Magic Quadrant for Endpoint Protection Platforms

Published: 30 January 2017 **ID:** G00301183
Analyst(s): Eric Ouellet, Ian McShane, Avivah Litan

Summary

The endpoint protection platform provides security capabilities to protect workstations, smartphones and tablets. Security and risk management leaders of endpoint protection should investigate malware detection effectiveness, performance impact on the host machines and administrative overhead.

Strategic Planning Assumption

By 2019, EPP and EDR capabilities will have merged into a single offering, eliminating the need to buy best-of-breed products for all but the most specialized environments.

Market Definition/Description

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)
- Memory protection
- Endpoint detection and response (EDR) technology (see "Market Guide for Endpoint Detection and Response Solutions")
- Data protection such as full disk and file encryption
- Endpoint data loss prevention (DLP)

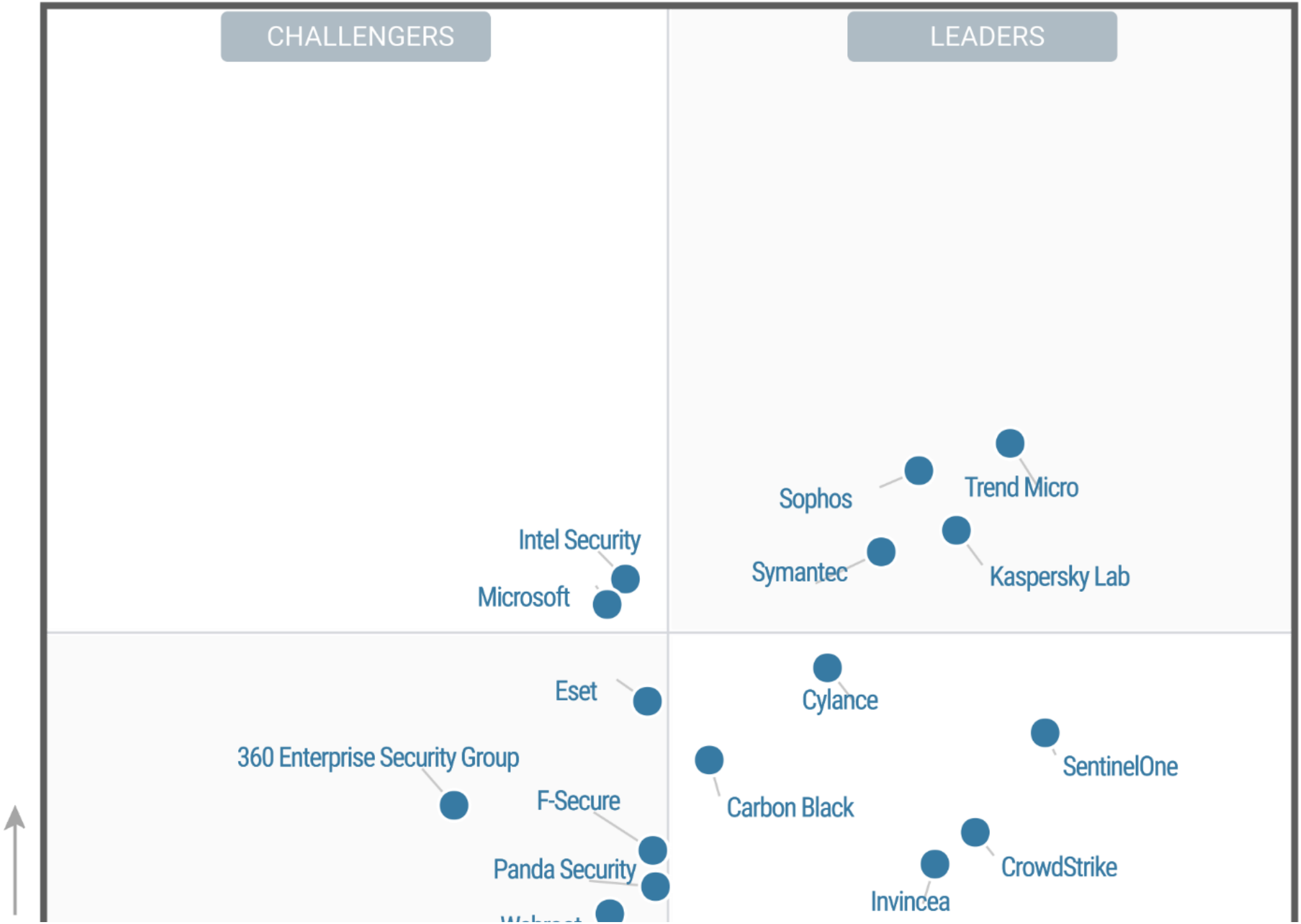
These products and features are typically centrally managed and ideally integrated by shared policies. Not all products in this analysis provide the same collection of features. Here, we focus primarily on anti-malware effectiveness and performance, management capability, protection for Windows and non-Windows 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. [1]

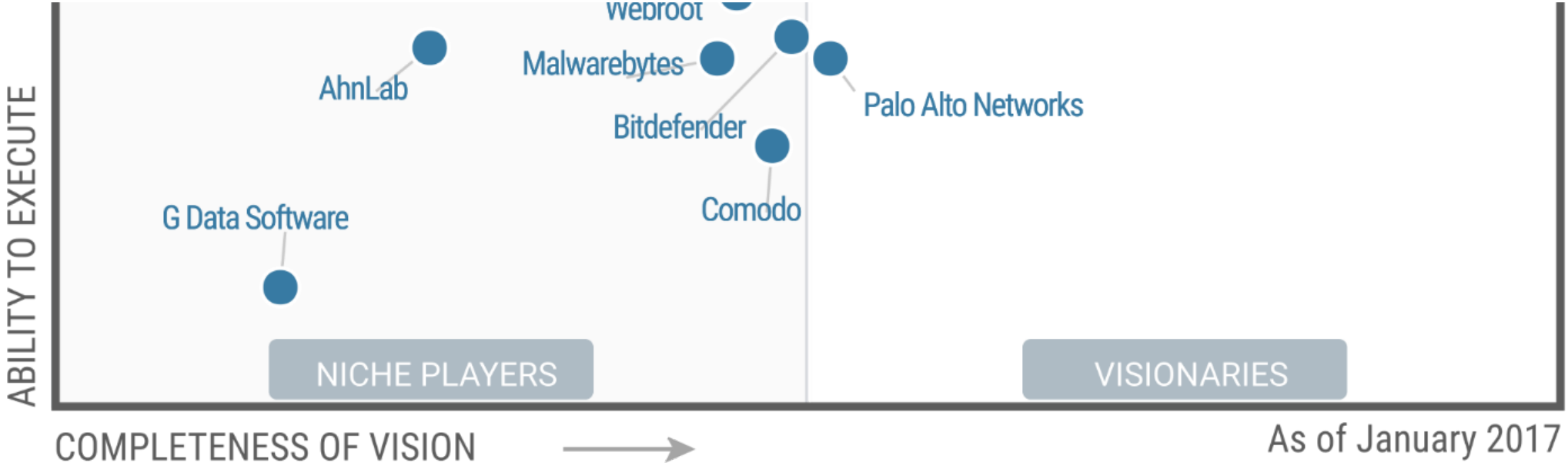
DLP, EMM and vulnerability assessment are also evaluated in their own Magic Quadrant analyses (see the Gartner Recommended Reading section). In the longer term, portions of these markets will be subsumed by the EPP market, just as the personal firewall, host intrusion prevention, device control and anti-spyware markets have been subsumed by the EPP market. EPP suites are a logical place for the convergence of these functions. Organizations continue the trend of using a single vendor for several EPP functions, or are actively consolidating products. In particular, mobile data protection remains 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 their EPP vendor's EMM capabilities.

