Magic Quadrant for Endpoint Protection Platforms

Published: 24 January 2018 **ID:** G00325704

Analyst(s): Ian McShane, Avivah Litan, Eric Ouellet, Prateek Bhajanka

Summary

Endpoint protection is evolving to address more of Gartner's adaptive security architecture tasks such as hardening, investigation, incident detection, and incident response. Security and risk management leaders should ensure that their EPP vendor evolves fast enough to keep up with modern threats.

Strategic Planning Assumption

By 2021, endpoint protection platforms (EPPs) will provide automated, orchestrated incident investigation and breach response. Separate, stand-alone endpoint detection and response (EDR) solutions will focus on managed security service provider (MSSP) and large enterprise security operations center (SOC) environments.

Market Definition/Description

In September 2017, in response to changing market dynamics and client requirements, we adjusted our definition of an EPP. An EPP is a solution deployed on endpoint devices to prevent file-based malware, to detect and block malicious activity from trusted and untrusted applications, and to provide the investigation and remediation capabilities needed to dynamically respond to security incidents and alerts. (see "Redefining Endpoint Protection for 2017 and 2018").

Organizations are placing a premium on protection and detection capabilities within an EPP, and are depreciating the EPP vendors' ability to provide data protection capabilities such as data loss prevention, encryption or server controls. Security buyers are increasingly looking to the built-in security capabilities of their OS vendors, and most organizations are adopting disk encryption at the OS level with BitLocker in Microsoft Windows 10, and FileVault in Apple macOS.

Concurrently, protection for servers has diverged from EPP, with specialized tools to address the modern hybrid data center (cloud and on-premises; see "Market Guide for Cloud Workload Protection Platforms"). Gartner recommends that organizations separate the purchasing decisions for server workloads from any product or strategy decisions involving endpoint protection. The evolutionary shift from hardware servers to VMs, containers and private/public cloud infrastructure means that server workloads now have different security requirements compared to end-user focused, interactive endpoints (see "Endpoint and Server Security: Common Goals, Divergent Solutions").

This is a transformative period for the EPP market, and as the market has changed, so has the analysis profile used for this research. In the 2017 Magic Quadrant for Endpoint Protection Platforms, capabilities traditionally found in the EDR market (see "Market Guide for Endpoint Detection and Response Solutions") were considered as "nice to have" features. In this 2018 research, some of these features are now core components of an EPP that can address and respond to modern threats.

Magic Quadrant

Figure 1. Magic Quadrant for Endpoint Protection Platforms

Source: Gartner (January 2018)

Vendor Strengths and Cautions

Bitdefender

Bitdefender provides good effectiveness across a broad range of platforms and capabilities. Bitdefender offers EPP and EDR in one platform, and one agent across endpoints, and physical, virtual or cloud servers.

While a large part of the installed base is in the consumer segment, the gap between enterprise and consumer business is narrowing. Bitdefender is a good choice for organizations that value malware detection accuracy and performance, as well as full support for data center and cloud workloads from a single solution provider. Bitdefender is also a partner for Microsoft's Defender Advanced Threat Protection (ATP) platform, providing agents for Linux and macOS.

The vendor continues to round out its endpoint features for larger enterprises, and its brand awareness is low, impacting its execution. Bitdefender's cloud-based, single-agent approach; large installed base; and recently released EDR module keep it relevant in this space.

STRENGTHS

Bitdefender's detection technology is well-regarded and performs well in third-party tests. The vendor has a long list of technology and service providers that use its detection capabilities as OEMs.

Bitdefender is noted by clients for ease of use, deployment and customer support, and in particular for its vision of single agent and single console (released in November 2017), providing a fully integrated EPP and EDR solution.

Patch management capabilities provide detailed information from the Common Vulnerability and Exposure (CVE) repository, and event severity, helping IT operations to prioritize updates and understand risks.

Bitdefender has partnered with Microsoft to provide protection to macOS and Linux systems in a Microsoft Windows Defender EPP environment, and will integrate with the Windows Defender ATP platform.

CAUTIONS

While the macOS agent does benefit from machine learning (ML)-based detection instead of the normal substandard signature-based detection typically used for macOS, it does not report EDR data, leaving a visibility gap for most organizations.

The Bitdefender EPP agent lacks basic investigation capabilities like real-time indicator of compromise (IOC) searching.

There are no options for orchestration or automation with security operations, analytics and reporting (SOAR) tools.

While Bitdefender has invested in growing its enterprise sales operations, mind share remains low with larger enterprises, thereby limiting shortlist opportunities and apparent viability to larger clients.

Carbon Black

Carbon Black is in the middle of a significant corporate transition, consolidating its overall offerings into a new cloud-based security platform called Predictive Security Cloud. The company's overall offerings consist of Cb Defense (EPP), Cb Response (threat hunting and incident response), and Cb Protection (application whitelisting and device lockdown). Carbon Black began to consolidate EDR features from Cb Response into Cb Defense in 2017 as it started to build a presence in the EPP market.

Carbon Black has earned a strong reputation as offering one of the leading EDR solutions in the marketplace. Cb Response (threat hunting) is typically found in more complex environments with very mature security operations teams. The Cb Defense agent collects and sends all the unfiltered endpoint data to the cloud using a proprietary data streaming mechanism that eliminates bursting and peaks on networks.

The majority of Carbon Black clients make tactical purchases, usually a one-year subscription with options to renew at the end of the term.

Carbon Black is in the Visionaries quadrant this year, but Cb Defense is still unproven, which impacts its execution. The vendor has a poor record of participation in public, independent malware accuracy and effectiveness testing, which impacts its vision and execution in this assessment.

STRENGTHS

Carbon Black provides an advanced toolset that has broad appeal with organizations that have mature security operations teams consisting of high-caliber and very experienced personnel.

Carbon Black's Cb Defense solution incorporates a blended approach consisting of signatures, ML, software behavior monitoring, process isolation and memory protection, along with exploit prevention.

Carbon Black's updated and streamlined console offers advanced administrators simplified views of threats via visual alerts and triage, resulting in faster detection and response.

Carbon Black's rich set of APIs and broad third-party partner ecosystem provide opportunities for mature SOCs to integrate Carbon Black findings into a diverse set of analysis, workflow and case management solutions.

CAUTIONS

Clients that have not yet moved to Carbon Black's cloud-based EPP and EDR product (Cb Defense) continue to report that they are struggling with the operational complexity of their Carbon Black deployments.

Some advanced prevention features such as cloud detonation and hash look-ups require online access to the Carbon Black cloud infrastructure, reducing the effectiveness for devices without a permanent connection to the internet.

Carbon Black has not yet integrated its threat hunting module from Cb Response or its application whitelisting capabilities from Cb Protection into its cloud-based platform, so customers that require those features will need separate agents and separate management

consoles.

Carbon Black continues to be at the premium end of cost per endpoint in terms of cost to acquire and cost to operate, especially if organizations require the EPP and the separate application whitelisting capabilities provided by Cb Protection.

Carbon Black has continued to favor private or sponsored malware accuracy and effectiveness tests of its product and has had a poor record of consistent participation in public tests in 2017. Consequently, it is difficult to determine its efficacy versus peers.

Cisco

Cisco's Advanced Malware Protection (AMP) for Endpoints is a new entrant to this year's Magic Quadrant. It consists of prevent, detect and respond capabilities deployed as a cloud-managed solution that can be hosted in a public or private cloud.

Cisco's AMP for Endpoints leverages similar technology to the AMP capabilities on other Cisco devices. Its AMP Cloud technology detects known threats, and uses threat intelligence data from Threat Grid and Talos security researchers for exploit prevention.

Gartner clients rarely shortlist AMP for Endpoints for its technology, usually because they get a strong financial incentive when purchasing other Cisco products. Although a component of AMP for Endpoints is present in VirusTotal's public interface, it did not participate in public endpoint-focused third-party testing in 2017, which impacts its execution and vision in this assessment.

Cisco's AMP solution has the most appeal for existing Cisco clients that leverage other Cisco security solutions and aspire to establish security operations around Cisco products.

