Magic Quadrant for Endpoint Protection Platforms

Published 20 August 2019 - ID G00352135 - 63 min read

By Analysts Peter Firstbrook, Dionisio Zumerle, Prateek Bhajanka, Lawrence Pingree, Paul Webber

The endpoint protection market is transforming as new approaches challenge the status quo. We evaluated solutions with an emphasis on hardening, detection of advanced and fileless attacks, and response capabilities, favoring cloud-delivered solutions that provide a fusion of products and services.

Strategic Planning Assumption

By 2025, cloud-delivered EPP solutions will grow from 20% of new deals to 95%.

Market Definition/Description

This document was revised on 23 August 2019. The document you are viewing is the corrected version. For more information, see the Corrections page on gartner.com.

An endpoint protection platform (EPP) is a solution deployed on endpoint devices to harden endpoints, to prevent malware and malicious attacks, and to provide the investigation and remediation capabilities needed to dynamically respond to security incidents when they evade protection controls. Traditional EPP solutions have been delivered via a client agent managed by an on-premises management server. More modern solutions utilize a cloud-native architecture that shifts the management, and some of the analysis and detection workload, to the cloud.

Security and risk management leaders responsible for endpoint protection are placing a premium on detection capabilities for advanced fileless threats and investigation and remediation capabilities. Data protection solutions such as data loss prevention (DLP) and encryption are also frequently part of EPP solutions, but are considered by buyers in a different buying cycle.

Protection for Linux and Mac is increasingly common, while protection for mobile devices and Chromebooks is increasing but is not typically considered a must-have capability.

While protection for virtual, Windows and Linux servers is common, the evolutionary shift from hardware servers to virtual machines (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.") As a result, specialized tools to address the modern hybrid data center that utilizes both

the cloud and on-premises deployments are diverging into a new market Gartner calls cloud workload protection platforms (CWPP; 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 due to the largely divergent nature of their features and management.

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 2019 Magic Quadrant for Endpoint Protection Platforms, capabilities traditionally found in the endpoint detection and response (EDR) market are now considered core components of an EPP that can address and respond to modern threats (see "Market Guide for Endpoint Detection and Response Solutions").

Magic Quadrant

Figure 1. Magic Quadrant for Endpoint Protection Platforms

Source: Gartner (August 2019)

Vendor Strengths and Cautions

Bitdefender

Bitdefender is a private software company that offers an EPP and EDR in one platform, GravityZone Ultra, and one agent across endpoints, and physical, virtual or cloud servers, delivered via a cloud or on-premises management.

Bitdefender has been consistently growing its enterprise segment presence and licenses its core engine to an extensive range of security products. It launched a managed detection and response

(MDR) service providing proactive alerting, assistance with alert investigation and periodic health checks. It also added a confidence score.

Bitdefender is a good choice for organizations that value malware detection accuracy and agent performance, as well as full support for data center and cloud workloads from a single solution.

Strengths

- Bitdefender has a large R&D team that focuses on threat research and that is a consistent top performer in malware protection tests.
- Bitdefender offers a single modular agent for physical, virtual and cloud platforms, and a single SaaS console for all endpoint/server security administration.
- Low-overhead EDR supported by several detection layers and automated response actions enable enterprises and midmarket organizations to benefit from EDR.
- Gartner clients praise Bitdefender for its ease of use, deployment and customer support.
- Bitdefender provides a series of features that can decrease the attack surface of the endpoint, including application whitelisting. GravityZone provides integrated vulnerability and configuration monitoring and can provide patch management with an add-on license. It also provides full-disk encryption, web content filtering and device control.

Cautions

- The Bitdefender EDR capability lacks numerous common features for advanced security operations center (SOC) users such as analyst workflow, automatic indicator of compromise (IOC) or threat feed integration, custom query and blocking rules, contextual information, and guided investigation.
- Bitdefender Patch Management module, firewall module and sandbox analysis feature are not available for the Linux platform yet, nor do they interoperate with other client management tools for remediation purposes.
- Anomaly detection and Bitdefender's MDR offering are new and unproven in the market.
- EDR capabilities are only available in the cloud platform. The app whitelisting capability is only available with the on-premises platform.
- While Bitdefender has taken steps to grow its enterprise presence and sales operations, mind share among Gartner clients remains low.

BlackBerry Cylance

Cylance was acquired by BlackBerry, effective 21 February 2019, and now operates as a division of BlackBerry. BlackBerry has publicly communicated its vision to secure the Internet of Things (IoT) by leveraging Cylance AI technologies as an essential component. Initial plans include cross-selling of Cylance into BlackBerry enterprise accounts and integration of Cylance AI into BlackBerry's unified endpoint management solution and QNX platform for automotive OEMs.

Cylance is best known in the market for its signatureless malware prevention using machine learning (ML). Cylance has also applied machine learning to its EDR product CylanceOPTICS. Cylance has a strong OEM business and technology integrations into nontraditional endpoint solutions, such as security gateways, industrial control systems and medical devices

Cylance now also offers on-premises and hybrid deployments along with SaaS delivery. On-premises and hybrid deployments are targeted to air-gapped environments. The newly introduced CylanceGUARD, its managed detection and response solution, provides proactive threat hunting; however, this capability was not publicly announced until after the analysis deadline for generally available features, and it was not included in the analysis.

Strengths

- Cylance's primary strength is the use of agent-side machine-learning-trained algorithms to detect file-based malware instead of signature databases. This approach avoids the maintenance and network burden of daily updates, is more effective at detecting known and unknown malware, and doesn't require a connection to the internet to protect. CylancePROTECT also provides memory protection and script controls for fileless malware.
- CylanceOPTICS provides EDR capabilities to provide endpoint visibility and incident response capabilities. Cylance is well positioned to use its machine learning expertise to provide user and entity behavioral detection capabilities.
- Response orchestrated with automated package playbooks was introduced in 2018. Playbooks allow for automatic preventive or remediation actions (e.g., terminate processes, suspend processes, delete files, delete registry keys, log off users, etc.) via Python scripts when a detection event is triggered.
- CylancePROTECT supports Windows, macOS, AWS Linux and Linux operating systems. It can be used in virtual environments owing to its minimal system overhead.
- Gartner clients report a good experience, effective customer support, quality of technical support, and effective malware and ransomware protection.

Cautions

- The acquisition by BlackBerry adds some uncertainty to Cylance's execution. BlackBerry's goals may not align with Cylance customers' aspirations for the product.

- The ML capabilities in CylancePROTECT have yielded good results at detecting new malware; however, CylancePROTECT is overly reliant on machine learning technology, which makes it easier to be bypassed by malware authors. Moreover, Gartner clients have reported false-positive rates in CylancePROTECT with custom or rare applications, requiring organizations to establish a whitelisting process. CylanceOPTICS is necessary to add behavioral detection.

- CylancePROTECT and CylanceOPTICS require two separate agents with two separate installations, although an integrated agent is due in 3Q19.

- CylanceOPTICS stores historic data on the endpoint, which makes it subject to loss if the endpoint is inaccessible. InstaQuery provides information only from devices that are online. Out-of-the-box automated remediation options are limited. CylanceOPTICS does not support Linux. CylanceOPTICS advanced threat hunting and custom behavioral rules are scripted in Python and do not leverage an easy-to-use UI.

- Cylance does not yet offer security operations capabilities such as vulnerability and configuration assessment; however, these features are on Cylance's short-term roadmap.

