Magic Quadrant for Endpoint Protection Platforms

01 February 2016 | ID:G00273851

Analyst(s): Peter Firstbrook, Eric Ouellet

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.

Strategic Planning Assumption

By 2018, 60% of EPPs will restrict executables that have not been preinspected for security and privacy risks, up from 22% today.

Market Definition/Description

This document was revised on 25 February 2016. The document you are viewing is the corrected version. For more information, see the Corrections (http://www.gartner.com/technology/about/policies/current_corrections.jsp) page on gartner.com.

The enterprise endpoint protection platform (EPP) is an integrated solution that has the following capabilities:

- Anti-malware
- Personal firewall
- Port and device control

EPP solutions will also often include:

- Vulnerability assessment
- Application control (see Note 1) and application sandboxing
- Enterprise mobility management (EMM), typically in a parallel nonintegrated product
- Memory protection
- Behavioral monitoring of application code
- 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)

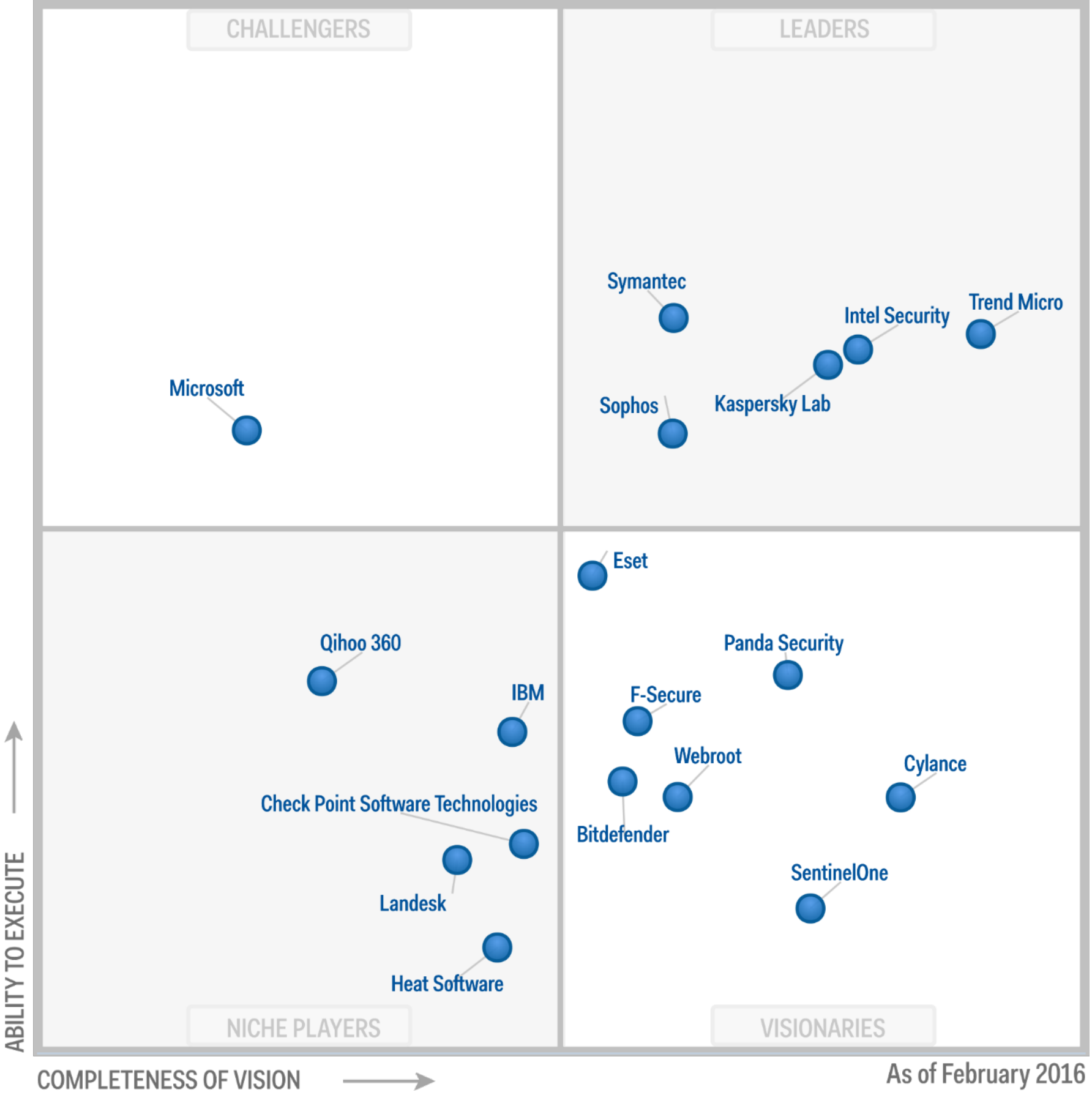
These products and features are typically centrally managed and ideally integrated by shared policies. Not all products in this analysis provide the same collection of features. Here, we focus primarily on anti-malware effectiveness and performance, management capability, protection for Windows and non-Windows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

DLP, EMM and vulnerability assessment are also evaluated in their own Magic Quadrant 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. 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 EPP 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, EMM is largely a separate purchase for more demanding large enterprise buyers; however, small and midsize businesses (SMBs) are likely to be satisfied with EPP vendor's EMM capabilities.

The total EPP revenue of the Magic Quadrant participants at year-end 2014 was slightly under than $3.2 billion, up 2% over the previous year. 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 2016.