STRENGTHS

The main strength of Cisco AMP is in threat intelligence and exploit prevention as a means of reducing the attack footprint available for compromise.

The Cisco AMP agent for Windows and macOS both collect process and usage data, providing EDR coverage and visibility for the most popular devices in enterprises.

Cisco offers a broad range of managed services, including SOCs, managed detection and response, active threat hunting, and incident support.

Reporting integration and data sharing between AMP and other Cisco security offerings, such as network, firewall, NGIPS, routers, email gateway and web proxies, are improving.

CAUTIONS

Cisco is, first and foremost, a network security and hardware vendor, and originally exited the endpoint protection market in 2010 when it discontinued the Cisco Security Agent (CSA) product before gaining the AMP technology through the acquisition of Sourcefire.

Advanced malware protection requires access to the Cisco AMP Cloud to perform advanced analysis.

While the data provided across the dashboard is relatively comprehensive, the workflow requires multiple clicks to multiple screens to get a full understanding of the state of an endpoint or the issues being caused by malicious software.

The Cisco workflow provides limited role-based access, and limited case management capabilities.

Cisco's AMP solution is part of a "better together" product ecosystem. Organizations that do not leverage other Cisco security solutions will realize fewer of the integration benefits, such as intelligence sharing and automated blocking of new threats at all control points.

Cisco AMP has not been tested widely in public, independent tests to determine its efficacy versus peers.

Comodo

The Comodo brand is best-known as a digital certificate authority and, in late October, Francisco Partners acquired a majority stake in Comodo's certificate authority business, with Comodo planning to focus on its endpoint protection strategy.

Comodo Advanced Endpoint Protection (AEP) includes malware protection, a host-based intrusion prevention system (IPS), web filtering, a personal firewall, sandbox analysis, vulnerability analysis and patching, and a 100% classification capability that helps guarantee a good or bad verdict on all executable files. When an executable is untrusted or unknown, it is run in a tightly controlled container to isolate any potentially malicious activity.

Comodo also sells small or midsize business (SMB)-focused web gateways, web application firewalls and mobile device management. Its security products are managed from a central web-based portal that manages service request ticketing and workflow.

STRENGTHS

Comodo AEP is best-known for its default deny approach, where unknown applications and executables are wrapped in secure, isolated containers, and known bad applications are blocked.

Comodo is showing sales strength and technical scalability as it starts making progress with a handful of global companies with more than 100,000 seats.

Comodo provides managed endpoint protection, detection, response and remediation services through integration with the cloud-based IT and Security Manager, and its patch, device, and asset management capabilities.

Comodo's Valkyrie file verdict system is focused on file analysis, and its cloud-based threat intelligence and analysis platform benefits from intelligence gathered from Comodo customers, honeypots, crawlers and partners.

Gartner clients report that AEP is easy to deploy and use, and that Comodo implementation support is very responsive. Support for end-of-life OSs, (e.g., Windows 2003) is good as well.

CAUTIONS

The solution depends on its autocontainment capability to prevent attacks, and detection is limited to known indicators of compromise (IOCs).

Gartner clients report that the Linux product is lacking in functionality, with ineffective detection and no central management or monitoring capabilities.

According to Gartner clients, it takes too much time to tune the AEP engine to accept custom applications. This is a common scenario with application control.

Comodo's new EDR product, cWatch EDR, is available for free, but has not been proven by organizations using EDR for advanced threat hunting and self-driven threat analysis. Event recording is limited, and detection is mainly based on IOC and indicators of attack (IOA) scanning.

cWatch EDR lacks automated remediation and incident response, but some of these capabilities are included in Comodo AEP itself.

CrowdStrike

CrowdStrike made strong progress in 2017 and managed to replace incumbent legacy EPP vendors at large organizations. With 79% of its business in North America, CrowdStrike has deployments in 176 countries and includes some very large organizations with more than 50,000 seats.

CrowdStrike Falcon's lightweight single agent supports all environments (physical, virtual and cloud) and functions with the same agent and management console for Falcon Prevent protection and Falcon Insight EDR. With its EDR heritage, CrowdStrike records most endpoint events and sends all recorded data to its cloud for analysis and detection. Some prevention is done locally on the agent.

Alongside EPP and EDR capabilities, CrowdStrike offers a complementary service called Falcon OverWatch, at an attractive price point, leading to extremely high adoption among its installed base. Falcon OverWatch provides managed threat hunting, alerting, response and investigation assistance.

Organizations with small or no SOC teams will find the combination of Falcon OverWatch and Falcon Endpoint Protection compelling. CrowdStrike also offers a well-respected breach response service.

STRENGTHS

Gartner clients report simple and easy Falcon deployments, in part due to the cloud architecture.

Ninety-eight percent of Falcon customers use CrowdStrike's Falcon OverWatch managed detection and response service, which provides varying levels of service to suit varying customer requirements. If appropriate, CrowdStrike can manage Falcon deployments, incident response and remote remediation services, which is especially attractive to smaller organizations.

Falcon uses a range of detection and prevention tools centered around behavioral analytics that essentially implement a "deny malicious behavior" policy. Falcon analytics enable very specific response capabilities, depending on the severity of malicious behavior.

CrowdStrike's cloud-based architecture provides an extensible platform that enables additional security services like IT hygiene, vulnerability assessment and threat intelligence. Its EDR and EPP functionalities are well-integrated.

CrowdStrike's Falcon Insight EDR agent provides parity across Windows, macOS, and Linux systems, providing a solid visibility base for most organizations.

CAUTIONS

CrowdStrike does not have an integrated deployment solution, but it does work well with third-party tools.

The full product is more expensive than other EPP solutions, but includes the OverWatch service, and covers the costs of cloud data storage for EDR.

CrowdStrike Falcon's offline protection is greatly enhanced when connected to the cloud-based Falcon platform, so is not suitable for air-gapped networks.

Like most other EDR platforms, Falcon's EDR functionality requires skilled technical staff to use, which is why CrowdStrike's OverWatch service is so popular with customers.

Customers report that CrowdStrike's roadmap is not proactively communicated in a timely manner.

Cylance

Cylance was one of the pioneers in using machine learning to detect file-based malware, but by 2017, most EPP competitors claimed to have added ML capabilities, pressuring Cylance to more aggressively address non-file-based attacks. In late May 2017, Cylance formally launched its EDR product, CylanceOPTICS, which was late to market compared to other vendors, and generally perceived to be lacking in advanced capabilities already available in key competing products.

Eighty-five percent of Cylance's business is in North America, although the company has about 3,700 customers across the globe, half of which represent organizations with fewer than 500 seats.

CylancePROTECT is cloud-based, with Cylance hosting and managing the console infrastructure directly. The vendor finally started participating in the VirusTotal community in 2017, but has a poor third-party test participation record when compared with established EPP vendors.

STRENGTHS

Cylance has a strong OEM business, with over half of its licensed seats sold through its OEM relationships, including Dell. It also launched an MSSP partner program in 2017 and onboarded 70 new MSSPs.

Aside from Windows, Cylance supports macOS, Linux and virtual environments.

Gartner clients report a good experience, effective customer support, and effective malware and ransomware protection.

CylancePROTECT has a small footprint and easy-to-use management console, with low maintenance support requirements.

CylancePROTECT runs effectively in offline mode and doesn't require a connection to the internet to remain effective.

CAUTIONS

Administrative functions in Cylance's management console need to be more fully developed, according to Gartner clients, in order to more easily manage several features, such as device and script control.

The aggressive ML capabilities prove very good at detecting new versions of known malware. As with any ML-based technology, however, it can be gamed by malware authors, and Gartner clients report that it can have a high false-positive rate. The lack of cloud-based look-ups hampers the vendor's ability to quickly resolve false positives, leaving the customer to manage the exclusion of false positives themselves, until the vendor is able to push out a client-side rule update (which it calls Centroids), before ultimately updating the ML model.

CylancePROTECT and CylanceOPTICS require two separate agents with two separate installations.

EDR functionality does not enable automated rollback. The UI and data captured in CylanceOPTICS is not robust enough for advanced threat hunting. Its InstaQuery only provides information from devices that are online.

