Gartner

Magic Quadrant for Endpoint Protection Platforms

Published 5 May 2021 - ID G00450741 - 62 min read

By Analysts Paul Webber, Peter Firstbrook, Rob Smith, Mark Harris, Prateek Bhajanka

Initiatives: Infrastructure Security

This Magic Quadrant assesses the innovations that allow organizations to protect their enterprise endpoints from attacks and breaches. Technologies and practices in this space are being shaped by two trends: the continued growth and stealth of endpoint attacks and the sudden surge in remote working.

This Magic Quadrant is related to other research:

View All Magic Quadrants and Critical Capabilities

Strategic Planning Assumption(s)

By the end of 2023, cloud-delivered EPP solutions will exceed 95% of deployments.

By 2025, 50% of organizations using EDR will use managed detection and response capabilities.

By 2025, 60% of EDR solutions will include data from multiple security control sources such as identity, CASB and DLP.

Market Definition/Description

Gartner's view of the endpoint protection platform (EPP) market is focused on transformational technologies or approaches delivering on the future needs of end users. It is not focused on the market as it is today.

Gartner defines the EPP market as follows:

Endpoint protection platforms provide the facility to deploy agents or sensors to managed endpoints including PCs, servers and other devices.

These are designed to prevent a range of known and unknown malware and threats and to provide protection from such threats; in addition, they provide the ability to investigate and remediate any incidents that evade protection controls.

The core functionalities of an endpoint protection platform are:

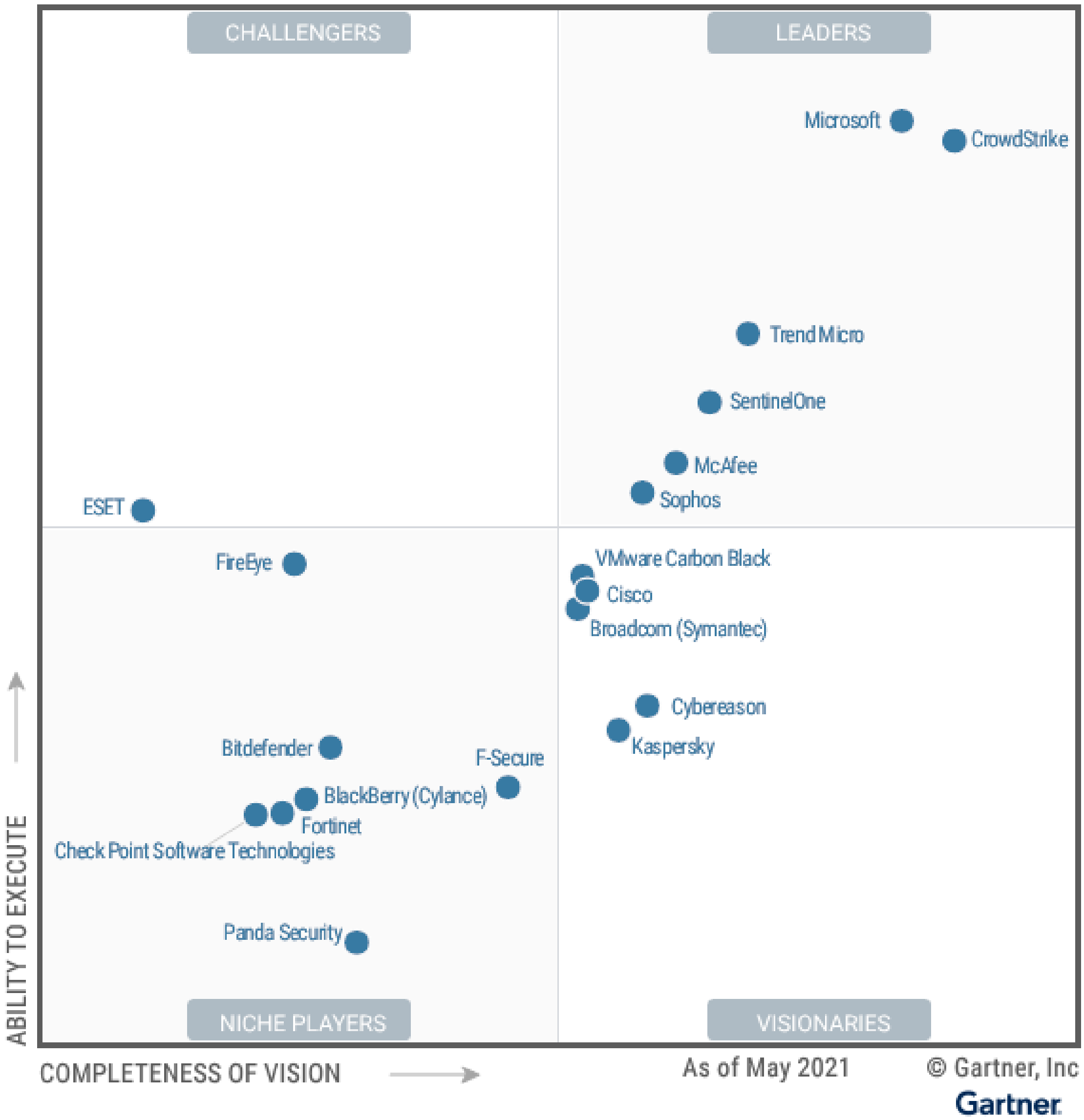
- Prevention and protection against security threats including malware that uses file-based and fileless exploits
- The ability to apply control (allow/block) to software, scripts and processes
- The ability to detect and prevent threats using behavioral analysis of device activity, application and user data
- Facilities to investigate incidents further and/or obtain guidance for remediation when exploits evade protection controls