- Cylance has not participated in tests of its antivirus effectiveness except for the NSS Labs test and VirusTotal, making it difficult for prospective customers to compare its efficacy to other solutions without a proof of concept. It is participating in the next round of MITRE evaluations.

Carbon Black

Carbon Black has recently transitioned its focus to selling and migrating customers to its cloud-based security platform, the CB Predictive Security Cloud (PSC). The company's overall offerings consist of CB Defense (EPP), CB ThreatHunter, CB LiveOps, and CB ThreatSight on PSC, and CB Response (threat hunting and incident response) and CB Protection (application whitelisting and device lockdown) on-premises offerings.

Carbon Black maintains 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.

Strengths

- Carbon Black's single cloud console, single-agent approach to integrated EPP and EDR provides ease of use and seamless integration between core product offerings and enhanced offerings such as threat hunting (CB ThreatHunter), and endpoint query and remediation (CB LiveOps).

- Carbon Black provides an advanced toolset (CB ThreatHunter) that has broad appeal to 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 both online and offline detection signatures, machine learning, software behavior monitoring, process isolation and memory protection, along with exploit prevention.
- Carbon Black's cloud-native console offers administrators simplified views of threats via visual alerts, triage and live remote Secure Shell access.
- Carbon Black's APIs and broad third-party partner ecosystem provide opportunities for SOCs to integrate Carbon Black findings into a diverse set of analytics, IT operations workflows, security operations and case management solutions.

Cautions

- The Predictive Security Cloud is the flagship platform; however, a substantial portion of Carbon Black's installed base is still on the CB Response and CB Protection product lines, which do not include an EPP capability. PSC will be the primary platform for new features and functions.
- 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 PSC is still missing common features such as rogue device detection. Some customers report lengthy issue resolution times and quality issues with Carbon Black's customer support services.
- A limited number of Carbon Black customers report endpoint device performance issues related to their CB Defense deployments, and that performance troubleshooting could be made easier in the CB Defense solution.

Check Point Software Technologies

Check Point Software Technologies is a global security vendor well known for its network firewall products. It has been a vendor in the endpoint protection market since the 2003 acquisition of Zone Labs' personal firewall. In 2016, Check Point introduced SandBlast Agent, which provides both advanced EPP and EDR capabilities. SandBlast shares ZoneAlarm prevention technologies, but it is targeted for the enterprise; while ZoneAlarm is now targeted commercially for consumers. In addition, Check Point SandBlast also offers endpoint VPN, encryption, URL filtering and anti-ransomware products.

SandBlast is integrated with Check Point gateways via the Infinity management console for alert consolidation and data sharing.

Strengths

- All endpoint protection capabilities are managed in a single management console delivered via a cloud service or an on-premises management server.
- Protection capabilities include memory exploit protection, behavioral protection and browser extensions for Chrome, Internet Explorer and Mozilla Firefox. These extensions provide downloaded file sandbox inspection, phishing URL protection and corporate password reuse monitoring. There is also a cloud sandbox for suspicious file detonation.
- The EDR incident response management experience is enhanced by contextual information on process and automatic correlation of suspect events. Remediation capabilities include encrypted file restoration, full attack chain sterilization and machine isolation.
- SandBlast Mobile for Android and iOS provides jailbreak detection, device configuration and profile monitoring, malware and man-in-the-middle attack prevention.

Cautions

- Despite its long history in the market, Check Point has struggled to gain market and mind share.
- Only incident-related data and event forensics reports are stored in the central management system. Raw data is stored locally on the endpoint. Other enterprise-class features such as workflow, advanced threat hunting and custom rule creation are lacking.
- Rogue client detection is limited to data stored in Active Directory. The vendor does not offer any vulnerability or configuration management capabilities.
- Management experience is inconsistent. Investigations traverse several different interfaces, tabs and windows. Some of the user interfaces are Win 32-application-style, while other components were more modern UI designs. Policy configuration involves myriad pop-up windows. Mac and Linux searching can only be done via command line.
- Check Point does not participate in regular testing of its effectiveness, appearing in only four tests in the past 12 months. Check Point cloud management for the SandBlast agent is new and has limited adoption at the time of publication.

Cisco

Cisco offers Advanced Malware Protection (AMP) for Endpoints, which consists of prevent, detect and respond endpoint security capabilities deployed with a cloud or on-premises management console.

Cisco's AMP for Endpoints makes use of AMP capabilities that are also available in other Cisco security offerings including threat intelligence data from Threat Grid and Talos security research.

AMP for Endpoints integrates with other Cisco security products, such as secure email and web gateways and network security appliances in the Cisco Threat Response incident response console.

Cisco's AMP will appeal to existing Cisco clients, especially those that that leverage other Cisco security solutions, and that aspire to establish security operations around Cisco products.

Strengths

- Cisco AMP is highly reputed for its threat intelligence from its well-known Talos security research team and for its exploit prevention capabilities, both used as a means of reducing the endpoint attack surface. Cisco recently licensed Morphisec to add exploit prevention.
- Cisco AMP can perform discovery of unprotected and unmanaged endpoints that present malicious behavior based on network security information.
- Cisco offers a broad range of managed services, including SOCs, active threat hunting, and incident support.
- Cisco Threat Response integrates AMP and other Cisco security offerings, such as firewall, intrusion prevention system (IPS), secure email and web gateways. This allows for centralized alert consolidation and incident response, as well as intelligence sharing and policy synchronization in the Cisco Threat Response console.

Cautions

- The Exploit Prevention engine, Malicious Activity Protection engine and System Process Protection (SPP) engine are only available for Windows. Mac and Linux rely on the open-source ClamAV for signatures.
- EDR navigation between screens is neither fluid nor intuitive to get a full understanding of the state of an endpoint or the incident and to pivot to find related items.
- Although the threat hunting functionality has expanded, Cisco AMP still lacks certain advanced threat hunting capabilities, such as the creation of customized behavioral protections and the integration of threat feeds. Also, it lacks a community portal for collaboration with industry peers.
- The majority of Cisco AMP deployments are deployed with another EPP solution to augment existing protection solutions and interoperate with other Cisco security solutions via Threat Response.
- Cisco still needs to consolidate its various endpoint agents for Duo, Umbrella, AnyConnect, Tetration and AMP.
- Cisco is new to public comparative testing, appearing in the NSS Labs test and one AV-Comparatives test. Its underlying antivirus engine (Bitdefender) is an active participant in tests.

CrowdStrike

CrowdStrike's cloud-native architecture provides an extensible platform that enables additional security services like IT hygiene, vulnerability assessment and threat intelligence. Its app store, the CrowdStrike Store, allows customers to acquire additional security functions, such as user and entity behavior analytics (UEBA) and file integrity monitoring, through partners that exploit the same client and cloud management console.

CrowdStrike has been a leader in the fusion of products and services, with very high adoption of the Falcon OverWatch service, which provides managed threat hunting, alerting, response and investigation assistance. CrowdStrike also offers the Falcon Complete service, which provides full managed detection and response, engagement consulting for incident response and a $1 million breach prevention warranty.

In 2018, Dell and Secureworks announced a strategic go-to-market alliance with CrowdStrike and the company launched a very successful IPO, improving its overall viability.

Organizations looking for a modern, cloud-native EDR-focused EPP solution with a range of managed services will find CrowdStrike very compelling.