Cylance lacks adjacent security applications, such as inventory of installed applications, IT hygiene assessments and vulnerability assessments, but does benefit from API integrations with some SOAR and security information and event management (SIEM) providers.

Custom applications, or applications that have not been analyzed by Cylance, may generate false positives, thereby requiring organizations to establish a whitelisting process when they release new builds of the custom application. As previously noted, once the false positive has been analyzed, Cylance's Centroid technology will push out a new client-side rule update to mitigate the false positives until they are included in the next ML model.

Endgame

Endgame is a new entrant to the Magic Quadrant this year. It is a privately held organization that has evolved from pure EDR for large enterprise and defense organizations, with the addition of prevention capabilities for the broader enterprise market.

Endgame is one of the few vendors in this analysis that sells a single product offering — meaning there are no additional add-ons or purchases — to address protection, detection and response use cases.

Although the platform is missing a number of traditional EPP-related features, like application control or suspicious file quarantining, Endgame scores well in protection capabilities by focusing on the tools, techniques and procedures used by adversaries, rather than simply looking for bad files.

Endgame's big differentiator is in its investigation and threat hunting capabilities, where natural-language understanding (NLU) queries, such as "Search for PowerShell" and "Find NetTraveler," allow organizations to make use of advanced detection capabilities without the need for deep experience.

Endgame is a good EPP shortlist candidate for organizations with an existing or emerging SOC where incident investigation and response is a key requirement.

STRENGTHS

The platform scales to very large deployments, and still performs fast, real-time investigation actions.

It lowers the barrier to entry for advanced capabilities like threat hunting, allowing less experienced security staff to begin, and often complete, investigation work.

Endgame has been evaluated against the Mitre ATT&CK matrix, which evaluates where in the kill-chain the product's capabilities are designed to prevent attacks.

Endgame's platform can function in a fully offline mode, with no internet required.

The agent utilizes hardware assistance (called HA-CFI), detecting in-memory exploit attempts by looking for abnormal behavior in the CPU register. However, this detection technology is not available when Endgame is deployed in a virtual environment, reducing the effectiveness to only DBI-based detection on those devices.

CAUTIONS

No application control capabilities are provided in the agent.

Despite deploying an agent to every endpoint, there is no vulnerability reporting, which leaves a disconnect and creates additional work for both IT operations and security.

Files cannot be temporarily quarantined, and are deleted if they are deemed malicious; however, false positives can be recovered and restored from the management console as samples are collected for further analysis.

There is currently no macOS agent for protection or EDR, leaving a gap in visibility for most organizations.

ESET

ESET has a strong EPP market share among SMBs to large enterprises, providing solid protection with a lightweight agent. But it still manages to provide a large protection stack, including a host-based intrusion prevention system (HIPS), ML, exploit prevention, detection of in-memory attacks and ransomware behavior detection.

ESET recently launched an additional platform for EDR capabilities, called Enterprise Inspector. Customers with experienced security staff will be able to inspect and modify the detection rules within Enterprise Inspector, and further tailor them to their unique requirements.

ESET has significant security community mind share through published research, disruption of organized crime and its WeLiveSecurity website. The vendor's completeness of vision is impacted in this assessment by its limited cloud management capabilities, and the relative lateness of its EDR capabilities.

ESET has localized support in 35 languages, which means it is an attractive choice for globally distributed organizations. Its protection capabilities make it a solid shortlist candidate for any organization.

STRENGTHS

Despite the low overhead from its lightweight client, ESET's anti-malware engine remains a consistently solid performer in test results, with a strong protection stack.

ESET has a comprehensive set of capabilities that incorporate operational IT into the protection and detection stack.

Managed EDR features delivering threat hunting and attack detection were recently made available to customers.

Customers can take advantage of free implementation services in some countries, reducing the burden of migrating from another vendor.

CAUTIONS

Cloud-based management options are limited to Microsoft Azure or Amazon Web Services (AWS) instances, rather than a true SaaS platform. These instances can be customer self-managed, managed by a managed service provider partner or managed by ESET for North American customers.

Although ESET's endpoint agent implements exploit prevention and in-memory scanning for attacks, there is no vulnerability discovery or reporting capability. These capabilities are supplied through ESET's partner ecosystem.

ESET does not include application whitelisting or system lock-down capabilities in its endpoint agent; instead, applications and executables are blacklisted by file hash or through HIPS control policies.

The ESET macOS agent does not support real-time IOC search and does not integrate with EDR, leaving a visibility gap for many organizations.

The role-based administration within ESET Enterprise Inspector only allows two user modes (administrator and end user), meaning larger organizations with defined escalation paths may find implementation challenging, due to the lack of case and incident management workflow within Enterprise Inspector.

FireEye

FireEye, a new entrant to this Magic Quadrant, is a security suite vendor that provides email, web, network, endpoint security and threat intelligence, which are managed in the new Helix security operations platform launched in April 2017.

FireEye revenue from its HX Series endpoint security product is a relatively small portion of the vendor's overall business. The HX management console is deployed through the cloud or as a virtual or on-premises hardware appliance that supports up to 100,000 endpoints. FireEye's HX endpoint security agent is installed on 9 million endpoints globally, with over 70% of customers in North America and 15% in EMEA. FireEye's appeal to Gartner clients is as a security suite and not as a best-of-breed endpoint security vendor.

FireEye Endpoint Security 4.0 shipped in late September 2017; therefore, market response to FireEye's endpoint protection capabilities was limited during this research period. FireEye met the inclusion criteria by participating in its only public third-party test in late 2017, which impacts both vision and execution in this assessment.

STRENGTHS

In 2017, FireEye HX added support for macOS and Linux hosts, cloud and hybrid management; bolstered prevention via an OEM signature-based AV component; and increased behavior analysis and exploit prevention.

HX customers that use Helix have 30 days of endpoint data stored in the cloud by default, and this can be configured for up to one year's worth.

HX benefits from threat intelligence from Mandiant's breach investigation team and iSIGHT Threat Intelligence service, as well as from FireEye products' shared threat indicators.

FireEye offers a global managed detection and response service, FireEye as a Service, to help clients that are short on resources.

CAUTIONS

Most of the EDR data is stored on the endpoint, with a subset stored on the HX server and, if enabled, in the cloud with FireEye Helix. Incident responders may not be able to perform a full root cause analysis involving compromised endpoints that are offline, or, as in the case of ransomware, have had their data encrypted.

A few Gartner clients report that HX produces high false-positive rates when the product is first implemented.

FireEye's cloud-based management offering was new in 2017, and uptake was small at the time of this research.

Manual remediation capabilities are restricted to endpoint containment, and there is no support for automated configuration rollbacks or file restoration.

At the time of this research, FireEye HX has not been tested widely in public, independent tests to determine its efficacy versus peers.

Fortinet

Fortinet is a network security suite vendor that sells enterprise firewalls, email security, sandbox, web application firewalls and a few other products, including its FortiClient endpoint security software. The vendor is a new entrant to this Magic Quadrant. FortiClient is not well-known to most Gartner clients inquiring about endpoint security, and we see little adoption of it outside of Fortinet's client base. FortiClient is becoming more focused on the enterprise space, but its current installed base is mostly in the SMB space, and about half of its customers have less than 1,000 seats installed.

In 2017, FortiClient generated less than 1% of the vendor's revenue. Its track record of endpoint-focused third-party testing is poor, and this impacts its execution and vision in this assessment.

STRENGTHS

The FortiClient EPP agent has four customizable modules that include components designed to work in conjunction with Fortinet products, including FortiGate (firewall), FortiSandbox, FortiMail, FortiWeb and others. It can be a good choice if an organization wants to consolidate its solutions with a network security suite vendor, rather than take a best-of-breed approach.

FortiClient is easy to deploy and easy to manage.

Patch management is part of the FortiClient application, which also benefits from FortiGuard Labs global threat intelligence and native integration with its sandbox.

FortiClient quarantines objects and kills processes in real-time using client-side analysis and, if present, based on the FortiSandbox verdict.

Fortinet's FortiGate firewall is a Leader in Gartner's Magic Quadrant for Enterprise Network Firewalls, enabling the vendor to leverage its good reputation to sell its FortiClient EPP application.

