be used to block specific applications or application classes that may be undesirable.
- Sophos' acquisition of unified threat management gateway vendor Astaro may create new opportunities to compete with companies in the UTM market, but it does not improve Sophos' competitive standing in EPP market yet.

Return to Top

Symantec

In January 2013, Symantec announced a new strategy to reinvigorate company growth by better utilizing its many technologies in a more consolidated and holistic manner. Its endpoint protection and management offerings are now in the User Productivity & Protection group, with a charter to create a more seamless endpoint security suite across multiple devices for consumers and businesses — and between consumers and businesses. Symantec remains the market share leader in EPP, and is a good 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], File Insight and its Network Protect technologies) that are beyond traditional signatures for protection from advanced targeted attacks.
- Symantec was one of the first vendors to develop Insight, a community-based cloud file reputation service. It exposes this for policy formation in the SEP 12 client.
- For optimization of scanning in virtualized environments, SEP 12 can share its Insight cache across instances, and has the ability to use a dedicated VM for this purpose.
- Symantec's large enterprise and consumer installed base gives it an advantage for detecting advanced threats by analyzing data across a larger and more diverse population. Furthermore, going forward, this agent presence can be leveraged for greater visibility for security monitoring as a sensor.
- Symantec is redesigning its endpoint agent to a unified platform with a plug-in architecture and software-key-based modular licensing that can be customized based on customer requirements.
- For server-based HIPS, Symantec Critical System Protection has broad platform support, compared with competitors.
- Symantec has solid MDM capabilities from its acquisitions of Odyssey Software and Nukona (which provides app isolation). Symantec is rated a Visionary in the "Magic Quadrant for Mobile Device Management Software."
- Symantec Power Eraser is a good tool for scrubbing hard-to-remove infections, and provides a free alternative to Malwarebytes.

Cautions

- The recent reorganization was designed to assimilate disparate development teams with a long-term road map of better integration across the Symantec endpoint portfolio. However, the road map is long. SEP 12 remains weak in proactive security state assessments as well as forensic and discovery capabilities, and addressing these weaknesses is 12 to 24 months away.
- The Insight file reputation technology only works on file downloads and is not a full application control solution.
- Symantec does not yet offer an "agentless" version for optimizing anti-malware scanning in virtualized environments (although its shared Insight cache feature can be used to improve performance).
- Symantec lacks a network-based sandbox product that can analyze suspect code and report on its behavior, while close competitors already have these products in beta or general availability.
- Symantec's server protection offerings center around Critical System Protection and its Control Compliance Suite, but they use a different management console and reporting framework, and are managed out of a different group within the new Symantec organizational structure.
- Although Symantec has mobile security capabilities, they are not yet integrated into the Symantec management console framework.
- Removable device encryption requires a confusing set of policies across Symantec's encryption products and SEP 12's device control functionality.

Return to Top

ThreatTrack Security

ThreatTrack Security was spun out of GFI Software and is now a private company that continues to sell the Vipre-branded EPP solution. Vipre was 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.
- One useful utility is a Web-hosted malware analysis engine that provides immediate forensic feedback on submitted application files.
- Signature-based anti-malware scanning is augmented with virtualization sandboxing technology, which analyzes malware in real time within a partitioned environment on the PC.

Cautions

- ThreatTrack is one of the smallest vendors in this analysis, and has a very low mind share and

market share in the enterprise market. The majority of its customers are SMBs.

- 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.
- 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.
- 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.

Return to Top

Trend Micro

Trend Micro is the third-largest enterprise endpoint protection vendor, with a large worldwide installed base focused on the Asia/Pacific region and EMEA. Trend Micro offers two primary endpoint protection offerings: OfficeScan and Worry-Free Business Security for desktops and laptops, and Deep Security for servers. An overlay console architecture called Control Manager can pull information from both offerings to provide an overall dashboard, as well as policy management across endpoint and messaging security. Control Manager is the new focal point for the integration of Trend Micro capabilities, such as MDM. Trend Micro is a good shortlist candidate for buyers looking primarily for anti-malware capability.