Magic Quadrant

Figure 1. Magic Quadrant for Endpoint Protection Platforms



Source: Gartner (February 2016)

Vendor Strengths and Cautions

Bitdefender

Bitdefender still generates the majority of its revenue from consumer sales, but the gap between consumer sales and enterprise sales narrowed in 2015. The company is investing heavily into its sales operations in Europe and the U.S. Updates to the enterprise offering included improvements in security event feeds from endpoints to the management console, formulating better insights into the presence of malware, unwanted applications, advanced threats and remediation. Bitdefender is a consistently solid performer in anti-malware test results, and noted by clients for ease of use and customer support. Increased evaluation

weight on malware effectiveness and company focus nudged Bitdefender into the Visionary quadrant this year. 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, too, with low overhead.

Enhancements to the GravityZone management interface provide enterprise clients with better insights into the state of malware, applications and advanced threats for physical, virtual and mobile endpoints.

Good support is provided for public and private hybrid cloud-based management of endpoints, virtualized endpoints, AWS security as a service and Exchange.

Device control and Exchange security module have been added to the Management Console, and improvements to the remediation process can be triggered via a single-click action.

The company received high marks from reference customers for support and service.

The company provides OEM solutions to many vendors included in this analysis.

CAUTIONS

Bitdefender is aggressively investing in growing its sales operations in the U.S. and EMEA; however, significant work remains for it to become a well-known name and to get mind share outside of its core SMB market.

Bitdefender does not offer full-feature parity between Windows, OS X and Linux. The Windows offering supports anti-malware, firewall, content control and device control. OS X and Linux have only anti-malware capabilities.

List price is at the upper end of the average pricing for this market.

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, continues to suffer from poor marketing and channel execution. However, it will still appeal to organizations that value strong integration among endpoint threat prevention and forensics with network-based detection.

STRENGTHS

Endpoint's URL filtering capability enables an off-LAN URL filtering security policy synchronized with a firewall blade policy.

Antivirus Software Blade centrally captures data from activity sensors and initiates algorithm-based analysis when triggers are tripped from within protection mechanisms. Relevant data is presented providing a complete picture of events under investigation.

Check Point's endpoint management console can be customized for each administrator with user-specific policy views across multiple devices.

The Endpoint Security Best Practice Report provides the main configuration/vulnerability issues, including vulnerable applications, misconfigurations, missing windows service packs and potentially unwanted applications.

CAUTIONS

Again this year, Check Point did not disclose sufficient detail for Gartner to adequately evaluate its progress in this market; however, based on Gartner client inquiry levels about Check Point's EPP solutions, it has again failed to significantly improve its market share or mind share in the EPP market beyond the acquired installed base of customers.

While Check Point has invested over the past year in its own malware research lab, it continues to depend on Kaspersky Lab's engine and signature updates for this offering.

Check Point's application control capabilities (which it calls "program control") remain largely unchanged for this year. Application control capabilities continue to rely on URL filtering, anti-bot and anti-malware for restricting unapproved and suspicious applications.

Check Point EPP protection is oriented toward 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, Microsoft SharePoint or Lotus Notes. It does not offer feature parity for OS X or Linux.

Although its agent will run in virtual machines (VMs), Check Point has no specific optimization for virtualized environments.

Cloud management is focused on Check Point Capsule and Mobile Threat Prevention products only, and does not include the management of endpoint offerings.

Cylance

Cylance is a fast-growing startup that provides an innovative new approach that replaces traditional signature database approaches found in traditional antivirus products. The company uses a machine-learning algorithm to inspect millions of file attributes to determine the probability that a particular file is malicious. The algorithmic approach significantly reduces the endpoint and network resource requirement. Because of its signatureless approach, it is capable of detecting both new threats and new variants of known threats that typically are missed by signature-based techniques. Cylance's approach is also disruptive, because the company does not require legions of signature authors to analyze new threats and codify them in signature updates. Cylance will appeal to organizations looking for improved zero-day malware protection, those looking for low-impact protection for resource-constrained platforms, and systems that are disconnected and cannot rely on regular signature updates.

STRENGTHS

The Cylance machine-learning algorithm has been demonstrated to be very accurate at detecting new variants and repacked versions of existing malware. Cylance also offers memory injection protection for a number of the most common classes of vulnerabilities, alternative protection techniques (such as script control) and lockdown.

Because the endpoint agent does not require a database of signatures or daily updates, it is extremely lightweight on the network and has a minimal performance impact on endpoints. It can remain effective even when disconnected for long periods.

The management console is cloud-based, making it very easy to deploy. However, Cylance does not rely on cloud-based detection, which means protection does not require exfiltration of potentially sensitive files or data to the cloud.

Cylance provides file assessment information showing static details on files and global assessment information, including what other customers do with detected files (that is, the percentage of other customers that quarantine suspect files).

Protection is available for Windows and Mac devices. Linux support is due in 2Q16.

Cylance is easily the fastest-growing EPP startup in the last ten years and is gaining traction as an OEM provider for other security solutions, such as Dell's Endpoint Security Suite Enterprise and Blue Coat.

CAUTIONS

The Cylance solution provides only anti-malware capabilities. Extended EPP functionality — such as personal firewalls, URL filtering, port protection, data protection, mobile device protection, enterprise mobility management, vulnerability analysis, endpoint detection and response (EDR), and application control — will have to be sourced and managed separately, if required.

Cylance is a rapidly growing startup and is likely to suffer from at least some growing pains. Existing customers are mostly in North America, but Cylance is expanding to the EU and Asia/Pacific (APAC).

Malware authors develop evasions for more popular anti-malware approaches. As Cylance gains in adoption and market share, its approach will come under more scrutiny from attackers.