CAUTIONS

Along with the lack of independent, third-party testing to validate the accuracy and effectiveness, Gartner clients report that FortiClient needs to improve on the malware protection it affords.

The management console needs to be more customizable, according to Gartner clients.

FortiClient, together with FortiSandbox, only provide partial EDR coverage. Full EDR recording is not provided.

Although FortiClient includes a signatureless anti-exploit engine, the primary malware protection engine is based on rules and signatures. As such, it has more difficulty detecting unknown malicious operations and malware and zero-day attacks without the other components of Fortinet's Advanced Threat Protection solution.

As a successful network security suite vendor, Fortinet is likely to continue focusing its R&D efforts on the interactions and interdependencies of its various suite modules. Without a focus on the EPP market, FortiClient is likely to be slow to develop into a complete and self-contained endpoint protection solution.

F-Secure

In 2017, F-Secure continued with its long track record for high-accuracy, lightweight and low-impact anti-malware detection with its cloud-based F-Secure Protection Service for Business (PSB) offering and on-premises solution F-Secure Business Suite. F-Secure added an integrated password manager with password protection capabilities and improved device control management to PSB and Business Suite. F-Secure also added ML capabilities to its Rapid Detection Service, which is its managed EDR solution.

Over the past 12 months, F-Secure further enhanced its product deployment and management capabilities, making it a good choice for larger, more complex enterprises.

F-Secure is focusing its investments in its managed service offerings, and has added product enhancements with a specific focus on preventing ransomware attacks.

STRENGTHS

F-Secure is unique in that it works with a very rapid iteration, agile development process, with a release update every two weeks. This small update approach allows it to automate much of the agent update process, and adapt rapidly to new threats and attack techniques.

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.

DataGuard, a new ransomware protection capability, provides advanced protection of sensitive local and network folders by preventing modification, tampering or encrypting from unauthorized applications and users.

Patch management capabilities are integrated in the endpoint client (on-premises and cloud) and offer automation capabilities via the management console to keep endpoints up to date. This reduces the complexities associated with traditional distinct patching processes.

Clients report that F-Secure's Rapid Detection Service provides strong security specialist review, analysis and response capabilities.

Clients report that the F-Secure EPP solution is easy to deploy and maintain.

CAUTIONS

F-Secure's EDR offering is still evolving, and is primarily designed as a managed service called Rapid Detection Service. Organizations looking for a hands-on investigation tool will notice missing features in the current version that are found in competitive offerings, such as global process and application inventory.

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

F-Secure has a healthy focus on malware detection effectiveness, but it has not delivered some common protection and detection techniques available in most competitive solutions. There is no application control, application whitelisting or network-based malware sandboxing capability. This reduces the appeal of F-Secure to organizations looking for a broad baseline of protection capabilities.

Despite a strong brand name, the majority of F-Secure clients are sub-5,000 seats, and it is unclear how well the cloud management and investigation platform scales for larger organizations.

Kaspersky Lab

Kaspersky Lab's "built not bought" approach has provided good integration and allows for a strong approach to managed services. The vendor is late to market with EDR capabilities, and has no vendor-managed, SaaS-type cloud-based management options for organizations with more than 1,000 endpoints to manage.

The vendor's research team makes up one-third of the organization, and is well-known for its accurate malware detection and in-depth investigation and analysis of many sophisticated attacks.

Kaspersky Lab has been the subject of media scrutiny, citing unnamed intelligence sources, claiming that Kaspersky's software was being used by the Russian government to access sensitive information.

While the U.S. government has issued a ban on the use of Kaspersky software by government agencies, the U.S. government has not given any evidence that Kaspersky software has been used by the Russian government to gain sensitive information. It has also not demonstrated that Kaspersky software is more vulnerable (technical or otherwise) than any other vendors' antivirus software. Kaspersky filed an appeal in U.S. federal court in late 2017, asking that the government ban be overturned.

From a technology and malware prevention perspective, Kaspersky Lab remains a good candidate as a solution for any organization that is not constrained by U.S. government recommendations. Despite the media stories surrounding Kaspersky Lab, it continues to grow its endpoint presence globally.

STRENGTHS

Kaspersky Lab is a consistent top performer in public, third-party AV tests.

The Kaspersky agent and management console provides detailed vulnerability reporting and prioritization, and the ability to automate the deployment of patches.

A semiautomated IOC search within the new EDR capabilities can take advantage of open IOC format files, making initial threat assessments fast and repeatable.

Kaspersky Managed Protection and Targeted Attack Discovery are fully managed threat detection services that will be attractive to organizations without a dedicated SOC.

Kaspersky R&D continues to publish more public reports on sophisticated attacks and threat actor investigations than any other vendor.

CAUTIONS

Gartner clients report that the management console, Kaspersky Security Center, can appear complex and overwhelming, especially when compared to the fluid, user-centric design of newer EPP and EDR vendor management consoles.

The mainstream EDR capabilities were introduced into the Kaspersky Anti Targeted Attack Platform in late 2017, one of the last vendors to begin adding these features.

The EDR investigation lacks step-by-step, guided investigations for less experienced organizations, but Kaspersky Lab can provide training on using its products for advanced topics like digital forensics, malware analysis and incident response.

The Kaspersky Endpoint Security Cloud — a cloud-based management solution — is currently available only for SMB customers. Larger organizations looking for cloud-based management must deploy and maintain the management server in AWS or Azure.

Malwarebytes

Malwarebytes continues to gain momentum, using its experience as the incident response tool of choice by organizations of all sizes, and has doubled its seat count in the past 12 months.

In 2017, Malwarebytes delivered cloud-based management, and added mainstream and advanced EDR capabilities to its single agent, which includes the breach remediation tools for remediating infections. It is one of the few vendors in this space that can roll back the changes made by ransomware, including restoring files that were encrypted in the attack. This ransomware remediation can be performed remotely from the cloud management console up to 72 hours after the attack, without the need for any local access to an endpoint.

For organizations with small IT or security teams, Malwarebytes provides strong protection capabilities and some advanced EDR capabilities, all at an attractive price point. For larger organizations, or organizations with a mature security team, there are some missing enterprise features that make it a challenge to incorporate into an existing SOC workflow.

STRENGTHS

The new EDR module included in Malwarebytes' cloud-based platform provides advanced investigation capabilities that are rarely seen outside of a dedicated EDR tool. For example, the Active Response shell provides remote access to interact with processes, view and modify the registry, send and receive files, and run commands and scripts remotely.

Ransomware rollback can be initiated remotely, including file recovery.

Malwarebytes offers application hardening and exploit mitigation, anomaly detection, ML, and behavior monitoring and blocking.

With the exception of EDR and investigation, Malwarebytes does not require an internet connection to provide threat protection. Organizations with untethered endpoints and no network connectivity will, therefore, continue to have the full protection.

The Malwarebytes endpoint agent can be orchestrated by workflows and triggers in enterprise-scale platforms such as IBM BigFix, Tanium, Phantom, ForeScout and SCCM.

CAUTIONS

The cloud-based management is lacking in visual reporting and quick-view dashboards. Customers report that the workflow for finding and responding to alerts is inefficient.

Although the endpoint agent implements strong protection against exploits, there is no vulnerability discovery or reporting capabilities within the Malwarebytes administration console.

There are no role-based access controls or directory-based access controls available for the management console. Larger organizations may find the lack of case and incident management workflow a challenge.

The Malwarebytes macOS agent does not report EDR data, leaving a visibility gap for most organizations.

McAfee

Intel completed the sale of 51% McAfee to TPG in April 2017 and, as a stand-alone company, McAfee hopes it can now refocus its efforts on the core aspect of its business: endpoint protection.

McAfee remains one of the top three incumbent EPP vendors by market share, and its execution issues over the past three years make it the top competitive target for displacement by other vendors in the EPP Magic Quadrant. Specifically, Endpoint Security (ENS) version 10.x (v.10.x) upgrades remained a very challenging adoption cycle for most McAfee clients. While the feature set and protection capabilities included in the most recent release are quite compelling, and public test scores have improved over the past year, McAfee's execution assessment is hampered by organizations continuing to be hesitant to adopt the latest version, leaving them vulnerable to commodity malware as well as more advanced threats. Gartner client inquiry data identified McAfee as the single most-quoted EPP vendor that clients were planning to replace. Customer satisfaction scores were low again for 2017.