Strengths

- CrowdStrike continues to be one of the fastest growing and most innovative vendors in this research. It is rapidly taking market share in 176 countries, including numerous very large organizations with more than 100,000 seats.
- Gartner clients report simple and easy Falcon deployments, in part due to the cloud architecture. 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. 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 via a machine learning antivirus engine.
- Recent improvements include vulnerability detection; discovery for Amazon Web Services (AWS) and for asset inventory; and security configuration for cloud assets. They also include Real Time Response and Real Time Query to enable remote commands on suspect machines; custom indicators of attack (IOAs) for detection and prevention; and blocking of driver-level ransomware attacks. CrowdStrike has also introduced Falcon for Mobile to isolate corporate apps from unmanaged devices.
- CrowdStrike is the first EPP vendor in this research to provide firmware visibility and vulnerability detection to reduce the risk of hardware-based attacks.
- CrowdStrike offers a FedRAMP-certified cloud in the U.S., and recently added a Germany cloud location for EU customer data.

- It offers agents for a broad range of endpoints and supports new Linux kernels in less than a week. It also added support for Oracle Linux and Amazon Linux.

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. Default cloud storage for full hunting and investigation data is very short (i.e., seven days) .
- The MITRE ATT&CK evaluation showed that CrowdStrike reported more detections with OverWatch than without, and some of those are delayed.
- The CrowdStrike/Splunk management interface is very capable, but it can be complicated; for example, searching requires the creation of scripts.
- The vendor does not offer a personal firewall, application control capabilities, configuration guidance or patch management to improve hardening of endpoints, but it has plans to add them via the CrowdStrike Store. Also, it does not have companion network security products.
- CrowdStrike does not offer an on-premises management console. Although it has enhanced client-based machine learning detection and pushed more Indicators of attack to the client to provide protection while offline, it still is not ideal for bandwidth-constrained or completely disconnected machines.

ESET

ESET provides ESET Endpoint Security, which is an EPP solution managed by its Security Management Center. It also provides an EDR solution called ESET Enterprise Inspector. ESET Dynamic Threat Defense — cloud-based sandboxing solution for detection of zero-day threats — and a Threat Monitoring and a Threat Hunting Service (managed services for its EDR) complete ESET's offering in the endpoint security space. ESET provides these solutions in a bundle called ESET Targeted Attack Protection, with ESET Threat Intelligence platform as an optional add-on.

ESET will appeal to globally distributed organizations looking for a comprehensive solution, and especially organizations that require an EPP solution with a particularly lightweight agent.

Strengths

- ESET is a long-standing EPP vendor with the sixth-largest market share by seat count. It has a large presence in the small and midsize business (SMB) segment, and in the European, Latin American and Asia/Pacific regions. The vendor also has a large presence in the consumer space.

ESET is a notable source of published security research, available through its WeLiveSecurity website.

- ESET is widely known for combining a lightweight client with the consistent performance of a solid anti-malware engine.
- ESET has a comprehensive set of capabilities, including a host-based intrusion prevention system (HIPS), ML-based detection, exploit prevention, detection of in-memory attacks and ransomware behavior detection.
- ESET provides its console in 21 languages and localized support in 38 languages, making the solution a good fit for globally distributed enterprises and enterprises requiring support in a local language.
- ESET customers praise the vendor's quality of customer care and service. In some countries, ESET offers complimentary implementation services.

Cautions

- ESET Cloud Administrator is for only the SMB client base. Enterprise customers looking for full functionality can use only hosted management servers. An enterprise cloud-based management console, ESET Security Management Center Cloud, is due in 2H20.
- 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 lockdown capabilities in its endpoint agent; instead, applications and executables are blacklisted by file hash or through HIPS control policies.
- The ESET macOS agent currently does not support real-time IOC search and does not integrate with EDR yet, leaving a visibility gap for many organizations. ESET macOS agent integration with EDR is due in 1H20.
- The role-based administration within ESET Enterprise Inspector allows only two user modes and lacks case and incident management workflows.
- Remediation options are limited. Certain remediation actions require moving from the separate Enterprise Inspector console back to the Security Management Center.

FireEye

FireEye is a platform vendor that provides endpoint, email, web, network and cloud security and threat intelligence, which are managed in the FireEye Endpoint Security console. Mandiant, the service arm of FireEye, provides a full range of security services and enjoys a high attach rate with the product.

The FireEye Endpoint Security management capability is deployed as a cloud-hosted solution or as an on-premises virtual machine or hardware-based appliance. FireEye's Helix is a security information and event management (SIEM)/security orchestration, automation and response (SOAR) solution that is included with the sale of the endpoint software.

FireEye's appeal to Gartner clients continues to be more as a holistic security platform provider with deep cyberthreat intelligence capabilities and less so as a product-specific security vendor.

Strengths

- FireEye Endpoint Security 4.5, shipped in late July 2018, introduced its MalwareGuard machine-learning-based engine for detection of malware threats alongside its existing Exploit Guard (exploit mitigation), signature-based malware protection and intelligence-based IOC detection capabilities.
- As a portfolio provider, FireEye has a broad set of security capabilities that allow it to integrate threat intelligence findings from across its full set of solutions and services to address multiple security use cases beyond endpoint security.
- FireEye Endpoint Security can pull forensic and threat artifacts, and it supports the acquisition of deleted or system-protected files without interrupting the operation of the system.
- FireEye Endpoint Security benefits from the threat intelligence from Mandiant's breach investigation team, as well as from FireEye products' shared threat indicators.
- FireEye offers global managed detection and response through two services: FireEye Managed Defense is a full security services offering, and its newly launched Expertise On Demand offering enables clients to tailor engagement to their specific needs on an a la carte basis. FireEye provides a complement of consulting, advisory and training services through its Mandiant brand that helps organizations at all stages of their security maturity.

Cautions

- FireEye has yet to offer a cloud-native multitenant SaaS offering, lagging some key competitors in the EPP market.
- FireEye Endpoint Security management console can be used for alert triage, policy management and threat investigations; however, more advanced use cases of incident handling, workflow and collaboration require the use of FireEye's Helix Security Platform.

- Some customers report the overall amount of time it takes to gather metadata, details and host information about a threat during an investigation is lengthy. Verbose historic data is not sent to Helix by default. Full stream-of-event data can be optionally sent to a Helix data lake or the customers' own data storage. Otherwise, EDR data is stored on the endpoint, which makes it subject to loss if the endpoint is inaccessible. Triage packages with more info are sent to the management console only when suspicious events trigger alerts and only stored for short periods of time.
- Manual remediation actions are very limited compared to other vendors. Support for automated configuration rollbacks or file restoration is included in the Helix Security Platform.
- FireEye's Threat Intelligence portal and user interface are not fully integrated into the user interface, requiring responders to manually investigate indicators in the FireEye Threat Intelligence portal.

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. Security Fabric enables existing Fortinet customers who are using multiple Fortinet products to have unified monitoring and control across different Fortinet devices in their network or across multiple networks..

Strengths

- Fortinet offers unified control and management across its multiple product lines through Security Fabric, and continues to focus on enhancements across the Security Fabric features. The Security Fabric-supported components are FortiClient, FortiGate firewalls, SIEM, access points, secure email and web application firewalls.
- 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.

Cautions

- 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. In 2018, FortiClient generated less than 1% of the vendor's revenue.

- The FortiClient Cloud go-to-market strategy is to target midmarket enterprises with up to 500 users. FortiClient is becoming more focused on the enterprise space, but more than 50% of its current installed base is in the midsize enterprise space, having less than 1,000 seats installed. Large enterprise will likely desire more granular policy options.
- FortiClient, together with FortiSandbox, provides only partial EDR coverage. Full EDR recording is not provided and detection is based on the logs collected from the endpoints rather than on the event recording. Full detection, investigation and response can only be performed by combining FortiClient with FortiAnalyzer, FortiInsight and FortiSIEM.
- FortiClient is not widely tested; it only appeared in the NSS Labs test.