Strengths

- 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 AWS. Capabilities include encrypting these workloads with its SecureCloud offering and an optional SaaS version of its Deep Security management console.
- Trend Micro offers broad platform support on servers, compared with competitors.
- OfficeScan protection is augmented by malicious URL filtering, critical resource and process protection, vulnerability shielding, and behavioral monitoring.
- For improved host-based firewall protection in OfficeScan, Trend Micro offers the deep-packet-inspection-capable firewall from Deep Security as a plug-in to OfficeScan, called Intrusion Defense Firewall (IDF).
- Trend Micro has released a competitive network-based appliance offering to FireEye for malware detonation called Deep Discovery, which is integrated into Trend Micro's overall set of protection solutions for email, Web and endpoint. Trend Micro has a strong vision to share security intelligence across its products for a coordinated and adaptive response to threats — for example, automatically quarantining a system that appears to be infected with a zero-day threat that was discovered by Deep Discovery and confirmed by the endpoint agent.
- Trend Micro recently added mobile security policy management capabilities to Control Manager for Android, iOS, Windows Phone, Symbian and BlackBerry.

Cautions

- Historically, Trend Micro has been very conservative and timid with new EPP capabilities, such as encryption and application control. More recently, however, it has shown signs of leadership with Deep Discovery and Deep Security.
- The core endpoint offerings — OfficeScan and Deep Security — are two separate products from separate teams with separate consoles. Deep Security has not been integrated into TMCM for deployment and policy management, but it has been integrated from a security reporting perspective. Initial Deep Security integration with TMCM shipped in December 2013 (a widget to drill into Deep Security Manager). Additional substantial functionality is scheduled to ship in 2Q14.
- Some capabilities (like encryption) that have been integrated into TMCM still require their native consoles to be deployed, but from that point forward, they can be managed within TMCM.
- 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.
- Trend Micro has limited release of Application Control in the German market. It is scheduled for release on a global basis in 1Q14.
- Trend Micro's installed base and market share in North America and EMEA are not as strong as in Asia/Pacific.
- 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 assessments.

Return to Top

Webroot

Webroot SecureAnywhere Business Endpoint Protection takes a behavior-based approach that uses cloud databases to keep its EPP client small and fast. 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 look-up results in a very small and fast EPP client. It also allows Webroot to mine aggregate behavior information from endpoints for new threats, and enables an entirely pull-based mechanism for detection and updates.
- Webroot SecureAnywhere provides a remote management tool, built-in application process monitoring, a change log and rollback functionality to ease remediation. It is the only vendor in this analysis to provide information in the logs showing the time stamp of a file versus its discovery. 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.
- 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 for Android and iOS devices from within the same management console. The Webroot management console is cloud-based and does not require a local server.
- Webroot received the highest Net Promoter scores from reference customers that were contacted for this Magic Quadrant.

Cautions

- The management console and features are aimed primarily at the needs of professional and SMB buyers.
- 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 provides neither port/device control, application control nor 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.
- Despite being the only vendor with log data that shows malware dwell time, there is no separate alert for the discovery of longer dwell time malware.
- Webroot does not protect the workload of specialized servers, such as Exchange and SharePoint. There is no specific optimization for virtualization, but the lightweight engine and cloud-assisted design help.
- MDM is currently a separate management console.

Return to Top

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.

Return to Top

Added

Bitdefender was added to this analysis due to its growing presence in the SMB market. ThreatTrack Security is a spun-out business unit of GFI Software.

Return to Top

Dropped

GFI Software spun out its Vipre Security business unit, which is now called ThreatTrack Security.

Return to Top

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

Return to Top

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 based on overall vendor satisfaction scores cumulated 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 (January 2014)

Return to Top

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 to 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 (January 2014)

Return to Top

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.

Return to Top

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.

Return to Top

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.

Return to Top

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.

Return to Top

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.

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.

In theory, any security solution can be bypassed. Buyers should look for good repair tools, as well as the capability to alert administrators about threats that may have had a longer dwell time (see Note 2) or more virulent infections. Forensic 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, as well as what other systems have handled the malicious content.

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.

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 coordinate 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.

Return to Top

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 35% 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 in 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.

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 is 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, McAfee 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 82%. While still dominant, the combined market share of the Leaders is down 3% 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 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.

▲ **Return to Top**