McAfee's ePolicy Orchestrator (ePO) continues to be the most quoted reason for clients initially adopting McAfee solutions in their environment, or for retaining McAfee over their contract terms and subsequent renewals. However, disenchantment with the EPP product is quickly eroding the perceived value of ePO, in favor of vendors with cloud-based EPP management.

STRENGTHS

McAfee's investment in developing an EDR solution has resulted in an offering with a useful feature set.

ePO provides a common administrative platform for all of McAfee's offerings and integrates with over 130 third-party applications. McAfee also offers a cloud-based ePO.

Available in McAfee's advanced endpoint suites, Dynamic Application Containment (DAC) provides behavior-based containment/isolation of untrusted applications using McAfee Global Threat Intelligence data.

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

CAUTIONS

Although adoption of ENS v.10.x versions has seen significant acceleration over the past year, a large number of McAfee's clients remain on v.8.8, 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 vendor reports that most McAfee customers are actively engaged with ENS, but many Gartner clients still running v.8.8 were still not aware that they are entitled to move to a newer version, despite having renewed their contract within the last 12 to 24 months.

Although McAfee was among the first of the traditional EPP vendors to provide EDR capabilities, it remains in the early stages of customer adoption when compared to other vendors.

The most common customer complaints continue to be with the effectiveness of the older multiple-agent architecture in v.8.8, 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, and are looking for alternative vendors.

Clients that complete the upgrade to ENS v.10.x report only modest performance improvements over the previous v.8.8 client.

Microsoft

Microsoft is unique in the EPP space, as it is the only vendor with the capacity to embed protection features directly into the OS. It has used this advantage to step up its efforts in security with Windows 10 features, improvements to Windows Defender (also known as System Center Endpoint Protection), the addition of Windows Defender Advanced Threat Protection and Windows Defender Security Center.

Windows 10 OS-level features and capabilities available with Windows Enterprise E3 and E5, such as Application Guard, App Locker, Secure Boot, Device Guard, Exploit Guard, Advanced Threat Protection (ATP) and Credential Guard, significantly improve protection against current common threats. However, these protections are not as integrated in previous OS versions.

Overall, Microsoft now provides a broad range of security protections that address a wide spectrum of threats across endpoint, Office 365 and email. The comprehensive solution set will resonate with most organizations' security requirements, provided their budget stretches to the higher-tier, E5-level subscription.

Microsoft has become the most-asked-about vendor during EPP-related Gartner client inquiry calls, and there is significant interest in using the security capabilities in Windows 10 to reduce security spend with other vendors.

STRENGTHS

Over the past two years, Microsoft has made steady improvements in the security solutions available as part of Window 10. A deployment of Windows Defender with Defender ATP can be considered directly competitive with some of the EPP solutions available from other vendors noted in this research.

Windows Defender provides file-based protection using signatures and heuristics, along with cloud look-ups to detect newer malware. The cloud look-up and cloud-based ML has dramatically improved Microsoft's detection accuracy in test results. Defender in Windows 10 will step up to protect clients automatically if a third-party EPP engine fails, is out of date or is disabled.

Microsoft's EDR solution, Defender ATP, leverages Microsoft's own Azure infrastructure offering to store six months of endpoint data at no extra charge.

Microsoft's Windows Security Research Team benefits from a vast installation of over 1 billion consumer endpoint versions of the antivirus engine and its online system-check utilities, which provide a petri dish of malware samples and IOAs.

CAUTIONS

The biggest challenge continues to be the scattered security controls, management servers, reporting engines and dashboards. Microsoft is beginning to center its future management and reporting around the Windows Defender Security Center platform, which is the management interface for the whole Windows Defender suite, including ATP. Microsoft Intune is replacing System Center as the primary management tool.

To access advanced security capabilities, organizations need to sign up for the E5 tier subscription, which clients report as being more expensive than competitive EPP and EDR offerings, reducing the solution set's overall appeal.

Microsoft relies on third-party vendors to provide malware prevention, EDR and other functionality on non-Windows platforms, which may lead to disparate visibility and remediation capabilities and additional operational complexities.

The advanced security capabilities are only available when organizations migrate to Windows 10. It does much less to address all other Windows platforms currently in operation.

Palo Alto Networks

Palo Alto Networks is still best-known to Gartner clients for its next-generation firewall (NGFW) product line, and this continues to be the main line of introduction to Palo Alto Networks Traps for Gartner clients.

Traps uses a stack of nonsignature detection capabilities, such as ML, static and dynamic analysis, as well as monitoring processes and applications as they are spawned for suspicious activity and events. Suspect files from the endpoint can be tested by Palo Alto Networks WildFire, its cloud-based threat analysis and malware sandboxing platform, which is included with a Traps subscription.

Palo Alto Networks acquired LightCyber in 2017; its behavioral-based analytics technology provides automated detection of suspicious user and entity activity indicative of malware. Traps without LightCyber currently offers limited EDR capabilities, which impacts its execution and vision evaluation in this assessment.

Gartner clients will find Palo Alto Networks Traps most appealing when it can integrate with an existing Palo Alto Networks NGFW deployment.

STRENGTHS

- Organizations with existing Palo Alto Networks NGFW devices will be good candidates for an integrated deployment.
- Traps does not rely on signature updates, and although it does use the WildFire platform to perform fast look-ups by file hash, it is able to block malware/ransomware when offline or disconnected from the internet.
- Traps provides solid exploit prevention and mitigation, which is useful for organizations with a difficult patch management process.
- There are strong integrations with orchestration and SOC automation vendors such as Splunk, ServiceNow and Phantom.

CAUTIONS

- There is currently no cloud-based management option; customers must use an on-premises management server.
- While Traps collects endpoint forensics data, it does not provide any response capabilities or postevent remediation tools. Organizations that do not use a Palo Alto Networks NGFW will need to take a multivendor approach to gain these capabilities.
- Traps lacks EDR capabilities beyond simple IOC searching, making investigation hard without an additional product.
- Palo Alto Networks acquired LightCyber in early 2017, but has not yet used the technology to improve the limited detection and response capabilities in Traps.
- Traps displayed a high rate of false positives in AV-TEST testing between August and October 2017.

Panda Security

Panda Security's unique value proposition is the classification or attestation of every single executable file and process on a protected endpoint device, and it is the only vendor to include a managed threat hunting service in the base purchase of its EPP. Adaptive Defense 360 is fully cloud managed, and combines EPP and EDR into a single offering and single agent.

The attestation service implements an automatic application whitelisting model, where only trusted and approved applications and processes are able to execute. By offloading the classification and authorization process to the vendor, organizations will have a much better deployment success rate than trying to deploy a manual application control solution.

Panda Security's cloud-first approach, and the managed services backing the EPP and EDR capabilities, are beginning to increase brand awareness outside of Europe.

Organizations without experienced security staff will find Panda Security a good shortlist candidate for an EPP solution, as will organizations considering managed detection and response solutions that are prepared to replace their incumbent EPP vendor.

STRENGTHS

The 100% attestation service can drastically reduce the threat surface of endpoints.

Due to the classification of all executable processes, Panda Security is able to provide detailed information on vulnerable versions of applications that are present in the environment.

Panda Security's Adaptive Defense platform was one of the first to combine endpoint protection features with managed EDR capabilities.

The price point is extremely attractive when buyers consider the capabilities and managed services that are included.

CAUTIONS

The macOS agent is limited to signature-based malware detection, and does not integrate with EDR capabilities, leaving a visibility gap for many organizations.

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

File and process classification requires access to Panda's cloud-platform. Administrators will need to decide the impact this has on an endpoint without internet access; running unclassified executables (albeit scanned and monitored for known IOAs) or blocking until connectivity to Panda is restored.