The total EPP revenue of the Magic Quadrant participants at year-end 2016 was slightly over $3.29 billion, up 2.8% over the previous year. EPP suites continue to grow in functionality. Consequently, some EPP revenue is inflow from other markets. Gartner anticipates that growth will continue to be in the low single digits in 2017.

Magic Quadrant

Figure 1. Magic Quadrant for Endpoint Protection Platforms


CHALLENGERS
LEADERS
Intel Security
Microsoft
Sophos
Trend Micro
Symantec
Kaspersky Lab
Eset
360 Enterprise Security Group
F-Secure
Panda Security
Cylance
SentinelOne
Carbon Black
CrowdStrike
Invincea



Source: Gartner (January 2017)

Vendor Strengths and Cautions

360 Enterprise Security Group

360 Enterprise Security Group, which had been publicly listed on the NYSE as Qihoo 360, was privatized in 2016. The company was merged with other solution providers in EPP, next-generation firewall (NGFW), security information and event management (SIEM), and entity and user behavior analytics (EUBA) to form 360 Enterprise Security Group (360 ESG).

360 ESG is a dominant consumer security company in China, owning 98% of the consumer EPP market. 360 ESG has gained a significant amount of Chinese enterprise customers via its "made in China" security software, which is compliant with Chinese government policy to localize most technologies, making it a good choice for the local enterprise EPP market.

STRENGTHS

360 ESG has a massive installed base of over 830 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.

360 ESG 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 connections initiated both internally and externally, and prevent access to peripherals.

Malware protection includes a machine-learning-based sample classification and behavior-based protection.

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

360 ESG offers a cloud-managed solution.

CAUTIONS

360 ESG has a dominant consumer market share in China, but it has no presence in enterprises outside of its local market.

While 360 ESG is growing its SMB and enterprise sales, less than 0.1% of total seats deployed are SMB or enterprise seats at this time, with the remainder being consumer seats.

Malware protection methods that are based on rapid sample collection and signature distribution lack global sample collection methods will hinder effectiveness at detecting regional threats outside of 360 ESG's main market.

While 360 ESG would like to expand sales of its product in and beyond China, it will have to provide an English-language version that is competitive with other EPP firms active in the region.

AhnLab

AhnLab is a new entry to the EPP Magic Quadrant. AhnLab controls more than half of South Korea's software security market, and demonstrated double-digit growth in the Asia/Pacific (APAC) region in 2016. The company has offices in China and Japan, and local partnerships in other jurisdictions. AhnLab is primarily an enterprise solution provider, with modest consumer presence. Consumer products, while limited in applicability in enterprise solutions, typically provide high profit margins that can be redirected to enhancing the enterprise portfolio.

AhnLab predominantly appeals to smaller organizations in the APAC region looking for an integrated EPP solution set that includes patch management.

STRENGTHS

AhnLab provides advanced malware protection, leveraging dynamic intelligent content analysis (memory analysis, code analysis) for pre- and postexecution scanning.

The EPP solution blends signature, blacklist/whitelist, reputation, correlation and behavior techniques to reduce false positives. Data is sent to the AhnLab cloud to share with other protected assets.

AhnLab's EPP offering consists of a centralized policy center controlling anti-malware, anti-spyware, intrusion prevention system (IPS), firewall, PC management, app control, web security, email security, data-wiping capabilities and endpoint patch management.

AhnLab's solution supports a wide range of operating systems, including current Windows, OS X and Linux, and other platforms, such as Windows XP SP2, Solaris SPARC 2.6, HP-UX11 and IBM AIX 5.2.

CAUTIONS

The majority of AhnLab's client base is organizations of fewer than 500 users, which may limit appeal beyond its SMB base.

While the management console interface offers good insight, both workflow and efficient event detection may become strained when large populations of endpoints are under management.

With many of the advanced protection features being cloud-based, untethered systems operating without a network connection will be disadvantaged.

AhnLab is currently not optimized for virtual server environments or integrated into Amazon Web Services (AWS) or Microsoft Azure. Support for AWS and Azure is planned for 4Q17.

Bitdefender

Bitdefender is a private software company that provides good effectiveness across a broad range of platforms and capabilities. While a large part of its revenue is currently derived from its consumer business, Bitdefender continues to focus growth in its enterprise segment with heavy investments in its sales organization and a new U.S.-based enterprise headquarters.

Updates to the endpoint security suite focus on protecting against ransomware attacks and adding anti-exploit technology. Bitdefender is a good choice for SMBs and for larger organizations that highly value malware detection accuracy, performance, and full support for data center and cloud workloads from a single solution provider.

STRENGTHS

Bitdefender has had continued, significant OEM business growth, with over 120 technology partners, which highlights third-party confidence in its solution set.

Bitdefender's solution is a solid high performer in third-party malware detection tests.

The agent has low system overhead, and includes a sandboxed application emulation environment, automatic unknown file analysis, continuous behavior monitoring, machine learning and exploit mitigation.

Bitdefender places special emphasis on a vendor-agnostic architecture for data center protection (physical and virtual servers) and cloud workload environments. Its flexible licensing options offer hybrid public and private cloud-based solutions that appeal to organizations looking for a single vendor experience for the entire ecosystem.

The management interface includes the ability to dedicate its GravityZone servers to specific tasks and processes, resulting in a scalable architecture that suits many different types of organizations.

CAUTIONS

While Bitdefender has invested in growing its enterprise sales operations, mind share remains low in the enterprise market outside the geographic strength in central EU, thereby limiting shortlist opportunities and apparent viability to larger clients.

Bitdefender continues to lack full-feature parity across its supported platforms, an issue that was highlighted in previous Magic Quadrants. This results in pockets within organizations with varying levels of protection. Specifically, its OS X and Linux agents have only anti-malware capabilities, and do not include firewall, device control or application control.

There are no EDR capabilities included in the GravityZone management platform.

With many of the advanced protection features leveraging cloud-based intelligence and analysis, untethered systems operating without a network connection will be disadvantaged.

Carbon Black

Carbon Black, a new addition to the EPP Magic Quadrant for 2017, is a high-double-digit growing solution provider. Since 2002, Carbon Black has raised over $190 million in venture capital. Carbon Black combines three solution categories as part of its protection ecosystem. Cb Protection (formerly known as Bit9 Security Platform) provides application whitelisting and device lockdown technology. Cb Response is the EDR component that enables incident response and indicator of compromise hunting. Cb Defense, a recent acquisition of the small anti-malware vendor Confer Technologies, aims to improve Carbon Black's standing as a replacement for more traditional EPP solutions.

Large organizations looking for a full range of protection and detection and response capabilities will find Carbon Black a good shortlist candidate to replace or augment endpoint protection platforms.

STRENGTHS

Carbon Black provides an offering that serves organizations looking to replace traditional antivirus (Cb Defense), in addition offering to an advanced toolset (Cb Protection) that has broad appeal to organizations with mature security teams consisting of high-caliber and experienced personnel.

Carbon Black offers a good balance of feature parity across supported platforms, except for device control, which is missing from OS X. Device control and file integrity capabilities protect applications on endpoints from tampering.

Cb Defense protects against file-based and fileless attacks, and monitors process behavior and events to gain more insight into suspicious activity and to reduce false positives. Information is sent to Cb Collective Defense Cloud for analysis and sharing among other clients.

Cb Protection implements strong application control policies, enabling protection through isolation and default-deny for endpoints, servers, virtual workloads and cloud.

CAUTIONS

Carbon Black is still integrating its recent acquisitions, and now has three independent agent products and three independent management consoles. While most Carbon Black clients will not deploy all three solutions concurrently, those who do will experience the challenges and increased deployment complexity associated with a lack of a single centralized management console for a vendor's set of offerings.

While Cb Defense has participated in private antivirus efficacy tests from a few testing organizations, it has yet to participate in independent public tests.