Optional capabilities often present in endpoint protection platforms may include:

- The collection and reporting of inventory, configuration and policy management of endpoint devices
- The management and reporting of operating system security control status such as disk encryption and local firewall settings
- Facilities to scan systems for vulnerabilities and report/manage the installation of security patches
- The capability to report on internet, network and application activity to derive additional indications of potentially malicious activity

Magic Quadrant

Figure 1: Magic Quadrant for Endpoint Protection Platforms



Source: Gartner (May 2021)

Vendor Strengths and Cautions

Bitdefender

Bitdefender is a Niche Player in the 2021 Magic Quadrant.

The GravityZone platform combines EPP, endpoint detection and response (EDR) and network analysis as a cloud-hosted or on-premises solution. Bitdefender also offers a managed detection and response (MDR) service.

Bitdefender continues to invest in improved detection accuracy, hardening and patch guidance. It provides good agent performance as well as support for a broad range of OS.

Bitdefender is best for Type B and Type C organizations and suits those in North America and EMEA that want a well-rounded, single solution.

Strengths

- Bitdefender has a large R&D team that focuses on threat research and that is a consistent top performer in file-based and fileless 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. It also offers complementary security tools for midmarket enterprises, such as patch management, email filtering, mobility management and file sandboxing.
- A low-overhead EDR product supported by many detection layers and automated response actions leads to high ranking for customer experience. The incident response UI provides a good visual analysis capability and detail on suspect behavior mapped to MITRE techniques.
- Bitdefender provides a number of features that can decrease the attack surface of the endpoint, including user risk, application control, vulnerability and configuration management, patching, full-disk encryption, web content filtering, and device control.

Cautions

- The Bitdefender EDR capability lacks advanced threat hunting, automated threat feed integration, custom blocking rules, advanced role-based administration and an incident-handling workflow.
- The Bitdefender Patch Management module, firewall module and sandbox analysis features are not yet available for the Linux platform.
- The application control 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 and is reflected in a low ranking for market responsiveness.

BlackBerry (Cylance)

BlackBerry is a Niche Player in this Magic Quadrant.

BlackBerry recently rebranded all Cylance products including the EPP tool, now BlackBerry Protect; the EDR tool, now BlackBerry Optics; and its MDR offering, now BlackBerry Guard.

Investment areas include new Spark Suites, combining BlackBerry's unified endpoint management tool with its unified endpoint security tool that also includes the new BlackBerry Persona, which incorporate continuous user authentication to proactively address stolen credentials, insider threats and physical device compromises.

BlackBerry is a good option for Type B and Type C organizations looking for cloud-managed capabilities that have a low performance impact and work well offline. The majority of BlackBerry clients are in North America.

Strengths

- BlackBerry offers the BlackBerry Cyber Suite of EPP, EDR, mobile threat defense (MTD), and Persona, which operates under a single console. Cyber Suite provides customers with better visibility, easier management and increased threat detection across all endpoint device types.

- BlackBerry Protect is a small, lightweight, artificial intelligence (AI)-based detection agent that is easy to deploy and manage and is able to work offline, which is popular with customers who have isolated/air-gapped systems.

- BlackBerry Protect has a strong reputation for machine learning (ML)-based protection. This protection uses agent-side algorithms with machine learning to detect file-based malware. BlackBerry Optics uses ML to provide user and entity behavioral detection capabilities.