F-Secure

F-Secure is a publicly listed security company based in Helsinki, Finland. F-Secure is known for its long track record of excellent test scores, lightweight and low-impact anti-malware detection with its cloud-based F-Secure Protection Service for Business (PSB) offering and its on-premises solution, F-Secure Business Suite. In May of 2018, the company launched its EDR solution, which provides visual investigation capabilities and visibility into application usage. In July 2018, F-Secure acquired MWR InfoSecurity. The acquisition gives additional threat hunting and advanced response functionality to F-Secure's existing MDR solution.

Strengths

- The company's PSB offering includes an array of features such as device control, web protection, vulnerability management and patch management. DataGuard, a ransomware protection capability, provides advanced protection of sensitive local and network folders by preventing modification, tampering or encrypting from unauthorized applications and users.
- F-Secure Radar provides vulnerability management capabilities that are integrated in the endpoint client (on-premises and cloud), and automation capabilities are provided via the management console.
- Clients report that F-Secure's Rapid Detection & Response Service provides strong security specialist review, analysis and response capabilities. Its Elevate to F-Secure service enables customers to get detailed analysis and investigation help from F-Secure specialists.
- Clients report that the F-Secure EPP solution is easy to deploy and maintain on Windows Mac and Linux.

Cautions

- F-Secure is late with an EDR capability. Threat hunting and query features in the solution were in beta deployment at the time of this analysis, and are thus immature compared to rivals.

- F-Secure's ransomware defense does not include the ability to roll back encrypted or infected files.
- On-premises deployment is targeted to customers that require more controls and more deployment options. Specifically, it offers more granularity in some of the settings and more flexible configuration of the data flows to optimize virus definition traffic.
- F-Secure's advanced internal threat hunting tools, in beta, are currently still in a separate console.

Kaspersky

Kaspersky is a private EPP provider headquartered in Moscow, Russia; founded and run by Eugene Kaspersky; and operated by a holding company in the United Kingdom.

Kaspersky launched its Global Transparency Initiative (GTI) framework, which offers actionable steps for organizations to ensure and verify that Kaspersky solutions meet corporate trust and compliance policies. It has also moved a large portion of its data processing operations to Switzerland to address customer concerns.

Kaspersky's researchers also publish primary research on active risks and trends, and provide community services to enhance its own products as well as providing an annual security analysts summit.

Strengths

- Kaspersky has one of the largest geographical footprints of the vendors in this research. The vendor's regional presence in Middle Eastern and African regions is unique in the industry.
- Kaspersky has a large R&D team, which allows for fast and frequent incremental product updates. Kaspersky develops its own products in-house and has not used the merger/acquisition route to extend its portfolio of products and services, which now provides EPP/EDR and managed services.
- Kaspersky's products consistently score high in external testing and have acquired a reputation among Gartner customers for strong prevention and detection capabilities. Kaspersky offers solutions for a broad range of server and endpoint types including monitoring of Docker containers.
- Kaspersky's EDR approach is to focus on automated detection and response to reduce the administrator burden. Detection and response can be extended to include visibility into network traffic utilizing the Kaspersky Anti Targeted Attack Platform (KATA) network component. The Kaspersky Private Security Network (KPSN) can be used in air-gapped networks.
- Kaspersky offers Incident Response and Managed Detection and Response (MDR) services that provide automated response as well as proactive threat hunting.

Cautions

- Kaspersky Endpoint Security Cloud (KES Cloud) was launched in September 2016, but still does not have significant traction with the Kaspersky user base; it is a simpler tool for less mature security organizations with fewer integration requirements. Kaspersky does not have an enterprise-class cloud offering; it is planned for launch in 3Q19.
- Although Kaspersky has integrated MITRE ATT&CK classification into its Kaspersky Endpoint Detection and Response (KEDR) tool and sandbox analysis capabilities for simpler threat identification, MITRE evaluations have yet been conducted for Kaspersky's EDR tools.
- The automated detection and prevention approach in Kaspersky Endpoint Security for Business (KESB) means that advanced EDR functions are lacking for mature SOCs. For example, threat hunting is weak; it is not possible to create a custom detection and block rule; remediation is limited to basic actions, and there is no summary of remediation actions to take; workflow is limited; and injecting IOCs is a batch process. Also, there is no community portal to share content. KEDR and/or KATA products are required for mature organizations with SOCs. Mature organizations with an SOC need to use KEDR and/or KATA for these advanced EDR functionalities.
- Use of Kaspersky products and services may be subject to restrictions currently in force in the U.S. and other regions for federal-regulated and government agencies. (In September 2017, the U.S. government ordered all federal agencies to remove Kaspersky's software from their systems. Several media reports, citing unnamed intelligence sources, made additional claims. Gartner is unaware of any evidence brought forward in this matter. At the same time, Kaspersky's initial complaints have been dismissed by a U.S. District of Columbia court. Kaspersky has launched a transparency center in Zurich where trusted stakeholders can inspect and evaluate product internals. Kaspersky has also committed to store and process customer data in Zurich, Switzerland. Gartner clients, especially those who work closely with U.S. federal agencies, should consider this information in their risk analysis and continue to monitor this situation for updates.)

Malwarebytes

Malwarebytes is best known for its malware removal capabilities, but it has a growing presence in endpoint protection and an emerging Endpoint Protection and Response solution. Both EPP and EDR modules are delivered via a single agent and are managed through a single, cloud-based management dashboard. Malwarebytes Breach Remediation (MBBR) provides an agentless remediation capability. Malwarebytes also offers an on-premises, managed EPP product.

Malwarebytes will appeal to organizations of all sizes that have limited cybersecurity resources and high remediation expenses.

Strengths

- Gartner clients praise Malwarebytes for its simplicity to use and its intuitive dashboard, as well as for its detection rates on long-tail malware and its malware remediation capabilities.
- Malwarebytes provides advanced remediation capabilities such as the ability to interact with processes, view and modify the registry, send and receive files, and run commands and scripts remotely.
- Malwarebytes' Endpoint Protection and Response product can roll back the changes made by ransomware, including restoring files that were encrypted in the attack. This action 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.
- Malwarebytes enterprise products integrate with operations suites such as IBM BigFix, Tanium, Phantom, ForeScout and Microsoft's System Center Configuration Manager (SCCM) through Malwarebytes Cloud Platform's available APIs.
- Its EPP capabilities do not require an internet connection to provide threat protection, allowing for protection for organizations with untethered endpoints that do not have network connectivity.

Cautions

- Malwarebytes is one of the smaller vendors in this analysis, and it lacks the scale of global operations of larger peers. Malwarebytes does not provide any managed services directly.
- Malwarebytes does not participate in regular tests of its anti-malware effectiveness. It only appeared in the NSS Labs test.
- Some large enterprise features, such as extensive role-based administration and support for non-Windows endpoints, are missing. Malwarebytes does not support application control or offer any vulnerability or configuration management capability.
- While Malwarebytes has gained recognition among Gartner clients for its malware prevention and remediation capabilities, it does not offer enterprise-grade EDR capabilities beyond attack visualization. It does not retain historic data, or enable hunting queries, searching for specific processes, alert automation and customized rules for event blocking.
- Although Malwarebytes has made some improvements to its cloud-based management dashboard, it is still lacking in visual reporting and quick-view dashboards.