Clients deploying Cb Protection may require additional staff with a keen understanding of applications to maximize the effectiveness and transparency of deployment. Managed service options are available via third parties, but at high cost.

Carbon Black has focused on a North American base to fuel its growth, and remains early in its international expansion in Europe, Middle East, and Asia/Pacific and Japan (APJ).

Comodo

Comodo, a new addition to the EPP Magic Quadrant for 2017, is primarily known to enterprises as an X.509 certificate vendor. Over the last few years, Comodo has expanded its product portfolio to include a baseline of EPP capabilities to enterprises, (free, premium and platinum) with Comodo Advanced Endpoint Protection; and to consumers (free), with its Comodo Internet Security. Comodo also provides free enterprise forensic tools that give insight into threats. The "freemium" model for Comodo Internet Security is in support of Comodo's effort to build brand awareness.

Comodo is a good choice for organizations looking for a default-deny approach without having to manually approve applications.

STRENGTHS

Comodo Advanced Endpoint Protection (AEP) provides a balanced approach with its default-deny approach to endpoint protection with application whitelisting and high-performance secure autocontainment for unknown applications until identified as safe. Unknown applications are sent to the cloud for a verdict.

A channel-partner-friendly solution set that supports value-added reseller (VAR), system integrator, managed service provider (MSP) and managed security service provider (MSSP) deployments will appeal to clients looking for a simplified deployment experience and a baseline of typical EPP features.

Comodo AEP offers core EPP feature support for Windows XP and newer Windows workstations and servers, OS X, Linux, iOS, and Android operating systems, along with AWS and Microsoft Azure cloud environments.

Script containment technologies are used to analyze behavior of fileless malware, including those executed in PowerShell and other script interpreters.

CAUTIONS

A lack of full-feature parity across Comodo's supported Windows, Mac OS X and Linux platforms results in pockets within organizations with varying levels of protection. Specifically, Windows has the most advanced feature set, while OS X and Linux agents primarily have only the antivirus signature engine and do not have the endpoint firewall, machine learning, endpoint containment technology or dynamic behavior analysis, among other missing components.

While Comodo is developing a security VAR channel, the reseller network for Comodo's well-known X.509 certificate offering may not be a direct fit for clients looking for a higher-touch EPP sales and support.

Linux is currently managed via its own console, with plans to integrate into Comodo's main console in 2017.

Comodo Valkyrie's advanced file analysis features leverage cloud-based intelligence and analysis, so untethered systems operating without a network connection will be disadvantaged.

CrowdStrike

CrowdStrike is a new addition to the EPP Magic Quadrant for 2017. CrowdStrike is well-known to enterprises for its EDR solution and is expanding into the EPP market. CrowdStrike has raised over $156 million in venture capital.

The company grew its installed base rapidly in 2016 due to the publicity from high-profile incident response work, and the attractiveness of the CrowdStrike Overwatch service, which provides monitoring and expert assistance to resolve alerts.

CrowdStrike has replaced incumbent anti-malware solutions in several large-profile accounts and is a good shortlist candidate for most organizations. CrowdStrike will have the greatest appeal to those already leveraging the Crowdstrike EDR solution, and that are looking to combine the EDR and next-generation anti-malware components in a single agent, as well as those looking for assistance in resolving alerts via the managed threat-hunting service.

STRENGTHS

CrowdStrike's Falcon Host was one of two next-generation signatureless anti-malware solutions selected for inclusion in the VirusTotal scanning engine.

The well-known presence of CrowdStrike EDR solution in diverse organizations — including SMB and large, complex deployments with strong channel partner networks — provides a simplified entry path for Falcon Host anti-malware.

CrowdStrike offers broad platform support of core anti-malware protection for Windows 7 and Windows 2008 servers (and newer), OS X 10.10 (and newer), Red Hat Enterprise Linux (RHEL), CentOS, Ubuntu, and SUSE Linux Enterprise Server (SLES) endpoints, data center servers, virtual machines and cloud, including AWS, Azure and Google.

Fully cloud-based management console simplifies deployment scenarios for organizations that accept this type of management infrastructure.

CAUTIONS

While CrowdStrike has added offices in the U.K. and Australia, the vast majority of their sales remain in the EDR segment of their business and specifically within the North American market, which may reduce the appeal of the solution with organizations in less-well-served geographies.

Windows remains the most feature-rich platform, whereas OS X and Linux lack memory protection and script protection, which results in pockets within organizations with varying levels of protection.

Application whitelisting and blacklisting is entirely customized and managed by end clients. This process can be accomplished either manually or via an API.

Lack of legacy OS support, such as Windows XP (typically used for point of sale, kiosks and other high-risk/high-value operations), restricts appeal to enterprise desktops and will force organizations requiring legacy support to look for solutions elsewhere.

Cylance

Cylance accelerated its high-growth pace in 2016 and is by far the fastest-growing EPP vendor in the market. Excellent marketing has created a very strong brand awareness, and Cylance customers report easy deployment and management, low performance impact, and high pre-execution detection rates against new threat variants.

New since the last EPP Magic Quadrant is the addition of CylanceOPTICS, an endpoint detection and response solution delivering visibility into the root cause of attacks, enabling threat hunting and incident response.

Cylance is a good choice for any size of organization looking to augment or replace an existing antivirus solutions, or those looking for a lightweight alternative to signature-based approaches to malware detection.

STRENGTHS

The Cylance Protect machine-learning anti-malware solution has been demonstrated to be lightweight and effective on some of the most resource- and network-constrained endpoints, including Windows XP SP3 and virtual desktop infrastructure (VDI) environments, even without regular update cycles.

The management console now offers the option of cloud-based or on-premises deployment.

Cylance does not rely on cloud-based detection enhancement solutions, 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).

In 2016, Cylance added script control support, including macros, memory protection, application control and device control features.

CAUTIONS

While Cylance’s algorithmic detection methods have been proven effective at this time, as more vendors enter the market with similar approaches, malware authors are becoming aware of signatureless anti-malware solutions and are beginning to focus their R&D efforts to reverse-engineer and evade them. Cylance clients will need to remain aware of the constantly changing threat landscape, and Cylance will need to be vigilant to ensure its methods remain effective.

Cylance's marketing and growth rate have prompted competitors to double-down their efforts to more aggressively compete against Cylance in 2017, including offering similar machine-learning detection solutions and developing specifically targeted competitive marketing. This attack from the technology and marketing flanks will require Cylance to simultaneously scale solution delivery, turn roadmap promises into product features, innovate and keep investing in aggressive marketing.

Cylance will operate in 2017 against a backdrop of unusually high market expectations, including validation of malware protection by third parties and the ability to turn cautionary one-year contracts supplementing legacy endpoint protection into multiyear endpoint protection replacements.

Eset

Eset is an EU-based company with a strong market share among both SMBs and large enterprises. U.S. sales have had dramatic growth over the past 12 months, and represent a good balance of revenue blend with EMEA, APAC and Latin America.

The installed base remained a strong, high-margin operation through 2016, and continues to be an engine for funding the 40% year-over-year (YoY) growth in R&D overall, as well as the expansion of development offices in Canada and Poland, together with new offices in Romania and the U.K.

Eset prevention technology performs well in third-party tests, with a lightweight client that continues to be of interest to organizations seeking a simplified and effective lightweight anti-malware solution.

STRENGTHS

Despite the low overhead from its lightweight client, Eset's anti-malware engine remains a consistently solid performer in test results. The EPP solution includes a local sandbox, a memory scanner that monitors process behavior and a vulnerability shield for widely exploited software.

Eset offers one of the broadest coverages of capabilities, across Windows, OS X, Linux/BSD, Solaris, Android, iOS and VMware vShield. Significant localization makes the solution appealing to clients with geographically dispersed users.