The Cylance algorithm can cause false positives on less-well-known files that have attributes similar to malware files, especially consumer files. However, evidence reports on convicted files, which include community ratings and severity scores, should provide sufficient info for admins to whitelist most false positives. Cylance is planning on improving forensic data in 2Q16.

Support for Microsoft Exchange and other specialized servers is lacking.

The management console is cloud-based, which may not be a desired deployment option for some buyers. Reference customers noted the absence of regular expressions for memory defense exclusions, and the need for improved search functions and agent tamper resistance.

Current Linux protection is only sold as an OEM solution.

Eset

Eset has built a substantial installed base in EMEA, and it has a rapidly growing 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. Increased evaluation weight on malware effectiveness and company focus nudged Eset into the Visionary quadrant this year. Eset is a good shortlist option for organizations seeking an effective, lightweight anti-malware solution.

STRENGTHS

Eset's anti-malware engine is a consistently solid performer in test results. The engine benefits from virtual sandbox that simulates executable files before execution in a virtual emulator, a memory scanner that monitors process behavior and a vulnerability shield for widely exploited software.

Eset offers broad coverage of capabilities for endpoint security (Windows, OS X), antivirus (Linux, Windows, OS X, Android), server security (Windows, Linux/BSD/Solaris), mail server security (Microsoft Exchange, Lotus Domino, Linux/BSD/Solaris, Kerio) and VMware vShield.

Device control offers OS X support via Endpoint Security and Endpoint Antivirus for OS X from 6.1.

Cloud-augmented malware protection system for advanced threat defense automatically processes suspicious objects and potential threats harvested via the Eset Live Grid network.

Network-traffic-based signatures extend network attack protection (Vulnerability Shield) and botnet protection analysis of malware network protocol changes via routine signature updates instead of code updates.

CAUTIONS

Eset was late to market with industry-leading functions, such as Web-based management consoles, EMM and virtualization support. It still does not offer application control or vulnerability scanning.

Vulnerability Shield does not report on Common Vulnerabilities and Exposures (CVEs) covered.

Eset SysInspector now supports the automatic triggering of snapshots when events occur; these can be viewed using Eset Remote Administrator. However, the dashboards still do not provide any vulnerability or configuration information that would aid in security state assessments.

Eset does not yet offer a cloud-based management console, despite its focus on SMB customers. Eset Remote Administrator 6 is currently being evaluated as a Microsoft Azure Certified virtual machine.

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, EMM and virtualization protection. Increased evaluation weight on malware effectiveness and company focus nudged F-Secure into the Visionary quadrant this year. Its Ability to Execute 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 as the most import decision factor in their EPP decision.

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. The sandbox environment tests unknown applications in a virtual sandbox for malicious behavior. Safe 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.

The F-Secure Security for Virtual and Cloud Environments solution is a hypervisor-agnostic, agent-based security solution that operates as a separate VM.

On-premises and cloud-based management portals have new user interfaces, with enhanced focus on security administrator management functions, and streamlined day-to-day activities.

F-Secure's advanced threat protection solution leverages sensor technology on endpoints and networks to detect attacks, and leverages F-Secure specialists for review, forensic analysis and response.

Freedome for Business supports Android and iOS devices, and includes mobile device management that includes anti-theft, management, monitoring and reporting, VPN, browsing protection, and cloud-based antivirus (AV).

CAUTIONS

In 2015, there continued to be very little awareness or brand recognition of F-Secure outside Northern Europe, despite having had an offering in the EPP market for many years, and adding sales presence in selected areas of Europe, China and the U.S.

The updates to the management interface in 2015 provide for a better experience, but still need to be improved to facilitate the integration of additional relevant data points in context to streamline the analysis process.

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 still does not natively support VMware NSX or vShield APIs.

OS X, iOS and Android are only managed via the cloud-based Protection Service for Business, and cannot be managed via the on-premises-based console that manages the rest of the suite.

Although F-Secure develops its own signatures and behavioral detection techniques for advanced threats, its solution continues to rely on Bitdefender as a reference engine of anti-malware signatures. Business disruptions at Bitdefender could impact F-Secure customers.

F-Secure's solutions do not have full-feature parity between the Windows platform and OS X or Linux.

Heat Software

Heat Software was derived from the acquisition of FrontRange by Clearlake Capital Group and its subsequent merger with Lumension. The Heat Endpoint Management and Security Suite (Heat EMSS) provides for the integration of client management tools, EMM and security. Current Heat Software customers, or those seeking integrated solutions for security, operations and compliance, should add this vendor to their shortlists.

STRENGTHS

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.

Heat replaced its Norman anti-malware engine with the more accurate Bitdefender engine.

Heat EMSS provides a generic framework for the management of third-party security agents, such as Windows firewalls.

Heat Endpoint Integrity Service (EIS) provides risk scoring of new applications. Local authorization lets end users make ad hoc changes with accountability by tracking changes and giving administrators the ability to reverse when required.

Heat Software Device Control is a very granular solution for managing and restricting USB and other ports, and provides shadow copy capability.

CAUTIONS

Heat Software drifted back into the Niche quadrant this year, as buying focus has shifted to malware detection capability, and as a result of its limited brand awareness in the EPP market outside of its patch management installed base. While it is growing, its EPP market share remains very low.

Heat Software has no anti-malware labs of its own; rather, it relies on a partnership with Bitdefender to provide this capability. Heat also leverages a disk encryption component from Sophos. Disruptions to these relationships could have consequences for Heat

Software customers.