McAfee

McAfee is a privately held security company. In 2018, McAfee launched MVISION, which delivers new products and functionality, branding and packaging, and simplified license options to better suit different markets. Uniquely, McAfee's standard endpoint offering provides flexibility to combine

McAfee's advanced detection capabilities, such as machine learning, credential theft monitoring, attack behavior blocking, and rollback remediation controls with native OS capabilities including Microsoft Windows Defender. McAfee's premium endpoint offer includes McAfee MVISION EDR capability. Notably, MVISION ePO uses a brand new cloud-native back end, while maintaining a consistent administrative experience with the on-premises version of EPO.

McAfee also offers additional security capabilities including network intrusion prevention, CASB, secure web gateway, DLP and endpoint encryption, which are managed by ePO and can exchange threat information via its Data Exchange Layer (DXL).

These changes are both welcome and timely, and will enable McAfee to offer more attractive SaaS hosted options.

Strengths

- MVISION EDR capabilities are comprehensive and flexible to work alongside (not instead of) Microsoft Windows Security. MVISION EDR can also be deployed stand-alone alongside other vendors' EPP products.
- McAfee's ePO management and reporting console can be consumed via a multitenant SaaS offering, hosted in a customer's AWS tenant or on-premises data center to suit a variety of preferences.
- MVISION EDR maps threats against the MITRE ATT&CK Framework; additionally, the automated AI-guided investigation capabilities use the MITRE ATT&CK Framework to drive faster, easier alert triage.
- Flexible cloud storage and retention options are provided along with real-time and historic threat hunting tools.

Cautions

- McAfee has been struggling to grow its EPP installed base.
- McAfee does not include any out-of-the-box vulnerability or configuration management capabilities.
- MVISION EDR does not yet include an extensive remediation capability or large, advanced SOC workflow features. The user interface has numerous capabilities, but does require extra steps to switch between different SOC tasks.
- The upgrade from older versions of McAfee ePO and McAfee VirusScan Enterprise to McAfee Endpoint Security (ENS) is not trivial and is still ongoing for some McAfee customers. Better migration tools have made this a less complex task and existing customers should upgrade ASAP.

- Cloud data storage in the standard SKU allows for examination of only seven days of historic data. This can be extended to 90 days at extra cost, but it is still less than competing EDR products.

- MVISION ePO SaaS has different capabilities than self-hosted ePO instances and vice versa. For example, multifactor authentication (MFA) and options to integrate with third-party SIEM, SOAR and other services are not yet available for self-hosted ePO instances. Some older McAfee ePO on-premises integrations are not yet available in the new MVISION ePO — such as granular role-based access control (RBAC) and workflow capabilities.

Microsoft

Microsoft is unique in the EPP space, as it is the only vendor that can provide built-in endpoint protection capabilities tightly integrated with the OS. Windows Defender Antivirus (known as System Center Endpoint Protection in Window 7 and 8) is now a core component of all versions of the Windows 10 OS, and provides cloud-assisted attack protection. Microsoft Defender Advanced Threat Protection (ATP) provides an EDR capability, monitoring and reporting on Windows Defender Antivirus and Windows Defender Exploit Guard ("Exploit Guard"), vulnerability and configuration management, as well as advanced hardening tools. The Microsoft Defender ATP incident response console consolidates alerts and incident response activities across Microsoft Defender ATP, Office 365 ATP, Azure ATP and Active Directory, as well as incorporates data sensitivity from Azure information protection.

Microsoft is much more open to supporting heterogeneous environments and has released EPP capabilities for Mac. Linux is supported through partners, while native agents are on the roadmap.

Microsoft has been placed in the Leaders quadrant this year due to the rapid market share gains of Windows Defender Antivirus (Defender), which is now the market share leader in business endpoints. In addition, excellent execution on its roadmap make it a credible replacement for competitive solutions, particularly for organizations looking to reduce complexity.

Strengths

- Defender provides malware protection using a range of techniques including behavioral, emulation, script analysis, memory scanning, network monitoring signatures and heuristics on the client, along with cloud protection engines to detect newer malware. Microsoft Defender ATP can work alongside some other vendors' EPP or EDR agents or will step up to protect clients automatically if a third-party EPP engine fails, is out of date or is disabled.

- Microsoft Defender ATP combines advanced EDR functionality with management and monitoring of Exploit Guard, Defender and other Microsoft products, critically Active Directory, to enable a common alert and incident response console. ATP leverages Azure infrastructure to store six months of data at no extra charge.

- Microsoft has one of the better out-of-the-box SOAR capabilities to integrate with Microsoft and partner products and to automate repetitive tasks. Conditional access rules enable a continuous adaptive risk and trust assessment (CARTA) architecture.

- ATP adds threat and vulnerability management, attack surface reduction (such as hardware-based isolation, application control, network protection and attack surface reduction rules) and threat analytics' contextual threat intelligence reports. Microsoft Secure Score and vulnerability and configuration information provide weighted recommendations and actions to improve endpoint hardening, and compare the current posture with the industry and global peers for benchmarking. This score gives admins and chief information security officers (CISOs) an excellent understanding of the overall security posture relative to peers and shows improvements over time.

- Microsoft recently launched a service called Microsoft Threat Experts to support customers' incident response and alert analysis.

Cautions

- Defender Antivirus and Exploit Guard are included with all versions of Windows 10. However, most enterprise buyers will want ATP to provide a competitive experience in EDR functions, such as attack visibility, reporting and threat hunting, as well as vulnerability management. ATP require an E5 license. Microsoft licensing is difficult to navigate and some customers report that E5 is more expensive than competitive EPP and EDR offerings.

- Although ATP is available for Windows 7 and 8, Microsoft's solution doesn't provide full feature parity with the security capabilities of Windows 10. ATP is not available for legacy XP and older. This will result in varying levels of protection in the organizations that have yet to fully migrate to Windows 10. EDR capabilities for macOS have not been released but are on the roadmap.

- Managing Microsoft security configuration settings in Group Policy Objects can be complex, especially for security teams that do not use System Center. Microsoft's roadmap includes consolidating all security policy objects into the security center by year end. In the meantime, customers can leverage Microsoft baselines and prebuilt GPO objects that customers deploy.

Palo Alto Networks

Palo Alto Networks is still best known to Gartner clients for its network and cloud security product lines, and this continues to be the main line of introduction for most of its customers to its EPP product, Traps.

Palo Alto completely rebuilt its EPP and created a new EDR offering with Traps 6.0 and Cortex XDR in February 2019 as a result of its Secdo and LightCyber acquisitions and internal development. This provides EDR, network traffic analysis (NTA) and UEBA capabilities that are integrated with Palo Alto's Next-Generation Firewalls, Traps, and cloud offerings for alert triage, incident response, and

hunting. Cortex XDR uses Palo Alto Networks products (such as Traps, Firewalls, etc.) as sensors to collect logs and telemetry data, or as a sensor performing collection and remediation functions only.

Strengths

- Traps provides solid exploit prevention to protect memory-based attacks that is not dependent on prior knowledge of threats.
- Traps does not rely on daily endpoint signature updates. Traps also offers local analysis, anti-ransomware and advanced malicious-behavior-protection-covering scripts for offline protection. It utilizes the cloud-based WildFire sandbox to analyze all unknown executable files as they are loaded, acting as a secondary validation.
- Cortex XDR collects and connects telemetry data from all Palo Alto products to correlate alerts and enable incident response actions from a single console. Cortex XDR converts related alerts into a single incident to reduce the number of alerts to be reviewed. Additionally the inclusion of network data in Cortex extends coverage into unmanaged and IoT-type endpoints.
- Palo Alto acquired Demisto, which provides a SOAR capability to improve orchestration and automation. It also has integrations with vendors such as Splunk, ServiceNow and Phantom.