When suspicious events occur on an endpoint, Eset will take a configuration snapshot, capturing details such as running processes, registry content, startup items and network connections. This detail can be used remotely to diagnose infections and to detect changes over time.

Flexible licensing options provide simple terms for organizations looking to migrate solutions from on-premises data center servers to virtual environments to cloud.

CAUTIONS

Machine-learning-based detection, while available on endpoints, is augmented with Eset Live Grid. Eset Live Grid findings are shared with all Eset endpoints. Loss of connectivity will affect access to enhanced capabilities.

Basic EDR functionality is added through a separate purchase of Eset Enterprise Inspector, rather than included in the EPP platform itself.

Eset does not yet offer a cloud-based management console, but plans to deliver Eset Cloud Administrator in 2017.

The management dashboards still do not provide any vulnerability or configuration information that would aid in security state assessments.

F-Secure

Through 2016, F-Secure continued with its track record for high-accuracy, low-impact anti-malware detection. F-Secure has reorganized itself into corporate and consumer product divisions to better focus product sales and development efforts. A new Cyber Security Services unit was created from its acquisition of nSense to provide enhanced threat and incident response.

Recent product updates have increased the overall product appeal and ability to sell to larger enterprises, including improved integration with SIEM and syslog servers to work with third-party analysis and orchestration platforms. Its Protection for Business service includes REST APIs for organizations looking for deeper integration.

As with most vendors in the EPP Magic Quadrant, F-Secure has added product enhancements with a specific focus on preventing ransomware attacks.

F-Secure remains a good choice for SMBs and mid-market organizations in supported geographies that weight malware protection as the most important decision factor in their EPP vendor selection.

STRENGTHS

F-Secure has consistently good malware test results and performance tests. It includes cloud-based file intelligence look-ups and a virtual sandbox for malicious behavior detection. DeepGuard exploit mitigation also aids in the detection of advanced threats and fileless attacks.

F-Secure client agents are lightweight, with minimal performance impact.

F-Secure's Rapid Detection Service is a managed security offering that uses sensor technology on endpoints and networks to detect attacks, and leverages F-Secure specialists for review, forensic analysis and response.

F-Secure's Virtual Security solution for virtual and cloud environments is a hypervisor-agnostic, agent-based security solution that operates as a separate security virtual machine (VM).

F-Secure continued to improve the administrative user experience in both on-premises and cloud-based management consoles.

CAUTIONS

While sales are strong in Northern Europe, Germany, France and Japan, global organizations should review their local vendor coverage and support options to ensure F-Secure or their chosen reseller will be able to adequately service the needs of their accounts.

The ongoing updates to the management interface provide for a better experience, but still need to be improved to facilitate the integration of additional relevant data points in context and to streamline the incident response 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, or network-based malware sandboxing capability, thereby reducing the appeal of F-Secure to organizations looking for baseline protection solutions.

Although the majority of the malware protection comes from F-Secure's own signatures and DeepGuard behavioral detection techniques, it continues to use Bitdefender as a signature-based malware as an additional detection engine. Business disruptions at Bitdefender could impact F-Secure customers.

Very modest penetration in the North American market emphasizes the vendor's decision to not invest in growing this region.

G Data Software

While G Data Software is a new entry in the EPP Magic Quadrant, it started shipping its first antivirus product in 1987. G Data has one of the longest histories in antivirus and endpoint protection. However, outside of the DACH region (Germany, Switzerland and Austria), it is a largely unknown vendor. The G Data Endpoint Protection Business product includes the most common features: personal firewall, behavioral analysis, basic application blacklisting/whitelisting and basic USB device protection.

The strength in DACH is based on very simple licensing that does not distinguish between a server or client operating system, as well as strong support for a "made in Germany" brand and excellent customer support.

Small businesses within supported regions that value simplicity and breadth of solution over market-leading features would find G Data a good shortlist candidate.

STRENGTHS

The comprehensive solution includes basic management capabilities for Windows, Mac, Linux, Android and iOS, patch management and distribution, an Exchange plug-in, and network traffic reporting from the endpoint clients.

Organizations that have strict operational requirements, or lower-specification hardware requirements, will find appeal in the granular configuration options where administrators can tune performance at the cost of detection by disabling core components, real-time scanning and even specific engines.

The management console includes the ability to list every application installed on endpoint devices, which can help prioritize patch management.

CAUTIONS

Although the localized malware threat protection initially comes from G Data's own engine, it continues to use Bitdefender as a signature-based malware detection engine. Business disruptions at Bitdefender could impact G Data customers.

Incident response is limited to a "remove virus" option, and the G Data client lacks market-leading features such as EDR-type searching and hunting.

The solution neither tracks nor logs the actions of individual security administrators, which will hamper change control and root cause analysis in the event of misconfiguration.

Intel Security

Intel Security in is the process of becoming McAfee Security, with a deal expected to close in the spring of 2017 where TPG will own a 51% stake in the new company and Intel will retain 49%.

Intel Security remains one of the top three incumbent EPP vendors, and is the second-most-quoted competitor by other vendors in the EPP Magic Quadrant. While it has benefited from cross-sales of a wide range of McAfee security solutions, the organization's overall sales growth has been reduced in recent years.

Customer satisfaction remains low, and EPP clients in particular remain disenchanted with the overall McAfee service and product experience.

Specifically, Endpoint Security ENS version 10.x (v.10.x) has been a very challenging adoption cycle for McAfee. This and other factors contributed to the movement of McAfee to the Challengers quadrant.

Initial issues in early 2015 with 10.0 stability, combined with a complex ePolicy Orchestrator (ePO) upgrade process that requires ePO version 5.03 for 10.x support, left clients, resellers and system integrators with significantly lowered interest in upgrading to 10.0 and 10.1 (available in December 2015). With the release of 10.2 in August 2016 and 10.5 in December 2016, the sentiment seems to be slowly changing.

These last two updates address the majority of the issues previously encountered, and introduced long-requested capabilities, including machine learning and other integrated advanced threat protection capabilities that also targeted ransomware.

STRENGTHS

Intel Security offers a broad array of protection mechanisms, including firewall, web controls, malware protection, dynamic application containment 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 offers organizations the benefits of ePO with significantly faster deployments and less solution management 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 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.

CAUTIONS

The significant percentage of Intel Security's clients remain on v.8.8, with a slow adoption of ENS v.10.x versions, resulting in client questions about McAfee's resellers' and system integrators' commitment to the upgrade, and the viability and effectiveness of the platform overall.

The most common customer complaints continue to be the effectiveness of the older multiple-agent architecture and its impact on deployment complexity and performance. Client inquiries reveal that many clients are not actively planning a migration process to the updated platform.

The lack of focus and direction by Intel Security over the last several years has resulted in a significant exodus of critical talent from McAfee, with most finding new homes with direct competitors both large and small. This deep insight of core Intel Security products and planned strategies by competitors means that Intel Security will be under significant pressure over the next 18 months to secure renewals, and to establish thought leadership positions and new innovative vision for the overall security offering.

Organizations must upgrade to the latest versions of Intel Security ePO 5.03 and 10.5 endpoint agent to take advantage of the latest detection techniques, performance enhancements and administration improvements. Even with a recently streamlined upgrade processes, many organizations report to Gartner that they find the upgrade path burdensome and are actively considering alternatives.

Invincea

Invincea is a new entry in the EPP Magic Quadrant. Started in 2009, with more than $21 million in Defense Advanced Research Projects Agency (DARPA) contracts, Invincea experienced healthy double-digit annual growth in 2016. It has just recently secured a new $10 million round of funding specifically to enhance its product sales and marketing efforts, bringing its total investment rounds to nearly $50 million.

Best known for its virtual-container platform, in 2016 the company added X by Invincea, which provides machine-learning analysis and behavior-based analysis for anti-malware protection.