Heat Software does not currently plan to offer Application Control, Device Control or AntiVirus to other platforms beyond Windows .

Despite the wealth of information in the Heat Software EMSS solution, security state assessment and support for forensic investigation are weak.

Heat Software does not provide a personal firewall, but instead relies on native OS firewalls, which don't provide as many policy options as dedicated solutions. Heat Software provides prebuilt wizards to configure and manage the Windows Firewall.

Heat Software does not provide antivirus for specialized servers (for example, Microsoft Exchange and Microsoft SharePoint). Although its agent will run in VMs, Heat Software has no specific optimization for anti-malware protection in virtualized environments.

IBM

IBM's EPP offering is built on the foundation of its client management tool platform, the IBM BigFix, previously called IBM Endpoint Manager (IEM). IBM Security Trusteer Apex provides application exploit protection technology and complements the repackaged 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

The complete set of solutions from IBM, both native and repackaged, represent a significant capability set that will be welcomed by large, complex organizations. BigFix provides a converged endpoint management and security operations console that supports multiple endpoint types, including mobile devices, Linux and Mac devices, and virtual environments. IBM BigFix 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.

Trusteer Apex integration into the BigFix console provides visibility, configuration and management of the Apex agent.

Trusteer Apex application fingerprinting identifies known good versus unknown, but does not identify applications performing risky tasks. Java environments are offered a lockdown mode for the execution of nonwhitelisted Java code.

IBM BigFix 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.

The security and compliance analytics Web interface can establish and monitor built-in and administrator-created key performance metrics, and show compliance over time.

CAUTIONS

IBM drifted back into the Niche quadrant this year. It is not showing leadership on pushing the state of the art in this market. As a result, although IBM is continuing to gain some market share, it is disproportionate to the potential advantages of its brand and channel. IBM is rarely seen in final competitive bids outside of where they have an existing, strong client relationship.

BigFix does not offer 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.

The Proventia Host-Based Intrusion Prevention Systems (HIPS) and Virtual Server Protection products went end-of-market in April 2014. They are being supported until April 2016, but are no longer available for new customers.

BigFix Protection does not provide antivirus protection for Microsoft Exchange, Microsoft SharePoint, Lotus Notes and other specialized servers.

Although IBM has its X-Force and Trusteer security analysis teams, it is dependent on Trend Micro for its broad signature database, personal firewall and behavioral monitoring solution, with cloud-based file and Web reputation analysis. Disruptions affecting this critical partner could have an impact on IBM's customers. Integration of the latest Trend Micro engine into the Tivoli Endpoint Manager (TEM) client can take 30 days.

IBM does not currently have an EDR offering and is still considering options. These include the possibility of an integration of Trusteer Apex with other IBM solutions; or incorporating QRadar and BigFix; or creating partnerships like the one between IBM Security (QRadar) and Palo Alto Networks (WildFire).

Intel Security

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, Endpoint Security ENS (v 10.1). Intel Security's ePolicy Orchestrator (ePO) policy management and reporting framework provides a platform for addressing several aspects of the security life cycle. It continues to be the leading feature that brings and keeps clients with Intel Security. 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, including firewall, Web controls, malware protection and HIPS, that share event data and have the ability to communicate in real time to take action against potential threats.

ePO provides a common administrative platform for all of Intel Security's offerings and integrates with over 130 third-party applications. The cloud-based ePO now offers organizations the benefits of ePO with significantly faster deployments and less complexity.

Mature Application Control supports trusted sources of change, and integration with Intel Security's Global Threat Intelligence (GTI) and Threat Intelligence Exchange (TIE) provides file reputation services.

Intel Security, through enterprise system management (ESM), provides countermeasure-aware analytics capabilities from which organizations can prioritize assets to be patched, by most vulnerable and least protected.

Intel Security has the optional TIE and Data Exchange Layer (DXL) to exchange local object reputation information across both network and endpoint products. TIE is also part of the new common endpoint framework.

Intel Security's Advanced Threat Defense (ATD) provides a centralized network-based sandbox for malware inspection. Intel v. 10.1 clients can send samples to ATD for inspection via the TIE module.

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.

CAUTIONS

The most common customer complaints continue to be the effectiveness of the older multiple agent architecture and its impact on deployment complexity and performance. The new version 10 agent should improve the situation as roadmap items become available, but currently t it does not support all functions (such as whitelisting). Additional agents will still be necessary to get full functionality.

The Intel Security integration framework — despite its broad set of security tools beyond Threat Prevention, Firewall and Web Control and TIE — continues its slow evolution, with policy and context layer integration still missing among core components.

ePO Real Time products are being wound down in favor of McAfee Active Response, an endpoint detection and response capability. McAfee Active Response is still relatively new and does not address all EDR critical capabilities.

Some Intel Security solutions require the advanced capabilities embedded in Intel-based chipsets. For example, Deep Defender is dependent on the presence of Intel Virtualization Technology (VT), and Deep Command is dependent on Intel vPro.

Organizations must upgrade to the latest versions of Intel Security ePO and endpoint agent to take advantage of detection performance and administration improvements.

Kaspersky Lab

Kaspersky Lab's global market share continues to grow rapidly, along with its brand recognition. Gartner's Kaspersky-related inquiries show an increase over previous years. 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, EMM, 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 of system changes made by malware.

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 Network Extensibility (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 provides a broad range of functionality across Windows, Linux, OS X, iOS, Android and virtual platforms, including VMware, Hyper-V and Citrix, which will appeal to organizations wishing to consolidate vendor capabilities into one offering.