An application control and application whitelisting approach are not suitable for all types of user roles. For example, developers who regularly run and test new software builds locally will need exceptions, and adding exceptions will reduce the overall security benefit of this approach.

SentinelOne

SentinelOne is a part of the new wave of EPP solution providers that have experienced fast growth over the past few years. The cloud-based solution is designed around fully embedded EDR and behavioral protection. SentinelOne was one of the first vendors to offer a ransomware protection guarantee based on its behavioral detection and file journaling features. In 2017, SentinelOne struggled to maintain its mind share and share-of-voice in a

crowded market, which impacts the marketing-related assessment criteria across both vision and execution. However, the vendor continued to sign on a broad range of partners and resellers.

SentinelOne is a good prospect to replace or augment existing EPP solutions for any organization looking for a solution with strong protection and visibility.

STRENGTHS

SentinelOne's single agent design provides fully integrated file and advanced behavioral anti-malware, based on its EDR functionality.

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

SentinelOne offers endpoint visibility (Windows, Linux, macOS and VDI) for investigative information in real time, and an API to integrate common-format, IOC-based threat feeds.

SentinelOne leverages volume shadow copy snapshots to return an endpoint to a previously known good state.

CAUTIONS

The most significant challenge that SentinelOne faced in 2017 was the churn in staff roles across product, sales, marketing, and other internal and client-facing groups. Gartner clients reported inconsistent interactions with SentinelOne throughout the year. This negatively impacts on its execution and vision in this assessment.

SentinelOne does not offer application whitelisting or leverage the use of sandboxing for suspicious file analysis (local, network or cloud).

While SentinelOne offers broad platform support, not all platforms provide the same level of capabilities or response options, which can lead to disparities in overall protection and workflow.

Larger organizations with advanced SOCs will find the management console lacking in visibility and workflow capabilities.

Sophos

In March 2017, Sophos acquired Invincea — a Visionary vendor in the 2017 Magic Quadrant for Endpoint Protection Platforms — giving Sophos access to its deep learning ML algorithms.

The Sophos Intercept X product, designed to protect against and recover from the malicious actions related to ransomware and exploits, proved popular with both existing Sophos Endpoint Protection customers and as an augmentation to an incumbent EPP. This momentum continued its increased brand awareness in the enterprise space.

Also included in the Intercept X purchase are Sophos' EDR-like capabilities — called Root Cause Analysis — and the ML malware detection technology from the acquisition of Invincea was added in late 2017.

Sophos' cloud-based EPP with the Intercept-X platform is a good fit for organizations that can take advantage of a cloud-based administration platform, and that value strong protection against ransomware and exploit-based attacks over advanced forensic investigation capabilities.

STRENGTHS

Intercept X clients report strong confidence in not only protecting against most ransomware, but also the ability to roll back the changes made by a ransomware process that escapes protection.

Intercept X is available as a stand-alone agent for organizations that are unable to fully migrate from their incumbent EPP vendor.

The exploit prevention capabilities focus on the tools, techniques and procedures that are common in many modern attacks, such as credential theft through Mimikatz.

The Sophos Central cloud-based administration console can also manage other aspects of the vendor's security platform, from a single console, including disk encryption, server protection, firewall, email and web gateways.

Root Cause Analysis provides a simple workflow for case management and investigation for suspicious or malicious events.

Root Cause Analysis capabilities are available to macOS, along with protection against cryptographic malware.

CAUTIONS

Although we credited Sophos for a cloud-first approach last year, it has now made parts of Intercept X available for on-premises customers. This is likely to hamper cloud adoption and extend the time that Sophos manages and maintains separate protection stacks.

Root Cause Analysis is not available in Intercept X for clients that use the on-premises version of Sophos Endpoint Protection.

Sophos' primary improvement was the integration of Invincea's deep learning technology. Beyond that, there has been little in the way of enhancements to the EDR capabilities of the Sophos Endpoint Protection platform in the last 12 months.

Sophos does not provide vulnerability reporting; rather, it relies on its mitigation and blocking technologies, so organizations will need to find other ways to prioritize their patch management program.

Symantec

The divestiture of the Veritas business in January 2016 and the acquisition of Blue Coat in August 2016 provided a new executive team with leadership and vision that has refocused the vendor and resulted in an improved execution score in this analysis. In 2017, Symantec successfully released product updates for its traditional products with enhancements and

new capabilities, such as deception technologies. In the EDR space, Symantec is the most successful of the traditional EPP vendors, where the Advanced Threat Protection (ATP) product uses the same agent as Symantec Endpoint Protection (SEP).

Throughout 2017, Symantec continued to be the leading vendor mentioned by other vendors as their main competition. Symantec continues to generate growth and increased revenue in both the consumer and enterprise businesses (roughly evenly split 50/50). It continues to lead the market in EPP revenue and market share.

Symantec continues to provide one of the most comprehensive EPPs available in this market, with third-party test scores remaining in the top tier, and has added advanced features to better address the changing threat landscape, becoming the first vendor to combine malware protection, EDR, system hardening and deception capabilities in a single agent.

Symantec has begun the process of migrating its offerings to a cloud-first model, with a hybrid option available to clients that prefer to maintain some of the management capabilities on-premises.

STRENGTHS

Symantec seems to have finally found a stable footing with its management team bringing stability across the company.

SEP 14 and, most recently, SEP 14.1 have proven to be very stable and efficient on resources. Clients report that the addition of ML and other advanced anti-malware capabilities have improved threat and malicious software detection, and containment.

Symantec ATP, its EDR-focused solution, provides good capabilities for detection and response, and existing SEP customers will benefit from its use of the existing SEP agent.

Symantec has started to embrace a cloud-first strategy with the introduction of its latest product updates, including SEP Cloud and EDR Cloud, which provide a cloud-based console with feature parity to the on-premises management console.

Symantec's broad deployment across a very large deployment population of both consumer and business endpoints provides it with a very wide view into the threat landscape across many verticals.

CAUTIONS

When compared with other vendors in the EPP market, Symantec is still perceived as more complex and resource-intensive to manage.

Although Symantec has gained strong traction with its EDR components, the vendor struggles to effectively message the benefits of its single agent approach. Many Gartner clients that use SEP and desire EDR capabilities are initially unaware of the availability of Symantec ATP.

Symantec offers a full managed service and managed SOC, which are only attractive when an organization wishes to offload its entire SIEM capability to the vendor. The larger scope of its Managed Security Services (MSS) is expensive when compared to other options from newer vendors that focus on a narrower set of services or features.

Symantec customers continue to report inconsistent support experience, even when large organizations are provided with dedicated support personnel. Symantec customers also reported poor client/account manager communication.

Trend Micro

Trend Micro is the third-largest vendor in the EPP market, with products ranging across network, data center and endpoint systems. It has a large worldwide footprint, with more than half of the business coming from Japan and the Americas.

Although the vendor has had a rather unremarkable year from a technology innovation perspective, it ticks boxes for mainstream EPP requirements, particularly for those looking for a comprehensive suite of solutions at an affordable price. Unlike the more visionary participants in this Magic Quadrant, Trend Micro's EDR solution is delivered as a separate agent to the EPP solution. And while it integrates with additional on-premises products like the Deep Discovery sandbox, it lacks integration with its cloud sandbox, and cannot be managed from Trend Micro's cloud platform.

One of Trend Micro's biggest advantages is the vulnerability assessment and virtual patching technology, which uses an IPS engine to detect vulnerabilities, and uses HIPS to create a virtual patch to block the exploitation.

Trend Micro remains a good shortlist candidate for organizations of all sizes.

STRENGTHS

Trend Micro participates in a wide range of third-party tests, with good results overall, and the OfficeScan client delivers functionality that other traditional vendors provide in their separate EDR add-on, such as IOA-driven behavioral detection.

The virtual patching capabilities can reduce pressure on IT operational teams, allowing them to adhere to a strategic patch management strategy without compromising on security.

For customers looking for a single strategic vendor, Trend Micro has strong integration across the endpoint, gateway and network solutions to enable real-time policy updates and posture adjustments.

Trend Micro offers managed detection and response services, in its Advanced Threat Assessment Service, to augment the technology with expert analysis and best practices.