Invincea Labs, a subsidiary of Invincea, continues to be a research arm for the company, with security research projects funded through various DARPA programs and private initiatives.

Invincea X was one of two next-generation anti-malware solutions selected for inclusion in the VirusTotal scanning engine.

STRENGTHS

Invincea Labs provides a unique research, testing and development platform that benefits its corporate entity through the productization of mature ideas, such as X, when combined with Invincea's deep learning malware genotyping technology and timeline analysis of process, system and file system behaviors. This is beneficial to customers with malware analysts or threat response specialists.

Invincea provides a unique hybrid solution consisting of next-generation machine learning and a behavioral monitoring anti-malware solution, with optional virtual container/application isolation support to minimize the risks of documents and files of unknown or questionable provenance.

Flexible licensing terms place endpoints, servers, virtual environments and cloud protection on similar licenses. Invincea's innovative "test drive" program provides a fully configured test environment for prospects to try the solution on their own, with supplied malware and bring-your-own-malware support.

The integrated EDR solution provides insights into endpoint events and can be used to dynamically assess potential issues and to perform postevent forensics.

CAUTIONS

Invincea currently offers support for Windows XP and newer, and Windows Server 2008 and newer only. OS X, Linux, iOS and Android malware detection and prevention capabilities are planned for 2017, but will not support application isolation.

Invincea does not provide extended EPP capabilities, such as personal firewalls, URL filtering, port protection, data protection, mobile device protection, enterprise mobility management, vulnerability analysis and application control. Organizations seeking these capabilities will have to source and manage them separately.

Invincea has an emerging presence outside of North America. The company will need to invest heavily in developing international sales and support channels to become a viable competitor to existing incumbent EPP providers and organizations with global presence.

Kaspersky Lab

Kaspersky Lab is the largest privately held EPP vendor, ranked fifth in terms of market share. It is repackaged by several large-name vendors. Kaspersky recently started focusing on high-touch sales and support efforts for enterprise customers.

Kaspersky continues to innovate from within, instead of through acquisitions, which has led to a well-integrated product portfolio. The company's malware research team has a well-earned reputation for rapid and accurate malware detection.

Kaspersky Lab's Completeness of Vision score benefits from very good malware detection effectiveness as measured by test results, as well as its virtualization support, Host-based Intrusion Prevention System (HIPS), integrated application control and vulnerability analysis.

It is a good candidate as a solution for any organization.

STRENGTHS

The Kaspersky agent offers strong protection with advanced HIPS features, behavioral detection, vulnerability shields, application and Windows registry integrity control, real-time code analysis at execution time, pre-execution detection using machine learning, and integrated URL filtering.

The endpoint agent (Kaspersky System Watcher) can perform a system rollback of system changes made by malware.

The Kaspersky Anti Targeted Attack (KATA) machine-learning platform provides protection against advanced threats with sandboxing capabilities.

Kaspersky Lab's vulnerability assessment scanner analyzes the versions of the Windows OS and other installed software, then compares that data with data in Kaspersky Lab's specialized vulnerability database.

Automatic Exploit Prevention (AEP) targets malware that leverages software vulnerabilities by mitigating common exploit techniques, especially in well-known targets, such as Java, Flash, Adobe Reader, browsers and office applications.

CAUTIONS

Kaspersky Lab's client management tool features (such as vulnerability and patch management) are not replacements for broader enterprise solutions. However, they are good for the enterprise endpoint security practitioner to validate operations, or to replace or augment SMB tools.

The solution still lacks EDR functionality, but Kaspersky Lab plans to add features to its KATA platform in the future.

Despite Kaspersky Lab's reputation as a very strong, research-driven organization, their installed base remains heavily skewed to SMB. While there has been growth in adoption by large organizations, they should ensure the Kaspersky management platform scales appropriately for their deployment needs.

Kaspersky has experienced flat growth since 2013, which it claims reversed in 2016. However, as a market-leading vendor in the EPP market, it will face increasing pressure from next-generation anti-malware solution providers vying for recognition and incumbent displacement credentials.

Malwarebytes

Malwarebytes is a new entrant to the EPP Magic Quadrant. It has previously been mostly associated as an incident response solution by Gartner clients, and typically used to remove stubborn viruses and other endpoint malware infections that other solutions were unable to eradicate. The past 18 months has seen a shift in the communications and marketing efforts from postincident response to prevention.

The company has demonstrated strong double-digit revenue growth in 2016, admittedly on a relatively small base. Consumers continue to represent the majority of licenses, with a roughly 3:1 ratio, but sales across business and consumer are drawing close to a 50/50 split, with a predominance of business sales to small North American businesses under 500 seats. Europe remains a distant second in market penetration.

External funding of $80 million has helped Malwarebytes grow sales and increase its subscription base dramatically.

STRENGTHS

Malwarebytes offers application hardening, exploit mitigation, application control anomaly detection, machine learning, and behavior monitoring and blocking.

Strong remediation capabilities using the nonpersistent agent can automatically be triggered by SIEM-directed events.

A flexible licensing model (where workstations and physical servers are equivalent), virtual desktop, virtual server and cloud are offered on a per-use basis.

Malwarebytes does not rely on cloud look-ups or external threat intelligence services for threat detection. Organizations with untethered endpoints and no network connectivity will therefore continue to have the full protection available in the solution.

CAUTIONS

Malwarebytes' OS X and Android offerings require their own management console, as they are not integrated with the on-premises console. This results in additional deployment complexity. Additionally, OS X currently only provides malware remediation; real-time protection is planned for 2Q17.

Advanced EPP prevention capabilities, such as application whitelisting, sandboxing and process isolation, are planned for year-end 2017.

Malwarebytes lacks typical large vendor EPP suite capabilities, such as port protection, data protection, mobile device protection, enterprise mobility management and vulnerability analysis. Organizations requiring this functionality will have to source and manage these capabilities separately.

While Malwarebytes has strong consumer awareness, and many businesses use Malwarebytes for remediation today, the company must increase its brand awareness in endpoint protection, where the competition is fierce from incumbents and well-funded next-generation anti-malware solution providers.

Microsoft

Microsoft is a unique vendor in the EPP space, as it is the only one with access to embed protection capabilities directly into its own operating system at the time it is designed and coded. This means that the Windows Defender agent itself (also known as System Center Endpoint Protection, or SCEP) includes few of the typical EPP agent functions natively. Instead, the protection features usually associated with EPP are provided separately within the operating system, including SmartScreen and the Windows Firewall. Each of these, along with the Office 365 Advanced Threat Protection (ATP) add-on, act as edge-level protection to prevent malware from reaching the system.

OS-level features, such as Windows Defender Application Guard, App Locker, Secure Boot, Device Guard and BitLocker, aim to prevent malicious activity from threats that do make it to the device.

It is important to note that while Microsoft is planning a series of advanced EPP features in the evolution of the Windows 10 platform — including Windows Defender ATP, identity protection, application isolation and microvirtualization, among others — none of these are planned for backward compatibility with previous OS releases.

STRENGTHS

Microsoft introduced several new security features in Windows 10, including a new anti-malware scan interface (AMSI), PowerShell logging, Device Guard, App Locker and Windows Information Protection (WIP), which are now managed as part of Microsoft Intune and System Center Configuration Manager.

Microsoft's Completeness of Vision score benefits from the direction of OS-level protection elements such as hypervisor-based isolation, Credential Guard, Device Guard and Windows Defender Application Guard. Allowing third-party vendors the ability to integrate with and provide the management overlay for these features demonstrates a mature security vision.

Organizations that are licensed under Microsoft's Enterprise Client Access License (CAL) or Core CAL programs receive SCEP at no additional cost, leading organizations to consider using it as a safety net, while redirecting EPP spend to a next-generation antivirus (NGAV) product.