Cautions

- Palo Alto has grown its presence in the EPP and EDR market primarily through acquisition of component parts it has integrated together.
- Traps is missing common enterprise EPP features, such as rogue device discovery, application control, USB device controls, resource utilization tuning, and extensive role-based administration. Palo Alto's EDR capability has limited workflow and no ability to create custom block rules.
- Palo Alto currently doesn't offer MDR/managed EDR (MEDR) services as part of its native offering and uses partner ecosystem for delivering these services.
- Palo Alto does not have vulnerability or configuration management information.
- While Traps is being licensed on an agent basis, Cortex XDR is sold based on storage size and period, in contrast to an agent basis, and it can only be purchased in discrete numbers of 1TB storage. Each TB license comes with 200 agent licenses included.
- Traps and Cortex XDR have two different management consoles; however, they are integrated to share data among each other and benefit from single sign-on for authentication, allowing analysts to switch between the two interfaces without reauthenticating.

Panda Security

Panda Security was one of the first vendors to deliver cloud-only products fused with services. The Adaptive Defense 360 solution combines an EPP and EDR product with managed services. Additional modules include system management, patch management, data control for regulatory compliance, BitLocker encryption management and a SIEM feeder service.

The first included service, 100% attestation, provides automatic whitelisting, where only trusted and approved applications and processes are able to execute. These are identified using predominantly automated processes, with additional manual inspection of the remainder by the vendor's experts.

The second service, Threat Hunting and Investigation, is led by Panda's own threat hunters and data scientists, with the option to add expertise via MSSP services where in-house capability is scant.

Panda recently launched a new brand, Cytomic, for more mature large enterprises. Cytomic delivers a product and service fusion that combines MDR services with an EDR functionality, called Orion, which delivers a management console for large enterprises to perform their own threat hunting reporting and investigations.

Strengths

- The 100% attestation service speeds and improves the classification and handling of all discovered executable files, whether malicious or benign, leading to fewer false positives.
- Comprehensive telemetry from endpoints is sent direct to a cloud database with a full 12-month retention capability and threat hunting across all endpoints in real time or using historic data.
- The new Orion and Jupyter Notebook capability, combined with an MDR service, add further appeal for organizations with SOC/threat hunting teams that want a fusion of product and services.
- Panda Security's Adaptive Defense 360 package represents good value and a full set of capabilities; plus, the two managed services are included as part of the product.

Cautions

- Cytomic and Orion products were only recently launched at the time of writing and are being offered only to select customers.
- Multifactor authentication for the console is limited to Google's authenticator service.
- Integration with other tools and services is limited, though support is provided for export to SIEM.
- Global presence is a goal for Panda Security; however, its current installed base is limited outside the EMEA region and tends to comprise small and midsize businesses.

- The Panda EDR capability without Cytomic is a very raw UI compared to competitive tools that are not linked to the MDR service. Services exposed to the administrator, such as remediation, are limited. The dependence on Jupyter Notebooks is a unique feature that can enhance the flexibility and usability of the Orion product, but will require training for the uninitiated.

SentinelOne

SentinelOne is a part of the new wave of private EPP solution providers that has rapidly grown over the past few years. Its solution is designed around an EDR agent that provides behavioral protection, and is offered both on-premises and cloud-managed. SentinelOne provides an MDR services via its Vigilance offering.

SentinelOne protection and detection logic resides on the endpoint agent, and the focus of the solution is on providing actionable insight without requiring manual analysis. SentinelOne was one of the first vendors to offer a ransomware protection warranty based on its behavioral detection and file journaling features.

SentinelOne is a match for organizations looking to augment existing EPP solutions with detection capabilities or to replace a legacy EPP with a newer approach to endpoint security.

Strengths

- SentinelOne's single-agent design provides fully integrated file and behavioral anti-malware, and EDR functionality. Recommended remediation actions are very clear and concise and can be executed from the management console.
- Agent performance is very good, particularly since the agents do the majority of the correlation on the endpoint.
- Vulnerability scanning is provided with the status of endpoints in the main dashboard. SentinelOne supports discovery of unmanaged endpoint-based network scanning, including IoT-type devices. Discovered devices are also cross-corelated with common vulnerabilities and exposures (CVE) info for vulnerability analysis.
- SentinelOne's "true context" offers real-time endpoint visibility for investigation. It also supports automated threat intelligence ingestion.
- SentinelOne supports endpoint rollback functionality by leveraging shadow copy to return a file to a previously known-good state.

Cautions

- SentinelOne's market presence is mostly in North America and EMEA.

- The vendor does not participate in regular malware prevention testing, although it does participate in the MITRE ATT&CK test and the NSS Labs test.
- SentinelOne does not offer application whitelisting, nor does it offer sandboxing for suspicious file analysis (local, network or cloud).
- While SentinelOne offers broad platform support, it does not support rollback on Linux and Mac due to operating system limitations.
- Workflow capabilities for large teams are limited. The EDR tool provides few guides or global contextual info. Watchlist alerts are limited to minimum three hours between runs, and thus, are not real time.

Sophos

Sophos offers a large integrated suite of security solutions spanning endpoint, mobile, network, email, public cloud, web, and managed detection and response. The company's flagship offering in the EPP space, Intercept X, has propelled Sophos beyond its SMB roots and increased its brand awareness in enterprise organizations.

In November 2018, Sophos entered the EDR market with Intercept X Advanced. Intercept X utilizes machine learning from its Invincea and SurfRight acquisitions and organically developed features. In January 2019, the company acquired DarkBytes, a startup specializing in endpoint forensics, to provide enhanced EDR capabilities. DarkBytes is now a foundational element of Sophos' managed detection and response services.

Strengths

- Intercept X clients report strong confidence in not only protecting against most ransomware, but also in the ability to roll back the changes made by a ransomware process that escapes protection.
- The analysis output of Intercept X deep learning algorithms is readily available, visually appealing to users and provides customers a demonstrable way to validate their use of deep learning.
- The exploit prevention capabilities focus on the tools, techniques and procedures that are common in many modern attacks.
- The Sophos Central cloud-based administration console manages other aspects of the vendor's security platform from a single console, including disk encryption, server protection, firewall and email gateways.
- Intercept X provides a simple workflow for case management and investigation for suspicious or malicious events.

Cautions

- Intercept X Threat Cause Analysis is not available for clients that use the on-premises version of Sophos Endpoint Protection. Indeed Sophos is intentionally focused on Sophos Central as the primary offering, and Sophos customers should expect it to receive the majority of development efforts.
- Customers should examine Intercept X EDR features in the Sophos Linux edition and determine if they fit their needs from a feature parity perspective.
- The Intercept X EDR workflow provides basic collaboration; however, customers must investigate whether their current offering provides advanced collaboration across incident response teams.
- Intercept X EDR full-journal forensic snapshot is stored on the endpoint, making it susceptible to tampering and difficult to query. Advanced hunting and custom detection rules require Forensic Console. The forensic console capability from the DarkBytes acquisition is not yet integrated into the Sophos Central management console or its on-premises console, and must be deployed separately with a separate agent. (An integrated agent is now in early access and is expected to be fully generally availability in September.)
- Some customers report that agent installs and software updates in low-bandwidth locations can be problematic.