Automatic Exploit Prevention (AEP) targets malware that leverages software vulnerabilities by reducing the chain of vulnerability exploits, especially in well-known targets, such as Java, Flash, Adobe Reader, browsers and office applications.

Zero-day, Exploit and Targeted Attack (ZETA) Shield scans data streams for code fragments resembling exploits in legitimate files, such as executable code in office documents or call commands typically not used by the file type.

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.

While Kaspersky has begun the development of a new console slated for the Kaspersky Endpoint Security for Business 10 SP2, due in mid-2016, the existing Microsoft Management Console (MMC) will continue to be used in many client environments for some time to come. Small deployments can use the cloud-based console associated with Kaspersky Small Office Security 4.

Kaspersky does not currently offer EDR or malware sandboxing capability, but is piloting the new Kaspersky Anti-Targeted Attack (KATA) platform, an anti-advanced persistent threat (APT)/EDR with sandboxing capabilities, at select clients.

Landesk

Landesk provides system, security, service, asset and process management. While it has developed its own security solutions, including firewall, vulnerability, patch and application control solutions, it also repackages leading offerings from Lavasoft and Kaspersky Lab. Landesk appeals to clients that have a blend of technology solutions from different vendors and wish to bring them under common management, with the flexibility of assigning different administrative personnel to control them. 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. Landesk Patch Manager includes vulnerability assessment, operating system patching, third-party patching, distributed and remote system patching for Windows, OS X, Red Hat Linux, SUSE Linux, and HP Unix, along with automated and advanced distribution modes.

STRENGTHS

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 Manager, which leverages an integrated Kaspersky Lab malware scan engine and application reputation database. Landesk can also manage the Windows Firewall.

Landesk expanded its Landesk One technology alliance partner program to support additional capabilities, including endpoint encryption, application containerization, privilege management and Security Content Automation Protocol (SCAP) compliance assessment.

Application control capabilities enable organizations to limit untrusted applications that may not be detected with traditional anti-malware technologies. Application control leverages the application database, containing reputation information of over 2 billion applications to quickly identify unknown and untrusted applications.

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 VMware ESXi hypervisors.

Automated provisioning and state management are particularly useful to easily reimage PCs in the case of pervasive malware.

CAUTIONS

Landesk drifted back into the Niche quadrant this year as a result of lack of focus on the needs of the security role and continued low market and mind share, despite good channel and market presence in the IT service support management tools market. Landesk security workspace should start to help address the needs of security operations when it is released in 2016, but will not address the emerging EDR requirement.

Landesk expanded its relationship with Kaspersky Lab to include both its anti-malware engine and application reputation database. 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 Linux, Microsoft SharePoint, Lotus Notes and Android, or for Windows Mobile clients.

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.

Landesk still does not provide either cloud or on-premises malware sandboxing in its product offering.

While the offering is comprehensive, pricing for the Landesk Secure User Management suite is considered to be at a premium over competing offerings.

Microsoft

Microsoft's System Center Endpoint Protection (SCEP, formerly Forefront) is intimately integrated into the popular System Center Configuration Manager (ConfigMgr) console. Microsoft licensing often includes SCEP, making it an attractive shortlist candidate. Gartner views 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 ConfigMgr, and that have additional mitigating security controls in place, such as application control or additional HIPS protection.

STRENGTHS

Microsoft's malware lab benefits from a vast installation of over 1 billion consumer endpoint versions of the SCEP engine and its online system check utilities, which provide a petri dish of common malware samples. A dedicated enterprise-focused team monitors telemetry from enabled SCEP, Forefront Endpoint Protection (FEP) and Microsoft Intune endpoint clients for enterprise-specific low-prevalence malware.

SCEP relies on the software distribution capability of System Center Configuration Manager for deployment and updates. Existing System Center ConfigMgr shops only need to deploy the SCEP agent. System Center ConfigMgr 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 non-domain-joined Windows PCs. Intune can also manage and enforce security policies for Windows RT, Windows Phone, Android or Apple iOS devices, and integrate with ConfigMgr.

Organizations that are licensed under Microsoft's Enterprise Client Access License (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. It is offered to all Windows users, independent of SCEP.

Microsoft introduced several new security features in Windows 10, including a new anti-malware scan interface (AMSI), PowerShell logging and device guard, App Locker, and enterprise data protection (EDP), which are now managed as part of Microsoft Intune and System Center Configuration Manager vNext (see "Windows 10 for PCs Will Let Organizations Choose How Often They Update").

CAUTIONS

Microsoft SCEP continues to rely heavily on signature-based detection methods. Test results (such as AV-Test and AV-Comparatives) of the effectiveness of SCEP remain very low when compared with industry averages. 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, the impact of which 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 and reporting interface.

While Microsoft supports anti-malware product updates independently, it 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 enterprises cannot upgrade OSs as fast as EPP versions.

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 EMM comes at an additional cost.

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 [Belgium, the Netherlands and Luxembourg] and North America).

STRENGTHS

Panda's Adaptive Defense product provides a good blend of endpoint protection, endpoint detection and response, and adaptive defense capabilities for Windows, OS X, Linux and Android at an aggressive price point that will have strong appeal to SMBs. Over 85% of deployed seats are managed via the cloud infrastructure, with the remainder planned to be migrated in 2016.

The automated classification process for executables has been optimized for better performance and real-time visibility.

Indicators of compromise (IOC) protection supports API for third parties to pull IOCs from Panda Collective Intelligence, along with support for endpoints protected by Panda Adaptive Defense to pull IOCs detected by other solutions via API.