To address the emerging threat of malware with polymorphic components, Microsoft added a new, cloud-based to its protection stack, called Block at First Sight (BaFS). BaFS uses machine learning, heuristics and similarity rules to reach a verdict on unknown files.

Microsoft's Malware Lab benefits from a vast installation of over 1 billion consumer endpoint versions of the Windows Defender 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.

CAUTIONS

Despite the additional cloud-based and non-signature-based detection methods, Microsoft SCEP continues to rely on Windows Defender's signature-based detection. Third-party test results show an ongoing improvement in the effectiveness of SCEP, but remain low when compared with industry averages and as reported by Gartner clients.

To take advantage of Windows 10 Secure Boot and Device Guard requires Unified Extensible Firmware Interface (UEFI) to replace Basic Input/Output System (BIOS) booting, leading some Gartner clients to tie their upgrades to hardware refresh and increasing the overall cost of the upgrade.

Most organizations cannot upgrade to Windows 10 as fast as they could update their EPP versions, which may result in the slow uptake of new OS-based security features, unprotected systems and increased opportunity for third-party vendors.

Microsoft has announced the end-of-life plans for the Enhanced Mitigation Experience Toolkit (EMET), which organizations use to protect against common exploits and vulnerabilities, and which third-party researchers had found still added significant value to Windows 10 defenses.

Microsoft does not have a central security-specific management interface, making it more complex to manage than rival solutions.

Microsoft's future vision, while very forward-thinking and technically elegant, only becomes available when organizations create new systems from scratch with Windows 10. As many organizations have linked their Windows 10 deployment plans to their hardware refresh cycle beginning in 2017, it is likely to take three to four years to complete.

Palo Alto Networks

Palo Alto Networks is best known to Gartner clients for its next-generation firewall (NGFW) product line and the introduction of its perimeter-deployed sandboxing and malware analysis solution, WildFire. In 2014, Palo Alto Networks acquired Cyvera, launching the Traps endpoint security platform.

Palo Alto Networks calls its Traps strategy "multimethod prevention," blocking attacks without the need for traditional antivirus or host IPS signatures on the endpoint. Traps leverages threat intelligence, machine learning, static and dynamic analysis, and advanced stack and memory manipulation prevention. Traps monitors processes and applications as they are spawned for suspicious activity and events, and data from the endpoint is correlated with events uncovered by Palo Alto Networks' NGFW devices and WildFire.

Traps has only appeared in one recent third-party malware detection test, and although Traps performed well in this test, Gartner would like to see a continued trend of participation.

Palo Alto Networks' Traps will have primary appeal to existing Palo Alto Networks NGFW customers that are looking specifically to enhance an existing EPP solution already deployed within their environment.

STRENGTHS

Organizations with existing Palo Alto Networks NGFW devices will be good candidates for an integrated deployment as an extension to their existing relationship with Palo Alto Networks.

Traps has very good attestation of the disposition of unknown files and application exploit protection. Analysis of processes and applications in real time provides enhanced protection against unpatched vulnerabilities and fileless malware attacks.

Palo Alto Networks recently added a machine-learning file analysis system to provide immediate assessment of unknown files while they are getting analyzed in the WildFire cloud.

Palo Alto Networks offers flexible licensing of the Traps agent and does not distinguish between Windows workstations, Windows-based VDI, or Windows servers in a data center or virtualized environment. Management of Traps is from a single console.

Traps has received Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry Data Security Standard (PCI DSS) certification, which has been a driver for much of its recent sales.

CAUTIONS

While Traps collects endpoint forensics data, it does not provide any response capabilities or postevent remediation tools. This will lead organizations that require these capabilities to take a multivendor approach.

Traps is a solution supporting nearly all variants of Windows, including Windows XP; however, there currently is no support for OS X or Linux devices.

Gartner clients report that troubleshooting false positives in Traps is almost impossible without the help of senior-level tech support. Memory dumps are available for analyzing exploit prevention events but tuning the modules to address a false positive has been difficult without support assistance. The release of a dynamic update mechanism now allows tuning to be proactively shared across the customer base.

While Traps is suitable for malware engine replacement or augmentation, it does not provide the other components typically demanded of EPP solutions, such as DLP, mobile device management, firewall or device control. Clients looking to replace their existing EPP suites will need to consider a hybrid vendor approach.

Panda Security

Panda Security still counts EMEA as its primary market, with U.S. and Latin America distant second and third, respectively. Recent wins with large clients are promising, as most of Panda Security's existing client base continues to be small organizations with fewer than 500 seats.

Panda Security's Adaptive Defense 360 incorporates traditional EPP and EDR solutions as a single offering, providing continuous monitoring and prevention of endpoint-based activity.

Panda 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.

STRENGTHS

Panda Security's Adaptive Defense product provides a good blend of endpoint protection, endpoint detection and response, and adaptive defense capabilities across a wide breadth of Windows environments, as well as some OS X, Linux and Android variants, at an aggressive price point that will have strong appeal to SMBs.

The automated classification process using machine learning provides real-time or near-real-time analysis of all running executables for suspicious activity. It also provides detailed forensics.

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

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 hybrid of machine learning, cloud database look-up and services to detect the latest threats.

CAUTIONS

Panda 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, the majority of its business remains in Europe.

Mind share is still weak across the broad marketplace, which results in limited RFI/RFP presence within the Gartner client base.

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).

Some of the advanced capabilities rely on cloud access. Untethered systems will operate in hardened or lock mode unless an administrator overrides this setting, until reconnected, which may result in unknown executables being blocked until analyzed and classified.

SentinelOne

Founded in 2013, SentinelOne has had stellar growth in the enterprise EPP market, and expects it to continue for the next couple of years as it maintains a reputation as a leading NGAV vendor. A new $70 million series C funding in January 2017 brings the total to $110 million in equity funding. SentinelOne possesses a strong channel partner program, strong base in U.S. sales and an overall good presence in EMEA, with plans for expansion into Asia.

SentinelOne provides behavior-based anti-malware, anti-exploit and script-based attack protection along with full EDR capabilities as a single, integrated, full-featured endpoint offering, incorporating prevent, detect and respond/remediate capabilities.

Cloud-sourced file blacklist and machine-learning-based static file analysis blocks known threats before they are executed. Multiple behavior-based detection techniques are used to detect suspicious and malicious activity at execution time.

SentinelOne is a good prospect to replace or augment existing EPP solutions for any organization looking for a solution with comprehensive EDR capabilities.

STRENGTHS

SentinelOne has shown strong performance in competitive displacements, even in very large accounts, due to ease of use and a single-agent deployment that provides both EPP and EDR capabilities.

SentinelOne offers on-device dynamic behavioral analysis to detect exploit attempts and fileless malware attacks without relying on traditional signatures, indicators of compromise (IOCs) or whitelisting. Gartner clients remark that this has reduced the number of infections, measured by the number of devices being reimaged following a malware incident.

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

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

CAUTIONS

Although development effort is underway, EPP functionality that is commonly provided by the incumbent EPP providers is missing, such as personal firewalls, URL filtering, USB device control, data protection, vulnerability analysis and reporting, and application control. For the time being, Gartner clients must find alternative providers for the traditional EPP capabilities that are not included.

Gartner clients and references customers have reported a need for greater visibility from the management interface and the type of available reports. While SentinelOne has typically addressed these issues quickly, organizations should ensure their reporting needs will be met as part of their proof-of-concept deployments.

As SentinelOne gains greater market share, Gartner clients and reference customers have reported a need to improve the level of service and support they are receiving from the vendor.

Sophos

Sophos is the fourth-largest EPP vendor by seat count and market share. All of its revenue comes from enterprises, since its consumer products are provided at no cost. The bulk of its sales are nearly evenly split between EMEA and North America, with a specific focus on midsize enterprise deployments.