- BlackBerry Optics delivers EDR capabilities to provide endpoint visibility and incident response facilities. Its recent release expanded custom detection logic and added new response capabilities that incorporate the MITRE ATT&CK framework.

Cautions

- BlackBerry continues to suffer from branding problems across its entire product range as most clients do not associate Cylance as being part of BlackBerry. The removal of the Cylance brand requires significant client education as most users know BlackBerry as a historic mobile device manufacturer.

- BlackBerry's plans to release an extended detection and response (XDR) solution for BlackBerry endpoint security tools comes after other vendors; thus, BlackBerry does not rank highly for market responsiveness in this research.

- BlackBerry Optics lags behind competing products in development and release of new features due to the company transitioning Optics to a cloud-hosted EDR architecture, with version 3 expected to be released in 2Q21.

- Clients frequently report a high level of false positive detections when using BlackBerry Protect, requiring careful folder exclusion management. They also cite the need to add BlackBerry Optics for behavioral-based detection to improve detection results.

Broadcom (Symantec)

Symantec is a Visionary in this Magic Quadrant.

Symantec's position reflects it's go-to-market strategy and execution, which left thousands of its customers scrambling to find support or alternatives.

Symantec's new focus on its largest customers has had some success upselling larger enterprises its broader portfolio of products. It relies on a global network of partners to service small and midsize business (SMB) customers.

Symantec's flagship solutions, Symantec Endpoint Security Enterprise (SESE) and Symantec Endpoint Security Complete (SESC) provide cloud-managed EPP and EDR. Symantec's wide portfolio of solutions share a cloud console.

Symantec appeals to large global Type A and Type B enterprise customers that are looking for an integrated XDR security solution with attractive pricing.

Strengths

- The integration of EDR and EPP features into a single agent and cloud management console, and broad endpoint (including mobile) and server coverage are key strengths. Symantec continues to do well in testing of antivirus effectiveness, and it participated in the MITRE ATT&CK Phase 2 and 3 evaluations in 2019 and 2020.

- Symantec Endpoint Security Complete includes attack sSurface reduction, mobile threat defense, EDR, and critical incident discovery by Symantec's Threat Hunter analysts. In addition, Endpoint Threat Defense for Active Directory improves protection against identity-based attacks.

- Symantec improved its EDR capability with better visualization of process lineage and behavior to identify the root cause, built-in playbooks to facilitate analyst workflows, automated and manual threat hunting using cloud analytics, and remote PowerShell sessions for investigation and remediation.

- Customers adopting Symantec's Integrated Cyber Defense will be able to leverage insights from multiple control points for extended detection and response.

Cautions

- The acquisition by Broadcom had a rocky start with confusion in the channel and poor communication with customers. Broadcom's focus on selling a broad portfolio of products and services to large enterprise accounts may not align with current and prospective SMB organizations, especially those that favor a direct support relationship with their EPP vendor.

- In 2020 Symantec stopped offering direct MDR and other managed services to enterprise customers, lowering the score for managed services.

- Symantec's XDR strategy still lacks prebuilt granular incident response and automation capabilities, relying instead on API-based integrations with third-party security information and event management (SIEM) and security orchestration, analytics and reporting (SOAR) solutions.

- SESC is increasingly designed for large enterprise organizations with experienced security operations center (SOC) teams. Its range of controls and policies may be excessive for smaller organizations with less experienced administrators.

Check Point Software Technologies

Check Point Software Technologies is a Niche Player in this Magic Quadrant.

At the start of 2021, Checkpoint rebranded It's SandBlast Agent solution under the Harmony brand. Harmony provides automated remediation of detected threats and protection and detection capabilities including machine learning, behavioral analysis and automated sandbox analysis. Recent development improved integration with the Check Point firewall, integrating monitoring and threat hunting across multiple products.

Check Point is present in all regions and its products suit all types of organization that are existing Check Point customers.

Strengths

- Check Point reported significant growth for its Harmony solution, which is offered as cloud and on-premises. While principally deployed as cloud, the on-premises option makes it popular in industries that do not wish to use cloud-based technology. It also scores highly for customer experience in 2020.
- Harmony includes a wide variety of protection technologies such as email phishing protection, content disarm and detection of reuse of corporate credentials. There is a strong integration with the network sandbox, and this even includes a video of the file during analysis.
- The user interface has also been significantly redesigned to make it more modern and streamlined. A lot of emphasis is put on automated remediation of threats, from analysis of the attack chain to automatic removal of artifacts. This makes it suitable for less mature security organizations and speeds up the remediation.
- Harmony also covers mobile platforms such as Android and iOS. The wide range of security products from Check Point provides opportunities for consolidation and integration to simplify operations and security. The Harmony suite brings together several of these in a single package to address the challenge of remote working.