Managed whitelisting is available for embedded systems, including point-of-sale and ATMs.

Panda Advanced Defense provides a service 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.

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.

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

CAUTIONS

The Spain-based vendor continues to slowly expand beyond its EMEA presence into Latin America and the U.S., with APAC adoption remaining very low. Even with this growth, more than 60% of its business remains in Europe. Mind share is still weak in other geographies.

While Panda is focusing on growing its enterprise business, which accounts for 60% of its revenue, nearly 70% of seats are still in the hands of consumers.

Although Panda has several large customers, the cloud-based solutions are primarily designed for SMBs that favor ease of use over depth of functionality, with the significant majority of enterprise sales to sub-500 seat deployments.

Even though the scan process is run with low priority, and users can delay scanning if they are authorized, the solution only offers one option to minimize the impact of a scheduled scanning (CPU load limitation).

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 500 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 of over 700 million endpoints and mobile devices, which provides over 9 billion samples for data mining to automatically and manually create signatures, and to monitor the spread of viruses and malware. 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.

System reinforcement capabilities add additional controls to monitor password complexity, shared folders, registry lists and account permissions, including audit to trace activity, detect illegal internally and externally initiated connections, and prevent access to peripherals.

Qihoo uses peer-to peer technology to upgrade software, signature files and patches to save network bandwidth.

360 Safeguard Enterprise for SMBs is a free, cloud-managed EPP offering for very small organizations (fewer than 200 seats).

360 SkyKey provides EMM solutions, including an antivirus engine for Android.

360 XP Shield Enterprise Edition provides specific protection for Windows XP platforms.

Qihoo offers a managed public cloud solution.

CAUTIONS

Qihoo 360 has a dominant consumer market share in China, but it has no presence in enterprises within Europe or the Americas.

While Qihoo 360 is growing its SMB and enterprise sales, less than 0.1% of total seats deployed are SMB or enterprise seats at this time.

The management interface is in Chinese, and does not provide native English support. It requires localization via the Web browser, which is not effective.

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.

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.

All product modules are not integrated into a common management console, making it more complex to administer.

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.

SentinelOne

SentinelOne is a rapidly growing startup developed to reinvent endpoint protection. The company focuses on behavior-based detection techniques, augmented by a cloud database of threat intelligence. SentinelOne is the only vendor in this analysis that includes full EDR-type functionality in the core platform. SentinelOne is a good prospect to replace or augment existing EPP solutions for any company looking for a fresh approach and integrated EDR, and that is willing to work with an emerging Visionary company.

STRENGTHS

SentinelOne offers on-device dynamic behavioral analysis to detect zero-day threats and APTs and prevent exploitation. The solution performs well in AV tests without relying on traditional signatures, IOCs or whitelisting.

The management console, including full EDR event recording, can be deployed as cloud-based or on-premises, easing installation and scalability.

Automated mitigation capabilities can kill processes and quarantine threats to minimize the impact of destructive threats, and provides a malware removal and remediation feature capable of rolling back changes made by malware, based on recorded behavior.

SentinelOne offers complete endpoint visibility (Windows and Mac) for full investigative information in real time, and an API to integrate in any common-format, IOC-based threat feed.

CAUTIONS

Extended EPP functionality is missing, such as personal firewalls, URL filtering, port protection, data protection, mobile device protection, enterprise mobility management, vulnerability analysis and application control. Application and device control, IP/URL reputation and filtering are planned for 2016. Gartner clients must find alternative providers for the traditional EPP capabilities that are not included in the offering.

SentinelOne is a rapidly growing startup and is likely to suffer from at least some growing pains. It has limited global presence, with most customers in North America and central EU.

SentinelOne participated in an AVtest.org test on Windows 8 and OS X in June 2015 and did well, but it has not been extensively tested for effectiveness against other vendors. Malware authors develop evasions for more popular anti-malware approaches. As SentinelOne becomes more popular, its approach will come under more scrutiny from attackers.

Support for Linux, virtual servers, Exchange and other specialized servers is lacking. Linux and Android are planned for 2016.

Sophos

Sophos is one of a few companies in this Magic Quadrant that sell exclusively to business markets. It makes available free versions of its offerings to consumers. Sophos has expanded into the mid-market network security market, and in 2015 delivered the first release of a consolidated network and endpoint security solution that offers a unified, context-aware approach to threat prevention, detection and response. Sophos is good fit for buyers that value simplified administration, and for organizations that are interested in a unified endpoint and network approach to security.

STRENGTHS

The Sophos Synchronized Security approach establishes a Security Heartbeat between endpoints and perimeter next-generation firewall (NGFW) to exchange contextual information on the overall security status, the health of endpoints and current threats. Synchronized Security triggers actions to address potential threats in real time.

The user threat quotient and application risk index provide insight into the level of risk associated with users and applications, based on history and other metrics.

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.

New prepackaged reporting capabilities provide better insight into day-to-day security operations, which will have broad appeal for the mid-market.

Sophos optimizes the scanning or rescanning of high reputation files by leveraging smart behavior detection from the exploit engine to trigger scanning when suspicious activities are identified.

Sophos' Mobile Control for mobile data protection is a strong product capability set.

Malicious Traffic Detection, crowdsourced reputation, exploit detection engine and Sophos Security Heartbeat enhance traditional signature, heuristic, behavioral and whitelisting techniques to enhance detection.

CAUTIONS

Sophos's innovative marketing campaigns have driven up awareness of the brand in specific targeted markets. However, traction remains focused on the mid-market. Gartner clients rarely report Sophos as a shortlist vendor.