In 2016, Sophos drove a cloud-first approach with investments in its Central Endpoint product line, which included the release of Sophos Intercept X — a set of signatureless detection and prevention technologies designed to protect against endpoint attacks targeting exploits in applications and operating systems, and to provide specific countermeasures to ransomware. Sophos' marketing campaigns have increased brand awareness, and Gartner clients are increasingly including Sophos as a shortlist vendor.

Buyers looking for cloud-based administration, a unified endpoint and gateway integration, and protection against next-generation threats and ransomware will find Sophos a good fit for both full EPP vendor shortlists and for shortlists of additional protection.

STRENGTHS

Intercept X provides strong exploit mitigation, protecting against both file-based and fileless exploit attempts, and includes CryptoGuard — a behavioral ransomware protection element that allows the recovery of files that were encrypted before ransomware was detected and stopped.

Unique to the group of "classic" antivirus/EPP vendors, Sophos has made Intercept X compatible with any other EPP product so that it can be used to augment solutions that lack exploit mitigation.

The cloud-based Sophos Central administration console is used to manage all aspects of the endpoint protection platform, including encryption and device control for Windows endpoints and servers, Linux servers, OS X endpoints, and Android and iOS mobile devices. In addition, the console manages the Sophos Web, Email and Wireless security offerings.

The Sophos Synchronized Security approach allows endpoints and firewalls to share threat intelligence and context, and can automatically trigger and orchestrate full-system scans, or isolate the endpoint from the network.

CAUTIONS

While the Sophos Intercept X client can augment other vendors' EPP technology, it cannot currently coexist with the on-premises version of Sophos Endpoint Protection. Sophos customers must upgrade to the Central Endpoint platform to get the full benefit of Intercept X including signatureless CryptoGuard and exploit prevention on-premises versions.

At this time, Sophos' cloud-first delivery of security features may leave existing on-premises customers waiting for product enhancements and behind the curve in terms of best available protection.

The Sophos Central Endpoint client does yet not have complete feature parity with the on-premises Endpoint Protection client.

With healthy investments in R&D, Sophos is gaining mind and market share, but has not yet reached the levels of its larger competitors. Its rate of growth, while also strong, is currently being surpassed by new entrants in the marketplace.

Symantec

Even with a generalized decline in growth and revenue in both the consumer and enterprise business (roughly evenly split 50/50) over the past 18 months, Symantec continues to lead the market in EPP revenue and market share.

However, at this time, the overwhelming feedback about Symantec from its client base would be best summed up in one word: fatigue; and specifically fatigue over the near-constant changes in product, company direction and leadership.

As in nearly all previous years, Symantec has yet again embarked on a new strategy fueled by acquisitions (Blue Coat at $4.65 billion and LifeLock at $2.3 billion), which has resulted in yet a newer and bolder vision of what it plans to become over the next 18 to 36 months.

Despite its management challenges, Symantec continues to provide one of the most comprehensive EPP suites available in this market, and to add advanced features like its EDR solution (Advanced Threat Protection: Endpoint) to better address the changing threat landscape. Test scores remain in the top tier.

STRENGTHS

Symantec Endpoint Protection (SEP) 14 introduces multiple forms of machine learning and adds behavioral heuristics as enhancements to its endpoint anti-malware solutions. In this release, Symantec also reduced the footprint of its signature database, and introduces additional streamlining of the endpoint agent for better performance and effectiveness.

Memory Exploit Mitigation in SEP 14 provides virtual patching for endpoints of vulnerabilities in popular software.

Symantec Data Center Security now provides better visibility and security for Docker application containers, as well as self-learning capability for autosandboxing.

SEP 14's Online Network for Advanced Response (SONAR) monitors endpoint processes for lineage, injection and other characteristics. The new version employs a more accurate classifier than in previous versions.

Symantec Risk Insight integrates with SEP 14 and provides a comprehensive view of the risk exposure of the enterprise and extended enterprise, such as its clients, and enforces policies and security protocols for end users.

CAUTIONS

Symantec has been experiencing nearly continuous churn in product direction and management since 2012, resulting in overall client fatigue and belief that a vendor alternative for the EPP programs may be desirable.

Symantec has started to embrace a cloud-first strategy with the introduction of its latest product updates, which are manageable via the cloud-based console.

Symantec's security product portfolio continues to be a mashup of individual solutions that are deployed and managed independently. When compared with new entrants in the EPP market, Symantec is perceived as more complex and resource-intensive to manage than alternatives.

With the need to ingest two very large acquisitions within six months, Symantec will be challenged to integrate technologies and personnel while remaining innovative in this fast-changing and competitive security landscape, where Symantec displacement is a top priority for competitors large and small.

Trend Micro

Trend Micro, the third-largest vendor, again increased revenue over the past 12 months, and is inching ever closer to the No. 2 spot in the EPP market.

Trend Micro is primarily focused on building out its overall enterprise business by growing its reseller and channel presences in North America and Europe, to better complement its very strong presence in its home region, APAC.

Trend Micro is facing stiff competition from other leading and new vendors, and has added new non-signature-based detection to complement its existing signature and behavioral technologies. Although the market is catching up with it on the EPP feature set, it does continue to lead the market in quickly addressing needs specific to the modern enterprise, data center and cloud computing.

Trend Micro remains a very good shortlist candidate for all types of buyers, and offers a unique deployment starting point that includes endpoint, data center and cloud.

STRENGTHS

The OfficeScan XG client provides comprehensive malware protection, and this year's improvements include pre-execution and postexecution detection by new client-side machine-learning technology. This addition also provides detailed analysis information, available within the Trend Micro Control Manager (TMCM) console, explaining the reasons behind a conviction and any comparisons to known malware.

The Vulnerability Protection component provides an easy-to-follow outline of vulnerabilities across all known endpoints, prioritized based on the severity vulnerability, and indicates when devices are "virtually patched" using the HIPS protection in the OfficeScan/XGen client.

The breadth of coverage supplied by Deep Security across endpoints and the data center, with optimized support for VMware, Microsoft Azure and AWS, is appealing to organizations looking to consolidate vendors.

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.

CAUTIONS

Trend Micro's fast growth is leading to client support issues. Gartner clients have increasingly reported concerns with customer support responsiveness and inconsistent experiences with an ever-growing reseller network over product knowledge and support expertise. This has caused some clients to migrate to alternate vendor solutions.

Trend Micro does not support application control, device control or DLP for OS X devices, which leaves groups of endpoints with different levels of protection.

The Endpoint Sensor client relies on the OfficeScan client for remediation and containment actions when new malicious files have been detected, which includes isolating an endpoint using firewall policy, quarantine malicious files and block process execution.

Webroot

Webroot's strong double-digit business growth over the past 12 months was driven by its success with the Managed Security Provider partnerships selling its endpoint solutions. However, the consumer market continues to represent a significant majority of its total deployed seat count.

Webroot SecureAnywhere Business Endpoint Protection uses a combination of machine learning, behavior analysis and contextual threat intelligence to protect users from known and unknown threats, while keeping its EPP client small with low impact on users.

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.

Webroot is well-known for its OEM relationships with third-party security technology providers that leverage its threat intelligence, which includes URL, file and Internet Protocol (IP) address reputation, and anti-phishing.

STRENGTHS

Webroot's solutions continue to have high satisfaction scores, and are reported by clients as providing a good blend of ease of management and effective protection from various threat vectors.

Flexible licensing does not differentiate between endpoints, physical servers, virtual servers or cloud.

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.

The vendor also offers security and basic EMM capability, including a mobile app reputation services for Android and iOS devices from within the same management console.

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, nor endpoint management utilities, such as vulnerability or patch management.