Symantec

Symantec is an industry veteran and continues to be the leading competitive threat mentioned by other vendors in this research. Broadcom, a global semiconductor provider, announced an agreement to acquire the enterprise security business of Symantec on 8 August 2019.

Symantec launched Complete Endpoint Defense that includes Symantec Endpoint Protection 15 (SEP 15) cloud-managed EDR, and attack surface reduction capabilities, all delivered through a single agent. Symantec EDR has the largest EDR market share of the traditional vendors. In 2018, Symantec made a number of acquisitions including Javelin Networks to protect Active Directory, Appthority to provide mobile application testing and catalog of known-good mobile applications, and Luminate Security, which provides secure remote access to data center applications.

Symantec's strategic direction is to provide an Integrated Cyber Defense (ICD) Platform to unite the broader portfolio of security products (including DLP, Web Security Service [WSS] and CASB) with a consolidated agent, data and reporting platform for monitoring and incident response (ICD Manager).

Symantec remains a solid competitor and a good choice for most organizations.

Strengths

- Symantec has embraced a cloud-first strategy with the introduction of its latest product updates, including SEP 15 and EDR, which provide a cloud-based console with feature parity to the on-premises management console and ability to run hybrid scenario.
- Complete Endpoint Defense introduces new features such as deception breadcrumbs to improve detection of active attackers, application whitelisting capabilities, vulnerability detection and remediation, and a VPN. SEP 15 also introduced automated posture assessment including vulnerability management and remediation technology.
- Symantec EDR is a capable EDR tool with extensive APIs for integration and automation with other security and system management tools.
- Symantec provides a very comprehensive endpoint security solution, Symantec Complete Endpoint Defense (CED), which covers multiple areas to include anti-malware, EDR, app isolation, app control, Active Directory defense and cloud connect defense on PC, Mac, Linux and mobile devices. Symantec also offers vulnerability remediation and endpoint management, mobile security (SEP Mobile), and a managed EDR service.
- 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

- The acquisition by Broadcom was not factored into this analysis as the acquisition has not closed. The acquisition by Broadcom adds some uncertainty to Symantec's execution. Broadcom's goals may not align with Symantec's customers' aspirations for the products.
- Symantec's has undergone numerous management changes over the past several years, including the recent departure of its CEO and replacement of several key managers. Symantec has been gradually losing market share as the market becomes more competitive, and it has lost its first place in market share by seat licenses to Microsoft.
- Although Symantec has made significant investments in integrating its various products into a more cohesive middleware platform called Symantec Integrated Cyber Defense Exchange (ICDx), it is still lacking a universal incident response environment. However, Symantec does offer a rich set of APIs to integrate with other security tools.
- Symantec EDR is missing advanced functions for large enterprise customers, such as case management workflow, remote shell response function (due 1Q20) and rapid pivot capabilities from one query to another. EDR does not provide blocking rules although automated actions can be scripted for specific detections. The user interface lacks guided investigation tips or contextual

information, which makes it difficult to use for mainstream buyers. EDR and SEP are different management consoles.

- SEP 15 Cloud console is relatively new and, although Symantec reports 55% of customers are using cloud, the vast majority are not using SEP 15 Cloud console. SEP Cloud is not FedRAMP-certified.

Trend Micro

Trend Micro has recently revised its suite of endpoint protection products, introducing a combined EPP/EDR solution for endpoints, Apex One, as an upgrade to OfficeScan. Apex One enhances fileless malware detection and EDR functionality. Concurrently, Trend has also an expanded its cloud management capability, reaching feature parity across SaaS and on-premises. This now includes a fully cloud-hosted sandbox solution.

Trend Micro also offers two tiers of managed MDR services and has extended its MSP network.

Trend Micro was one of the first vendors to recognize the divergence in server protection strategies and to create a specific product line called Deep Security to address server protection.

Strengths

- Apex One retains the vulnerability assessment and virtual patching technology and adds detection classifications based on the MITRE ATT&CK matrices, automated response options, and new threat hunting options for organizations with proactive hunting teams.
- Deep Security for servers is tailored specifically for server workloads including virtualized workloads and containers. Trend is the only vendor in this analysis that offers IaaS marketplace consumption models for burstable workloads.
- Vulnerability management includes prioritization guidance linked to virtual patching to mitigate late-breaking threats and before traditional patches become available, with low impact or risk to the endpoint.
- Geographical presence in all global regions is a strength, and Trend also has an extensive partner and managed service capability in most regions. Regional hosting meets local/regulatory needs. It also provides more localization support and double-byte character set support than other vendors.
- Comprehensive OS support is provided in both the latest server and endpoint products, with an unusual capability to protect legacy and out-of-support OSs for customers with older systems.

Cautions

- EDR capabilities are more limited than some of the class-leading products. Notable omissions are extensive remediation options, advanced threat hunting, customizable behavioral rules and alerts,

and workflow. The investigation capability is complicated for a solution aimed at the midmarket.

- Trend has not fully leveraged the OS-provided Antimalware Scan Interface (AMSI) detection engines and other Windows 10-specific security enhancements; this is planned for 2H19.
- Servers and endpoints use different management consoles, although they both report into Apex Central.
- Trend customers wishing to migrate to Apex One must upgrade their local management server or migrate to the cloud management service. Customers with older perpetual licenses must pay to upgrade to cloud management.

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

Check Point Software Technologies was added back this year due to changes in the inclusion criteria.

Dropped

Endgame and Comodo did not meet the minimum business licenses inclusion criteria.

Inclusion and Exclusion Criteria

Gartner methodologies restrict the number of vendors in a Magic Quadrant to 20 vendors. In most markets, this is a reasonable restriction; however, the EPP market has more than 30 credible vendors. We changed the inclusion criteria this year to exclude smaller vendors.

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

- The vendor's nonconsumer EPP must have participated in independent, well-known, public tests for accuracy and effectiveness within the 12 months prior to 30 June 2019, or be a current participant in the VirusTotal public interface. Examples include MITRE ATT&CK Evaluations, Virus Bulletin, AV-TEST, AV-Comparatives, NSS Labs and SE Labs.
- The vendor must have a minimum of 4.5 million deployed licenses, protecting nonconsumer endpoints.

Honorable Mentions

Gartner surveyed 24 vendors for this analysis, and it was difficult to pare down the list to 20 vendors. The following vendors offer competitive products in this market with unique qualities and capabilities that clients may find valuable, but failed to meet all the inclusion criteria.

Cybereason

Cybereason is one of the new crop of vendors in the EDR market that have added EPP functionality. Its core differentiator is its cross-machine correlation engine that automatically combines alerts from all impacted endpoints into single alert for automated threat detection and that allows threat hunters to envisage attacks across multiple devices. It simplifies hunting for threats with a syntax-free UI. Cybereason provides a comprehensive EPP solution with both definition-based and machine learning detection. The same single agent also provides EDR capabilities with script control, behavioral analysis and deception techniques. Cybereason has made significant enhancements to both visibility and detection capabilities with a strong focus on the MITRE ATT&CK Framework. The company provides on-premises, cloud and managed service offerings. Unfortunately, it did not meet the market presence inclusion criterion, which required a minimum threshold of 4.5 million centrally managed license instances.