The simplicity of Sophos' management console, which Sophos developed for the mid-market, 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.

Performance test scores for Sophos remain in the middle of the pack.

The movement to a full cloud-managed, network-to-endpoint security platform is promising, but it is still a work in progress, and not all components are fully integrated.

Symantec

In October 2014, Symantec announced a 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 limited capabilities of its application control, the just-introduced malware sandboxing, vulnerability analysis and forensic investigation. Its Ability to Execute score is impacted by three years of corporate strategy adjustments, 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, Norton Power Eraser, into the Symantec Endpoint Protection client.

Symantec continues to be listed as the top overall competitive threat by vendors reviewed in this Magic Quadrant.

Symantec's Security Technology and Response (STAR) technology allows evidence of compromise (EOC) scanning on the endpoint via SEP and is used by Symantec Managed Security Services and Symantec ATP.

Cynic is a cloud-based sandboxing platform that provides bare-metal hardware and network sandboxing analysis of objects submitted by Advanced Threat Protection (ATP), Endpoint Protection and email. Results are passed to ATP for remediation.

Application control offers one-click lockdown via a whitelist or blacklist of applications.

Synapse integrates, correlates and prioritizes SEP, email security, cloud and ATP information.

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 input/output (I/O)-sensitive scan, virtual image exception and file cache, offline image scanner, and randomized scanning.

Symantec's new Advanced Threat Protection will combine network-based object and traffic scanning with existing SEP clients to provide EDR functionality without the need for existing customers to deploy new client agents.

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. Strong competition from vendors in this market and client concerns over the long-term direction of the organization are beginning to show signs of strain with renewals.

Symantec's security product portfolio is not integrated at a meaningful level, and requires five distinct consoles to manage the complete endpoint solution set.

The OS X offering only includes AV and IPS.

Although Symantec has mobile management and protection capabilities and advanced data protection 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 using SEP 12's device control functionality.

Trend Micro

Trend Micro is the third-largest enterprise EPP vendor, with a large worldwide installed base. Trend Micro has made significant visionary investments in the areas of application control, vulnerability detection and shielding, malware sandboxing, and EDR, and continues to lead the market in addressing the specific needs of the data center. It also offers very tightly integrated EMM capabilities, including mobile app reputation service and data protection capabilities. The Smart Protection Suite offers one of the most complete, integrated packaging of protection technologies in this market. Trend Micro is a very 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 detection and shielding, and behavioral monitoring. Trend Micro has also invested in leading-edge security solutions, including a malware sandbox, application control and an incident response investigation tool.

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 and Microsoft Azure. Additional capabilities include encrypting these workloads with its SecureCloud offering and an optional SaaS version of its Deep Security management console.

Trend Micro is the first of the established EPP vendors to deliver an EDR solution. The Endpoint Sensor records endpoint activity, and is used to aid investigation of alerts generated by the Network Monitor, or for malware hunting activity based on a suspicious object, OpenIOC or Yara rules. The Endpoint Sensor EDR tool has an excellent graphical representation of the threat event chain.

Deep Discovery Analyzer, Trend Micro's network-based malware detection sandbox, can be centralized to receive files from Trend Micro Web gateway and email security products. Trend Micro also offers sandboxing as part of its Cloud App Security offering for Office 365. It received top scores from NSS Labs in a breach detection sandbox test.

Trend Micro Control Manager provides security dashboards to give the administrators quick visibility of users and endpoints with multiple points of view to accomplish investigative tasks.

Trend Micro Endpoint Application Control is very complete and includes support for self-updating applications and software deployment tools as trusted sources, as well as out-of-the-box inventory reports.

Trend Micro integrates mobile device management capabilities in Trend Micro Control Manager, with support for Android, iOS, Windows Phone, and BlackBerry.

CAUTIONS

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.

The unifying Control Manager interface is suitable for high level reporting but insufficient for managing individual products. Native consoles for Trend Micro Endpoint Encryption and Application Control must still be deployed to enable day-to-day management within Trend Micro Control Manager. The individual console are still required to updating policies and sending tasks to their agents.

Application control, encryption, DLP and device control do not extend to all OS platforms.

The Endpoint Sensor stores history locally on the agent, rather than a central database. There is no detection capability outside of the network sensor alerts. Remediation and containment actions are based on the OfficeScan client, and are limited to isolating an endpoint using firewall policy, quarantine and block process execution.

Policy-level integration of the various Trend Micro products is still emerging. For example, the application control agent cannot automatically send unknown files to the Deep Discovery Analyzer sandbox for analysis.

Reference customers have commented on the size of Service Pack updates and their effect on the network.

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 and cloud-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 EMM 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 primarily an anti-malware utility. It does not provide port/device control, or endpoint management utilities, such as vulnerability or patch management.

SecureAnywhere provides a basic malware event investigation capability.

Webroot does not protect the workload of specialized servers, such as Microsoft Exchange and Microsoft SharePoint.

Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant may change over time. A vendor's appearance in a Magic Quadrant 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

SentinelOne and Cylance are new entrants this year.

Dropped

ThreatTrack Security was not included in this year's analysis, as the focus of the offering is small and midsize businesses.

Stormshield was not included in this year's analysis, as it did not fit the new inclusion criterion of the ability to displace existing AV solutions in Gartner clients.

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 and worms) that is capable of stand-alone EPP replacement

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 (February 2016)

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 roadmap 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 performance, accuracy, transparency and completeness of malware 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.

Data protection: Minor additional marks were awarded to vendors that offered optional components for data protection, such as encryption, port protection and data loss prevention capabilities.