Advanced protection capabilities rely on cloud access. Untethered systems will operate in hardened or lock mode until reconnected, which may result in unknown executables being blocked until analyzed and classified.

Both the endpoint security consoles and the new Global Site Manager management consoles are cloud-based, with no on-premises server requirement, which may not be appropriate for all client environments.

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

AhnLab, Carbon Black, CrowdStrike, G Data Software, Invincea, Malwarebytes, Palo Alto Networks

360 Enterprise Security Group was formerly known as Qihoo 360

Dropped

The following vendors were not included in this report, as all license their primary anti-malware engine from other vendors. The inclusion criteria this year was changed such that the primary engine needed to be owned and developed by the company:

Check Point Software Technologies

Heat Software

IBM

Landesk

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 and is developed by the company itself

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 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 evaluated 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 evaluated vendors by their market share in total customer seats under license.

Marketing Execution: We evaluated 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 evaluated 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

Evaluation Criteria	Weighting
Overall Viability	High
Sales Execution/Pricing	Medium
Market Responsiveness/Record	High
Marketing Execution	Medium
Customer Experience	High
Operations	Medium

Source: Gartner (January 2017)

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.

Innovation: We evaluated vendor responses to the changing nature of customer demands. We accounted for how vendors reacted to new threats, 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

Evaluation Criteria	Weighting
Vertical/Industry Strategy	Not Rated
Innovation	Medium
Geographic Strategy	Low

Source: Gartner (January 2017)

Quadrant Descriptions

Leaders

Leaders demonstrate balanced progress and effort in all execution and vision categories. They have broad capabilities in advanced malware protection, and proven management capabilities for large enterprise accounts. 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. Leaders tend to be more cautious and only gradually react to the market when Visionaries challenge the status quo.

Challengers

Challengers have solid anti-malware products that address the foundational security needs of the mass market, and they have stronger sales and visibility, 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 and 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. Most visionaries are complementary solutions. That is, they do not necessarily need to replace the incumbent EPP and can coexist on the same machine.

Niche Players

Niche Players offer solid anti-malware solutions but rarely lead the market in features or function. Some are niche because they service a very specific geographic market. Niche Players are often a good choice for conservative organizations in supported regions.

Context

The EPP market is heating up again, as new entrants challenge the old-guard signature vendors. Leaders continue to dominate the market, but several Visionary vendors are rapidly gaining market share. The Visionary vendors are challenging the old guard with easy-to-use products that generally perform better and are more effective at catching new variants of threats. Most of the Visionary vendors are still considered "complementary," meaning they can be added to a machine without displacing the traditional EPP solution in place. Indeed, we estimate that 90% of Visionary products are running in tandem with other solutions. Roughly, 6% of organizations are now running with two solutions. However, as confidence in the Visionary vendors is increasing, we are starting to see complete displacements. Concurrently, the old guard is starting to innovate or acquire new technology.

Given the rapid pace of innovation, EPP administrators should upgrade to latest version as soon as practical. We also recommend EPP admins get a configuration policy checkup with their incumbent vendor to ensure the most effective protection features are enabled.

Lean-forward security organizations should consider investing in a complementary solution for added protection.

Early adopter organizations may consider replacing EPPs completely with a Visionary vendor, but should be aware of the limitations of the new solutions. Most do not have the totality of EPP features, such as personal firewalls, USB port protection, data protection, application control, vulnerability detection or EMM. Moreover, most of the Visionaries only have one or two detection techniques, which makes them lightweight and easy to use; however, this will also make them vulnerable to the inevitable evasion attacks that come with large market share.

Market Overview

Critical capabilities of EPP suites have narrowed considerably to three primary concerns: malware detection effectiveness, [2] performance impact on host machines and administration overhead.

Standardized testing, such as AV comparatives and AV tests, are still the best indicators of effectiveness; however, they still overreward reactive solutions and undertest detection of new attacks. In the real world, malware detection effectiveness of EPP solutions continues to lag the changing attacker techniques. With the exception of some of the emerging Visionary vendors, too many EPP solutions' malware detection techniques remain overly reliant on reactive indicators of compromise (i.e., IP address, URL, file hash, partial hash, registry key values). These static indicators are the easiest part of the kill chain for the attackers to change rapidly.

Several emerging vendors are demonstrating that non-signature-based protection can be more effective against rapidly changing threats. However, their claimed real-world success is not reflected in standardized tests, making improvements difficult to quantify. Emerging vendors have fewer protection techniques than traditional vendors, and it is not clear that they would remain effective if attackers devoted more time to finding product flaws. Concurrently, established EPP vendors are responding by adding more proactive techniques to their malware detection funnels. As a result, most buyers consider emerging solutions to be complementary, rather than outright EPP replacements, at least for now (see also "The Real Value of a Non-Signature-Based Anti-Malware Solution to Your Organization").

Most attacks exploit well-known unpatched vulnerabilities, use social engineering to trick users to install trojan malware, or use interpreted code such as Java or Visual Basic to download and install malware. Comprehensive patching programs and application control remain extremely effective measures to thwart all three common malware attack techniques, and leading EPP solutions are adding them as preventative strategies. However, these proactive measures require more administration overhead, consequently they have failed to gain widespread adoption. Vendors are responding to this dilemma by containing unknown code and automating the classification process to streamline the change control process.

The next wave of attacks will be fileless. Advanced attackers have been exploiting script-based attacks for years. Common Windows utilities, such as the command line interface, PowerShell, Pearl, Visual Basic, Nmap and Windows Credential Editor, can be exploited to compromise machines without dropping any executable files, evading all traditional forms of malicious file detection. We are starting to see malware authors experimenting with mass-propagating fileless malware using the same techniques. As a result, EPP buyers should look for vendors that focus on memory exploit protection, script analysis and behavior indicators of compromise. Ultimately, we believe that vendors that focus on detecting behavior indicative of attacker tradecraft (that is, tools, tactics and techniques) will be the most effective.

The modern data center is changing rapidly with the introduction of virtualization, cloud infrastructure, and now agile application development and containerization. A few of the EPP vendors are keeping pace with these rapid changes, but we expect this will be an area for new vendors to disrupt the old approaches (see "Security Considerations and Best Practices for Securing Containers" and "Market Guide for Cloud Workload Protection Platforms").

More EPP vendors are adding EDR capabilities to improve detection of more advanced threats. Integrated EDR functions can provide an early warning that threats have bypassed malware detection, as well as an invaluable tool for investigating alerts and recovering. Integrated EDR capability can be a valuable option, but mature IT organizations must consider the overall strength of the EDR solution, versus the slight advantage of integration with EPP (see "Market Guide for Endpoint Detection and Response Solutions").

Data protection features, such as encryption and DLP, are common among EPP solutions. Again, the quality of the products must be weighed against the value of integration. Only one vendor has integrated threat protection and data protection in a meaningful way beyond reporting and deployment ease.

Mobile protection is also branching from traditional laptop/desktop protection. Mobile protection is primarily a configuration and management problem controlled by EMM solutions. Several EPP solution providers offer integrated EMM solutions; however, large enterprises often prefer stand-alone EMM solutions (see "Magic Quadrant for Enterprise Mobility Management Suites").

Lastly, several new vendors have received unprecedented levels of super-funding from venture capital firms, with several at levels topping out at nearly $200 million. This reflects the new nature of the EPP market, and a pent-up desire by the market to find viable alternatives to incumbent solution providers. It also can become a significant distractor to smaller firms focusing on hypergrowth.

Organizations considering EPP solutions need to assess their current and future needs, and evaluate the overall viability of any solution in their shortlist.

Evidence

[1] Gartner conducted an online survey of 115 EPP reference customers in 4Q16.

[2] 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/) .

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.

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.

covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "Guiding Principles on Independence and Objectivity. (/technology/about/ombudsman/omb_guide2.jsp)"