Cautions

- The emphasis on automated remediation means that Check Point has only very recently added to Harmony some of the threat hunting and investigation capabilities of other solutions, such as remote access to an endpoint for those cases where the automatic remediation has missed something.
- Harmony has a larger footprint than many solutions, both in memory and the number of services and processes used when all components are installed. Despite using machine learning and behavior-based detection, Harmony includes signature-based protection that needs to be updated on a regular basis.
- Check Point scores lower for marketing strategy and execution in 2020 and has failed to demonstrate a strategy that competes with the leading vendors despite having a competitive product set and the potential to reach a wide market through its networking solutions.
- Check Point has limited managed service offerings.

Cisco

Cisco is a Visionary in this Magic Quadrant.

Cisco's SecureX solution is an XDR platform that integrates its Secure Endpoint's EPP and EDR with security analytics, threat hunting and threat intelligence in a single view to investigate and respond to threats. Cisco Threat Response is now called SecureX threat response and is the investigation and response feature within SecureX.

SecureX is cloud-native, built into every Cisco Security product and provides centralized orchestration for each product. SecureX also integrates with a wide range of third-party solutions.

As well as investing in the creation of the SecureX platform, Cisco has enhanced and simplified threat hunting capabilities with the Orbital Advanced Search capability and associated automated playbooks.

Cisco's focus is on the North America and EMEA markets, with a presence in Asia/Pacific and Japan, and South America. Most Cisco customers are Type A and Type B enterprises.

Strengths

- Cisco is rated high for market understanding in 2021. Cisco augments its SecureX threat response capabilities with Talos threat intelligence, network and endpoint behavioral analytics, case management, and hunting, plus cross-product response and investigation capabilities.

- Cisco Secure Network Analytics (Stealthwatch) network flow data is aggregated into the console for proactive alerting from both Cisco's own network appliances and other vendor's devices alike.

- Cisco introduced improvements such as automated playbooks and simplified threat hunting via the recently developed Orbital query capability, and threat hunting by Cisco specialists to appeal to organizations with mature SOC teams; the automated playbooks will appeal to resource-constrained SOC teams.

- Cisco has a broad variety of training, managed services and reseller channels around the globe and offers a Managed Detection and Response service as well as an incident response service via Talos threat intelligence for customers that prefer managed services.

Cautions

- While the Cisco Secure Endpoint agent has benefited from the inclusion of third-party in-memory exploit prevention, overall, its detection capabilities are not as comprehensive as those of the leading solutions in this Magic Quadrant.

- While the Windows agent has gained useful additional capabilities via AMSI and MITRE ATT&CK integrations, the capabilities for macOS and Linux OS are less comprehensive.

- Remote shell facilities do not match those of the best EDR providers in this Magic Quadrant, leading to lower product and service scores than leading competitors.

- Cisco's SecureX XDR platform appeals more to customers who also have Cisco network solutions (e.g., Firepower or Identity Services Engine [ISE]), or the Duo authentication, Umbrella cloud security and AnyConnect VPN via the common endpoint agent.

CrowdStrike

CrowdStrike is a Leader in this Magic Quadrant.

Its Falcon platform includes an EDR product that focuses on detection and response capabilities to identify and remediate advanced threats; however, it also has file-based malware prevention exploiting static and behavioral ML to protect against known threats.

CrowdStrike continues to invest in additional features, for example, with the acquisitions of Preempt Security and Humio for its platform, and has introduced advanced firewall management as well as mobile device protection options.

CrowdStrike is present mainly in North America and EMEA. Products suit Type A and Type B organizations, with options for Type C organizations without security staff to consume managed services; either partially or fully managed.

Strengths

- CrowdStrike Falcon provides all core EPP capabilities in a single agent, with customers appreciating the low resource utilization and storefront for add-on third-party solutions. An easy-to-use management console and simplified deployment experience add to the high rating for market understanding and innovation.
- CrowdStrike has a strong reputation in the market as the single solution for endpoint security for organizations looking to consolidate their EPP and EDR agents/solutions. Falcon X threat intelligence and Threat Graph cloud-based data analytics provide the ability to detect advanced threats and analyze user and device data to spot anomalous activity.
- CrowdStrike has strong brand awareness and has built a reputation around its professional services. The Falcon OverWatch and Falcon Complete services are highly rated and popular with customers who don't have their own SOC/threat hunting teams and those wishing to mature/augment their internal security operations teams.
- CrowdStrike has a customer base that is highly targeted by attackers. As a result, it has consistently adapted early to shifts in attack techniques. It achieved positive results in the MITRE Phase 2 evaluations with consistent identification of tactics and techniques.