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 (February 2016)

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 anti-malware solutions that are typically component parts of broader solutions via OEM-provided component parts, or are vendors that offer solutions that complement, rather than replace, incumbent EPP solutions. Some Niche Players have not demonstrated sufficient focus on the core needs of buyers, despite long tenures in this market.

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. [1] 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 processes 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 EMM capabilities and data protection for mobile and employee-owned devices. Buyers should favor solutions that have a short-term integration roadmap of the EMM 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.

Clients investigating solutions for VMware environments need to consider that VMsafe APIs will be going end of life from ESXi 5.5 and beyond. Those wishing to implement ESXi 5.5 or updated versions need to consider how vendors plan to support vCloud Networking and Security.

Solutions that take a more operational tool approach will be more flexible, and will 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 managed security service providers.

Market Overview

When 44% of reference customers for EPP solutions [2] have been successfully compromised, it is clear that the industry is failing in its primary goal: blocking malicious infections. Yet only a few of the EPP vendors are taking radical steps to improve the detection accuracy of their solution. Presumably, protecting 60% of customers has somehow become the industry benchmark for success. The lack of success and customer satisfaction with EPP solutions has driven a massive increase in competition from startup companies and adjacent security vendors, all trying to find a reliable method to thwart malware infections. See the "Market Guide for Application Control Solutions" and the "Market Guide for Endpoint Detection and Response Solutions" for more on emerging alternatives. However, only a few of the new startup vendors have the guts to claim that they can replace incumbent EPP solutions; most are advertised as supplemental protection. As such, they don't qualify for this report. Still, these newer vendors are showing some promising new techniques to block malware. Endpoint detection and response approaches, malware sandboxing for custom file analysis, and application control are becoming more common from the leading vendors and some of the Visionaries.

New approaches,— such as containment, behavior detection, decoy honeypots and algorithmic approaches — are less common among established EPP vendors.

Containment approaches isolate the clean system from potentially malicious files like Microsoft Office docs, Adobe content files, scripts and browsed Internet content files. Interpreted files such as these can have sufficient privileges to attack the system or to attack the container using an unpatched or unknown vulnerability. These files are difficult to detect using a signature-based system. Containment approaches, such as those offered by Invincea

and Bromium, isolate the core system from untrusted interpreted code by policy. This approach is akin to the policy-based isolation layer provided by the app privilege management systems in Android and iOS.

Behavior detection has been around for a while, Webroot is the pioneer of a dedicated behavioral detection engine. However, new entrant SentinelOne continues to refine the technique.

Decoy honeypots, servers and credentials can provide high-fidelity early detection of hackers that are already inside the network. Illusive Networks, Javelin Networks and Attivo Networks are examples of vendors with solutions that provide early warnings of lateral attacks, but have not yet built out extensive investigation or remediation capability.

Algorithmic techniques can detect unknown malware or attack techniques without comparing them to a database of known bad artifacts. Algorithmic techniques (such as machine learning) are based not on a database or list of what is known (good or bad) artifacts, but are based on a computational method that would include characteristics of known good and bad. Machine learning discovers a detection equation, based on predefined datasets (known good and known bad), and it is the equation (not a database traversal) that determines the probability that a new event is good or bad. Cylance and Deep Instinct are representative vendors of this trend toward algorithmic approaches to file detection.

At the same time, traditional data protection features (DLP, encryption and port controls), protection for servers (such as VMware, Microsoft Exchange, Microsoft SharePoint and network-attached storage/storage area network [NAS/SAN]) and personal firewalls are common in incumbent EPP solutions, but rare among new entrants.

However, history has clearly shown that no single approach will be successful for thwarting all types of malware attacks. Organizations and solution providers have to use an adaptive and strategic approach to malware protection.

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, Internet Protocol (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 — such as 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, managing applications and 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 EDR "detection" or "investigation" capabilities, 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 incident 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 a wide array of endpoints (such as Mac, iOS and Android devices), and to integrate those into the management console. Today, many large enterprise buyers are selecting a best-of-breed EMM 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 Microsoft Exchange, Microsoft 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. Collectively, the Niche Players and Visionaries 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 RT, and Apple's iOS and OS X Mountain Lion) is the biggest market threat. While advanced Windows 10 security features, such as Antimalware Scan Interface (AMSI), PowerShell logging or Device Guard, are not broadly supported at this time, we expect them to be over the next three years. These solutions shift the value proposition of EPP solutions from traditional anti-malware to EMM and data and privacy protection capabilities. Concurrently, there are numerous startups responding to the market demand for better protection and detection capacities, and looking to displace or augment incumbents. Vendors such as Bit9, Invincea and Bromium are primarily focused on the "protect" phase of the market. Dedicated EDR is 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.

Evidence

[1] Good performance and malware detection testing information is available from AV-Comparatives (http://www.av-comparatives.org/) and the AV-Test Institute (http://www.av-test.org/en/home/) .

[2] Gartner conducted an online survey of 75 EPP reference customers in 3Q15.

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 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.

(http://gtnr.it/1KsfgQX)

About (http://www.gartner.com/technology/about.jsp)

Careers (http://www.gartner.com/technology/careers/)

Newsroom (http://www.gartner.com/newsroom/)

Policies (http://www.gartner.com/technology/about/policies/guidelines_ov.jsp)

Privacy (http://www.gartner.com/privacy)

Site Index (http://www.gartner.com/technology/site-index.jsp)

IT Glossary (http://www.gartner.com/it-glossary/)

Contact Gartner (http://www.gartner.com/technology/contact/contact_gartner.jsp)