Comodo

Comodo's cloud-managed EPP product differentiators include a 100% file attestation capability, which resolves all unknown files, and a capability to run unknown or risky applications in a software-based isolated container. Comodo also offers a maturing EDR product. Recent improvements include: strengthened security policy for file-less attacks; improved HIPS; rule optimization to reduce false positives; detection of credential theft; and improved agent performance. Comodo also provides vulnerability and patch management and a network of cloud-delivered sandboxes for file analysis. Unfortunately, it did not meet the market presence inclusion criterion, which required a minimum threshold of 4.5 million centrally managed (excludes consumer) license instances.

Endgame

Endgame is one of the new crop of vendors from the EDR market that have added EPP functionality. Its core differentiator is ease of use and good efficacy test results with multiple major labs. Endgame provides a single-agent architecture and has feature parity across Windows, macOS and Linux. As well as providing full event fidelity, Endgame's EDR features remediation of exploits via guided response actions to revert damage to the system. Recent enhancements include: Reflex, an autonomous behavior detection engine and Artemis 3.0, which is a chatbot that provides security admins with a natural language interface for hunting and guided investigation and remediation. Endgame also provides instrumentation for detailed examination of PowerShell and other scripts. Unfortunately, it did not meet the market presence inclusion criterion, which required a minimum threshold of 4.5 million centrally managed license instances.

enSilo

The enSilo Endpoint Security Platform provides both EPP and EDR in a single, lightweight agent. enSilo features automated EDR response and vulnerability patching capabilities including virtual patching for latest threats. Stand-out features of enSilo's solution include patented technologies around code-tracing exfiltration detection and ransomware prevention. The vendor has automated incident response playbooks with actions that function across multiple types of endpoints and operating systems. enSilo provides full support for Windows Linux and OSX and has comprehensive support for down-level and legacy OS versions. enSilo is developing solutions for containers and serverless workloads. The platform can be deployed either in the cloud or on-premises. Protection and detection operate on the endpoint, not in the cloud, which makes it a good choice for disconnected endpoints. Unfortunately, it did not meet the market presence inclusion criterion, which required a minimum threshold of 4.5 million centrally managed (excludes consumer) license instances.

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 convergence of EPP and EDR products, cloud delivery and the fusion of managed services with the product. We also evaluated the ability of the vendor to provide timely improvements to its customers and licensing models such as perpetual license versus subscription.
- **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:** We evaluated the vendor's growth rate in licensed seats relative to the size of the organization and the installed base.
- **Market Responsiveness/Record:** We evaluated vendors by their market share in total customer seats under license.
- **Marketing Execution:** We evaluated vendor's execution of marketing initiatives such as social media interactions, fresh marketing messages, tradeshow representation, product testing participation, and press, which resulted in driving a differentiated brand awareness.
- **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 ↓	Weighting ↓
Product or Service	High
Overall Viability	High
Sales Execution/Pricing	Medium
Market Responsiveness/Record	High
Marketing Execution	Medium
Customer Experience	High
Operations	Medium

Source: Gartner (August 2019)

Completeness of Vision

The key Completeness of Vision criteria in this analysis were Market Understanding and 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:** This refers to 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. These include:

- 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.
- Hardening: This refers to the ability to detect rogue network agents that do not have the EPP agent installed via a network scan; vulnerability and configuration guidance to reduce the attack surface; as well as the ability to provide application control and ease of configuration of the EPP product.
- Incident prevention capabilities: We evaluated the test results of vendors to detect common file-based attacks, and gave extra credit for enthusiastic and consistent test participation.
- Detection and remediation: We look for vendors that provide educated guidance for customers to investigate incidents, remediate malware infections and provide clear root cause analysis. 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.
- Supported platforms: Several vendors focus solely on Windows endpoints, but the advanced solutions can also support macOS with near parity of the features delivered in both clients, notably in the activity and event monitoring areas of EDR.
- Product and services fusion: We evaluated the range of vendor direct services to support EDR deployments and incident response, from light monitoring to full managed detection and response and on-the-ground incident responders.

- **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, including localization, as well as the number of languages supported.

Table 2: Completeness of Vision Evaluation Criteria

Evaluation Criteria ↓	Weighting ↓
Market Understanding	High
Marketing Strategy	Low

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

Source: Gartner (August 2019)

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 late with new capabilities, lack some advanced capabilities, 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 and have yet to accumulate significant market share. 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

The endpoint protection market is undergoing its biggest transformation in the past 20 years. Three disruptive trends are at play in this transformation:

- There has been a shift from client/server architecture to more agile cloud-native solutions and services (see "Innovation Insight for Cloud Endpoint Protection Platforms").
- The failure of traditional approaches to address the volume of portable, executable file-based attacks, and the shift to fileless attacks, has opened up the market to new approaches including machine learning and behavioral detection.
- The security mindset has shifted to acknowledge that prevention alone is not enough; security and risk management leaders must be able to more easily harden endpoints and perform more detailed incident response to resolve alerts.

As a result, security and risk management leaders responsible for endpoint protection must reevaluate their endpoint protection solutions and make plans to address the changing market landscape.

Specifically security and risk management leaders responsible for the security of networks and endpoints should:

- Evaluate cloud-delivered solutions, seeking a truly elastic and agile cloud-native architecture.
- Favor solutions that are supported by a range of vendor-delivered service options, such as incident response assistance and managed detection and response services.
- Seek fully integrated EPP solutions with EDR capabilities that use the same detection funnel, data repository, management console and agent.
- Ensure that EPP detection capabilities include more-modern behavioral approaches that are immediately adaptive to detect or block new attack techniques.

- Favor vendors that can help harden the endpoint against attacks that target vulnerabilities and common misconfigurations.

Market Overview

The rapid growth of frequent disruptive attacks such as ransomware and the migration of more persistent attackers to fileless techniques, combined with the growing security skills shortage, has ushered in a new age for endpoint security solutions.

The most disruptive change is the shift from LAN-managed endpoint security solutions to cloud-delivered solutions. Cloud-delivered products reduce the maintenance burden of EPP solutions, specifically the crucial task of staying on the latest releases. Too many customers are suffering breaches because they simply do not have the time to update to the latest EPP version. However, not all cloud-delivered solutions take full advantage of modern cloud architectures to deliver adaptive and extensible solutions to address the continuously changing threat landscape. (See "Innovation Insight for Cloud Endpoint Protection Platforms.")

The integration of and endpoint detection and remediation capability is the second most significant trend in the EPP market; in many cases, with solutions having feature parity across the board under a single agent and console. EDR brings critical incident response visibility, search, a threat hunting capability, and, most importantly, a better detection capability that is based on behavior modeling rather than IOCs. Known-attacker behavior is a much smaller and more stable detector of malicious intent than traditional IOCs (see "Market Guide for Endpoint Detection and Response Solutions").

The skills requirement of EDR solutions compounded by the skills gap in most organizations is an impediment to the adoption of EDR in the mainstream market. As a result, product vendors are increasingly offering a fusion of products and services ranging from light incident response and monitoring through full managed detection and response and consultative incident response services.

Finally, there has been a great deal of investment made into endpoint hardening. Solutions are increasingly providing application and device control, vulnerability and configuration management, patching, and community portals where administrators and incident responders can share insights and proactive detection and reactive hunting rules.

Evidence

The Magic Quadrant team relied on data from the following sources to complete this iteration:

- Gartner responded to more than 1,500 client inquiries since 24 January 2018.
- Gartner conducted an online survey of 157 EPP reference customers in 3Q18.
- Data from more than 5,000 Peer Insights reviews on gartner.com.

- Data from a 200-question survey and one-hour demonstrations provided by each vendor conducted in 2Q19.

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.