Cautions

- CrowdStrike Falcon deployments often require extra cost options to provide the full range of capabilities, and this increases overall cost when compared to more inclusive competing solutions.

Also, for multiyear contracts, CrowdStrike insists on upfront payment. This is reflected in lower scoring for pricing in this Magic Quadrant.

- Threat Graph Standard retains just seven days of enriched sensor data in the standard option; longer retention options are available as add-ons, which are shorter than the default retention period of other participants in this research. However, detection-related details and summaries are available for 90 days and one year respectively, across the options.
- CrowdStrike has been slow to meet the demand for security of serverless cloud systems and runtime protection for container workloads, although container runtime security capabilities were announced in February 2021.
- Despite the acquisition of Preempt Security and new partnerships with Proofpoint, Netskope and Okta, CrowdStrike's platform is not considered a strong XDR solution yet. However, CrowdStrike has recently announced the acquisition of Humio, which should strengthen its XDR story.

Cybereason

Cybereason is a Visionary in this Magic Quadrant.

The Cybereason Defense Platform is a cloud-native solution that provides EPP and EDR functions. It also offers a mobile threat defense solution, managed detection and response, and incident response services.

Cybereason has invested in automation of SOC activities as well as in its AI hunting engine.

Cybereason is suitable for Type A and B organizations. Its managed services make it attractive to Type C organizations looking to outsource.

Strengths

- The Cybereason Defense Platform collects a comprehensive near-real-time stream of endpoint telemetry in the cloud and correlates both known malware and behavioral detections for unknown malware across multiple assets to show the full attack timeline. The solution can also consume data from select network, domain controllers and other external sources such as Office 365 and G Suite.
- The management console is efficient and easy to use. Threat investigations are aided by root cause analysis, visual investigations, automation and a custom detection capability. Remediation options are automatically created and can be initiated from the console across all affected machines. Manual remediations are aided by a remote shell. Quick triage actions such as kill process, quarantine or isolate can be manual or automated.
- Cybereason is enhancing integration capabilities via partner products providing actions such as deactivating or suspending accounts, forcing multifactor authentication (MFA) or deleting messages in email inboxes.

- Cybereason offers an on-premises or hybrid deployment option, and supports Windows, Mac, Linux and mobile coverage; in addition, it offers support for containers with agentless protection in Kubernetes nodes. PC policy options include control of Microsoft personal firewall, disk encryption and USB protection from the console.

Cautions

- While global headquarters are located in the United States, market share and mind share in the U.S. are still low for Cybereason.
- The solution does not offer any hardening guidance, such as vulnerability or configuration management or reporting.
- Cybereason does not offer any network sandbox solution or related gateways, such as secure email gateway (SEG) or secure web gateway (SWG), although it does have API and syslog data integration with G Suite and Office 365.
- Third-party integrations in the newly announced XDR platform are limited, and Cybereason does not yet have additional telemetry sources of its own, such as network or identity data.

ESET

ESET is a Challenger in this Magic Quadrant.

ESET's product collection includes Endpoint Security (EPP), Enterprise Inspector (EDR), Dynamic Threat Defense (sandbox), Threat Intelligence and managed services.

ESET's flagship product, ESET PROTECT Enterprise, has been enhanced with cloud management, browser anti-tampering functionality, Windows Management Instrumentation (WMI) scanning, and management of Apple FileVault 2 encryption.

ESET will appeal mostly to smaller Type B and Type C organizations for a solid EPP and EDR solution with a lightweight agent that can be managed with on-premises servers.

Strengths

- ESET combines a lightweight client with a solid anti-malware engine that gets consistently good malware effectiveness test results. It was an early adopter of machine learning techniques. ESET is a notable source of published security research, available through its WeLiveSecurity website.
- ESET recently added more support for fileless malware with WMI and registry scanning, script-based detections and PowerShell execution scanning.
- The ESET management console is available in 23 languages, making the solution a good fit for globally distributed enterprises and enterprises requiring regional localization.

- ESET customers praise the vendor’s quality of customer care and service. In some countries, ESET offers complimentary implementation services.