CAUTIONS

EPP and advanced EDR capabilities such as process visualization for investigation and threat hunting are delivered by separate agents.

Although the cloud management and on-premises management consoles for the OfficeScan EPP agent are identical, some organizations may need to continue with on-premises management if they wish to use functions beyond the base EPP, such as EDR.

Although more than 50% of its installed base is running the latest product release, a number of Trend Micro customers reporting poor malware detection told Gartner they were unaware of the availability of new products or new capabilities. This is not unique to Trend Micro, it is

common across the larger, traditional vendors.

There is no macOS support for EDR, leaving a visibility gap for most organizations.

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

Cisco (AMP for Endpoints)

Endgame

Fortinet (FortiClient)

FireEye (HX Series and Helix)

Dropped

The following vendors appeared in the 2017 Gartner Magic Quadrant for Endpoint Protection Platforms but were not included in this research, due to their specific focus on single segments:

360 Enterprise Security Group. One of the best-known brands of endpoint security in China, 360 Enterprise Security Group provides endpoint protection and other security suite solutions — including web gateway, data loss prevention, and mobile threat defense — that are compliant with Chinese government policy and are good choices for organizations based in China.

AhnLab. With a very large SMB installed base within South Korea, and serving some very large enterprises, AhnLab focus on the Korean, Japanese, Chinese and other Asia/Pacific markets with endpoint protection, mobile security and data loss prevention.

G Data Software. G Data Software is a popular vendor in the DACH region (Germany, Switzerland and Austria) that offers a suite of solutions including endpoint, web gateway and email. Its location and compliance with German data protection regulations provides a "No Backdoor Guarantee" for its solution, and the processing of telemetry takes place solely in Germany. Customers report reliable, local language customer service as a key part of their purchasing decision.

Webroot. Webroot primarily focuses on delivering capabilities to managed service providers and channel partners, which use Webroot as part of a managed service offering including endpoint security, network security, security awareness training and threat intelligence services. Webroot's technology is embedded in a number of other security vendors' solutions.

Inclusion and Exclusion Criteria

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

The majority of detection events must be from the vendor's own detection technique, and designed, owned and maintained by the vendor itself. Augmenting with an OEM engine is acceptable, provided it is not the primary method of detection.

The vendor's nonconsumer EPP must have participated in independent, well-known, public tests for accuracy and effectiveness within the 12 months prior to 18 November 2017 *or* be a current participant in the VirusTotal public interface. Examples include Virus Bulletin, AV-TEST, AV-Comparatives, NSS Labs and SE Labs.

The vendor must have more than five named accounts larger than 10,000 seats that use the vendor's EPP as their sole EPP.

The vendor must have a minimum of 500,000 deployed licenses, protecting nonconsumer endpoints, with at least 50,000 of those licenses protecting nonconsumer endpoints within North America.

The vendor must satisfy at least 12 of the following "Basic" capabilities, and at least four of the following "Desirable" capabilities:

Basic capabilities:

Blocks known and unknown file-based malware, without relying on daily signature distribution

Detects suspicious and malicious activity based on the behavior of a process

Implements protection for common application vulnerabilities and memory exploit techniques

Can perform static, on-demand malware detection scans of folders, drives or devices such as USB drives

Suspicious event data can be stored in a centralized location, for retrospective IOC/IOA searching/analysis

Allows real-time IOC/IOA searching across all endpoints (e.g., file hash, source/destination IP, registry key)

Allows remote quarantining of an endpoint, restricting network access to only the EPP management server

Automatically updates policies, controls, and new agent/engine versions without connecting directly to the corporate network

Continues to collect suspicious event data when outside of the corporate network

Detections and alerts include severity and confidence indicators, to aid in prioritization

Provides risk-prioritized views based on confidence of the verdict and severity of the incident

Displays full process tree, to identify how processes were spawned, for an actionable root cause analysis

Automatically quarantines malicious files

Identifies changes made by malware, and provides the recommended remediation steps

Detects, blocks, and reports attempts to disable or remove the EPP agent

Desirable capabilities:

Primary EPP console uses a cloud-based, SaaS-style, multitenant infrastructure, and is operated, managed and maintained by the vendor

Implements vulnerability shielding (aka virtual patching) for known vulnerabilities in the OS and for non-OS applications

Can implement default-deny whitelisting with a vendor maintained "app store"-type approach, and user self-service features

Can implement application isolation, to separate untrusted applications from the rest of the system

Includes access to a cloud or network-based sandbox that is VM-evasion-aware

Includes deception capabilities designed to expose an attacker

Vendor itself offers managed detection services, alerting customers to suspicious activity

Vendor itself offers managed threat hunting, or managed IOC/IOA searching, for detecting the existence of threats (not via third party or channel)

Supports advanced natural-language queries with operators and thresholds (e.g., "Show all machines with new PE >1 week old AND on <2% of Machines OR Unknown")

Provides guided analysis and remediation based on intelligence gathered by the vendor (e.g., "85% of organizations follow these steps")

Provides attribution information and potential motivations behind attacks

Can utilize third-party, community and intelligence feeds

Allows remote remediation via the management console

Includes APIs for integration with SOAR/orchestration for automation

Evaluation Criteria

Ability to Execute

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

Product or Service: We evaluated the protection and capabilities of the product used by the majority of a vendor's installed base, and the ability of the vendor to provide timely improvements to its customers.

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 satisfaction with their technical training, sales incentives, marketing and product quality, and on their price and packaging strategy relative to other vendors in the market.

Market Responsiveness/Record: We evaluated vendors by their market share in total customer seats under license, and their performance relative to the market and other vendors.

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, and on the execution of marketing initiatives driving brand awareness and customer satisfaction.

Customer Experience: We evaluated vendors based on reference customers' satisfaction scores as reported to us in an online survey, and through data collected over the course of over 2,100 endpoint-security-related Gartner client interactions, and through Gartner Peer Insights.

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	
Product or Service	
Weighting	
	High
Overall Viability	
Weighting	
	High
Sales Execution/Pricing	
Weighting	

	Medium
Market Responsiveness/Record	
Weighting	
	High
Marketing Execution	
Weighting	
	Medium
Customer Experience	
Weighting	
	High
Operations	
Weighting	
	Medium

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	
Product or Service	
Weighting	High
Overall Viability	
Weighting	High
Sales Execution/Pricing	

Weighting	Medium
Market Responsiveness/Record	
Weighting	High
Marketing Execution	
Weighting	Medium
Customer Experience	
Weighting	High
Operations	
Weighting	Medium

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	
Product or Service	
Weighting	High
Overall Viability	
Weighting	High
Sales Execution/Pricing	
Weighting	Medium
Market Responsiveness/Record	
Weighting	High
Marketing Execution	

Weighting	Medium
Customer Experience	
Weighting	High
Operations	
Weighting	Medium

Source: Gartner (January 2018)

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.

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

Offering (Product) Strategy: When evaluating vendors' product offerings, we looked for an approach to product development and delivery that emphasizes market differentiation, functionality, methodology and features as they map to current and future requirements.

Anti-malware protection and detection capabilities: This is the quality, quantity, accuracy and ease of administration of an EPP's anti-malware technology. It covers the tools required to block file-based malware attacks, detect and prevent fileless malware attacks, and mitigate the risk of OS and application vulnerabilities. We look at test results from various independent testing organizations and data from VirusTotal, and use Gartner client inquiries as guides to the effectiveness of these techniques and implementations against modern malware.

Management capabilities: This is the provision of a centralized, role-centric console or dashboard that enhances the real-time visibility of an organization's endpoint security state. It provides clearly prioritized alerts and warnings, and provides intuitive administration workflows. Vendors that have delivered a cloud-first model with feature parity to an on-premises management platform are given extra credit, as organizations struggle to maintain visibility and control over endpoints in use by the increasing remote workforce.

Incident prevention and investigation capabilities: This includes the discovery, reporting and prioritization of vulnerabilities present in the environment. We look for vendors that provide educated guidance for customers to investigate incidents, remediate malware

infections and provide clear root cause analysis, helping reduce the attack surface. Vendors that focus on lowering the knowledge and skills barrier through guided response tools, and easy to-understand-and-use user interfaces are given extra credit here.

Operational IT: Vendors committed to reducing their customers' attack surface do so with risk-based, prioritized security state assessments — highlighting known vulnerabilities and misconfigurations. We look for vendors that help their customers understand weaknesses in security posture and process, and those that help audit and measure the impact of security investments.

Supported platforms: Several vendors focus solely on Windows endpoints, but the advanced solutions can also support macOS with near parity on the features delivered in both clients, notably in the activity and event monitoring areas of EDR.

Innovation: We evaluated vendor responses to the changing nature of customer demands. We accounted for how vendors reacted to new threats, invested in R&D and/or 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	
Market Understanding	
Weighting	
	High
Marketing Strategy	
Weighting	
	Medium
Sales Strategy	
Weighting	
	Not Rated
Offering (Product) Strategy	

Weighting	
	High
Business Model	
Weighting	
	Not Rated
Vertical/Industry Strategy	
Weighting	
	Not Rated
Innovation	
Weighting	
	Medium
Geographic Strategy	
Weighting	
	Low

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	
Market Understanding	
Weighting	High
Marketing Strategy	
Weighting	Medium

Sales Strategy	
Weighting	Not Rated
Offering (Product) Strategy	
Weighting	High
Business Model	
Weighting	Not Rated
Vertical/Industry Strategy	
Weighting	Not Rated
Innovation	
Weighting	Medium
Geographic Strategy	
Weighting	Low

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	
Market Understanding	
Weighting	High
Marketing Strategy	
Weighting	Medium
Sales Strategy	
Weighting	Not Rated

Offering (Product) Strategy	
Weighting	High
Business Model	
Weighting	Not Rated
Vertical/Industry Strategy	
Weighting	Not Rated
Innovation	
Weighting	Medium
Geographic Strategy	
Weighting	Low

Source: Gartner (January 2018)

Quadrant Descriptions

Leaders

Leaders demonstrate balanced and consistent 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, and solid detection and response capabilities that can address the security needs of the mass market. They also have stronger sales and visibility, which add up to a higher execution than Niche Players offer. Challengers are often one or two core capabilities short, or lack a fully converged strategy, which affects their completeness of vision when compared to the Leaders. They are solid, efficient and expedient choices.

Visionaries

Visionaries deliver in the leading-edge features — such as cloud management, managed features and services, enhanced detection or protection capabilities, and strong incident response workflows — 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 consistent execution. Clients pick Visionaries for best-of-breed features.

Niche Players

Niche Players offer solid anti-malware solutions, and basic EDR capabilities, but rarely lead the market in features or function. Some are niche because they service a very specific geographic region or customer size, while some focus on delivering excellence in a specific method or combination of protection capabilities. Niche Players can be a good choice for conservative organizations in supported regions, or for organizations looking to deploy an augmentation to an existing EPP for a "defense in depth" approach.

Context

In the past 12 months, EPP solutions have continued on track to consume features from the EDR market, and some of the traditionally pure-play EDR vendors have continued to bolster their solutions with protection capabilities more often found in EPP (see "Market Guide for Endpoint Detection and Response Solutions").

This trend of playing catch-up from two directions has resulted in a slew of vendors with similar capabilities and with little to differentiate themselves.

Those that do differentiate do so with managed features backed by automation *and* human analysts; a focus on cloud-first management and reporting, and improving the operational side of IT with a focus on vulnerability protection and reporting; and, most importantly, pushing full-stack protection for EPP and EDR use cases to organizations of all sizes.

The new wave of endpoint security vendors was previously considered by risk-averse buyers as complementary to, rather than direct replacements for, traditional EPP. This year, however, Visionary vendors are now gaining traction across all market segments. Although these new-wave vendors attempt to position themselves at a premium price when compared with the renewal costs of a traditional vendor, the sheer volume of vendors in the space makes it a buyer's market. Heavy discounting is apparent, especially with traditional vendors keen to keep their installed base, and with new-wave vendors that have investors and venture capital firms to please.

Gartner clients should look to vendors that have faster development cycles, providing quicker responses to changing attack trends, and delivering smaller updates that do not need a full uninstall and reinstall. Regardless, organizations should endeavor to upgrade to the latest version as soon as practical; we recommend a minor version upgrade within three months and a major version upgrade within six months.

Market Overview

Testing, Transparency and Evaluation

Malware attacks in early 2017 were seminal to the increased scrutiny on security vendors by the media, independent researchers, and customers and prospects. Gartner's endpoint protection analyst team received hundreds of inquiries driven by media stories, showing that vendor-client trust is a huge part of any buying decision.

As with previous Magic Quadrants, this year's inclusion criteria mandate that vendors must have participated in public, independent testing during 2017. Gartner is disappointed with several vendors' weak participation in standardized tests. There are legitimate complaints about current testing methods and scenarios; however, short of an organization putting a red team together to perform custom-made penetration testing, these tests remain the best indicators of effectiveness, and can be a useful data point to compare trends and performance over time in the same test framework.

Participating in independent tests by AV-Comparatives, AV-TEST, Virus Bulletin and other platforms with public interfaces like VirusTotal demonstrates not only that the products are fit for purpose, but also that the vendor is comfortable with and committed to engaging in a more transparent industry. It's worth noting that many vendors, from traditional to the new wave, are embracing the shift to a more open community. Solutions from vendors without a long-term commitment to engagement and transparency should be approached with caution.

When evaluating a security solution, it is critical to understand which areas that organizations are currently over- or underinvested in. Gartner provides a simple framework in the Adaptive Security Architecture, which many vendors use to communicate their value and feature set in a simple way. Other frameworks exist for more technical evaluations, and the Mitre ATT&CK [1] framework, in particular, is growing in popularity as a way to understand which distinct attack techniques an EPP can prevent or detect.

EPP, EDR and IT Operations

Successful attacks still make use of known vulnerabilities and weaknesses in an organization's security policy and device configuration. Even the most damaging and high-profile attacks in 2017 (WannaCry and NotPetya) could have been mitigated or the impact reduced by better IT operations, and by better education and communication from security vendors to their customers. Organizations that suffered despite their growing investment in strong endpoint security capabilities felt let down by their vendors. Many of these clients were dissatisfied when their request for help in recovering was met with, "Well, you should have deployed a patch." These clients asked Gartner, "If these weaknesses were common knowledge, why didn't our vendor warn us when they have a presence on all our endpoints?"

The most visionary and leading of vendors in 2018 and 2019 will be those that use the data collected from their EDR capabilities to deliver actionable guidance and advice that is tailored to their clients. Detecting known IOCs and suspicious behavior is only one side of the EPP coin — solutions must detect and proactively alert on weaknesses or vulnerabilities that are being exploited right now, or are likely to be exploited in the future.

The fast-moving nature of attacker tools, techniques and procedures means that an organization's endpoint security strategy must be continually assessed and adapted (see "Use a CARTA Strategic Approach to Embrace Digital Business Opportunities in an Era of Advanced Threats").

Organizations that are approaching renewal for their incumbent EPP should appraise their current security posture. For example:

- How effective is our patch management strategy, and do our EPP controls protect against the misuse of vulnerable applications?
- How fast is our time to resolution of alerts and incidents?
- Will our staffing level — and the experience of those employees — allow us to take advantage of advanced tools to deliver stronger security capabilities?
- Should we make a short-term, tactical investment in additional managed services, or switch to a vendor that can provide on-demand managed assistance when we need it?

With a better understanding of current state, organizations can make educated purchasing decisions, based on the features and capabilities that make a difference to them and their security posture. Gartner clients can use the Adaptive Security Architecture framework to assess their capabilities within the protection, detection, response and prediction (see "Designing an Adaptive Security Architecture for Protection From Advanced Attacks").

Evidence

- Gartner responded to more than 2,100 client inquiries.
- Gartner conducted an online survey of 129 EPP reference customers in 4Q17.
- Gartner conducted an online survey of 55 EPP channel references in 4Q17.

[1] "Adversarial Tactics, Techniques & Common Knowledge." (https://attack.mitre.org/) ATT&CK.

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.