Cautions

- ESET was slow to fully embrace enterprise-level EDR capability and cloud product delivery.
- ESET protect cloud does not manage the Enterprise Inspector, or agentless virtualization security.
- ESET does not offer direct-to-customer MDR services; instead, it relies on exclusive partner delivery in select regions.
- ESET does not offer any vulnerability or configuration management capability to help proactively harden endpoints.

FireEye

FireEye is a Niche Player in this Magic Quadrant.

FireEye‘s XDR platform provides endpoint, email, web cloud, SIEM and network security, all supported by a common SOAR console. Mandiant, its service arm, has security services suiting targeted industries. FireEye is reportedly growing in line with the market.

Recent investment has been in prevention and investigation, plus detection and expansion of Linux and macOS capabilities (macOS Big Sur support), identity deception breadcrumbs, remote shell and PowerShell malicious event detection.

FireEye Helix is a cloud-hosted XDR platform; but FireEye does offer an endpoint management console that can be hosted locally.

FireEye’s appeal is mostly to Type A organizations that need a holistic security platform with deep cyberthreat intelligence capabilities and services, and that see it less as an EPP-specific security vendor.

Strengths

- FireEye Endpoint Security provides multiple prevention engines for endpoint threats and ransomware. It includes the Bitdefender antivirus engine, which blocks highly prevalent malware; and MalwareGuard, the FireEye machine learning engine for unique malware. EDR hunting capabilities include query of real-time data on endpoints, as well as less verbose streamed events and metadata to Helix.
- As a portfolio provider, FireEye has a broad set of security capabilities that allow it to coordinate threat intelligence findings across all security control points and to provide integrated incident response. FireEye Endpoint Security benefits from the threat intelligence of Mandiant’s breach investigation team, as well as from FireEye products’ shared threat indicators.

- FireEye remediation options include pulling full forensic and threat artifacts, and the acquisition of deleted or system-protected files (without interrupting the operation of the system), plus real-time commands and batch scripts.
- FireEye offers global managed detection and response through two services: Mandiant Managed Defense, a full security services offering; and its newly launched "Expertise on Demand" that enables clients to tailor engagement to their specific needs.

Cautions

- FireEye is still lacking a cloud native EPP/EDR SaaS management offering for organizations that do not want to standardize their SOAR strategy around Helix.
- The management console is designed for more seasoned incident responders. The remediation capability is enhanced this year with reverse shell capabilities; however, investigation and remediation guidance are still weak.
- FireEye's default is to store data locally on the client and send more complete triage information only if suspicious activity is detected. Local data can be inaccessible during an incident. The Event Streamer module is required to stream data in syslog format for centralized storage.
- FireEye lacks some common features such as port control and mobile threat defense, and does not provide system hardening guidance.

Fortinet

Fortinet is a Niche Player in this Magic Quadrant.

Fortinet is a platform vendor providing cloud security, firewalls, email security, sandbox and endpoint security software, and more. The 2019 acquisition of enSilo provided a much needed EDR capability with telemetry to boost XDR facilities.

2019/2020 investment focused on enhancement of the newly acquired enSilo EDR and integration with the Fortinet Security Fabric and introduction of FortiXDR. FortiEDR enhancements include attack surface reduction, vulnerability scanning and application/enterprise Internet of Things (IoT) discovery tools.

Fortinet is present globally, with products well suited to Type B and Type C organizations seeking an integrated XDR security platform.

Strengths

- Customers who are using multiple Fortinet products have unified monitoring and control across different Fortinet devices in a single console. FortiClient integrates seamlessly into this ecosystem. This is especially useful for posture checking of remote users as they connect into the corporate VPN to ensure a device is meeting IT compliance requirements.
- FortiClient and FortiEDR both have a minimal agent footprint and are easy to deploy and manage.

- FortiClient and FortiEDR have broad platform coverage covering most major Linux distributions.
- FortiEDR has significantly improved over the past year with Fortinet's acquisition of enSilo.

Cautions

- Gartner sees little adoption of Fortinet's endpoint security solutions outside of Fortinet's network security client base.
- Fortinet's core focus is on a complete security ecosystem where endpoint security is just one component. Individually, the feature set of FortiClient is less complete than the EPP component of the leading vendors in this research.
- FortiClient only offers content filtering for mobile with no current plans to integrate MTD as part of the solution.
- FortiNet did not participate in the MITRE ATT&CK Phase 2 evaluations in 2019 and the effectiveness of its full kill chain capability using both FortiClient and FortiEDR together has therefore not yet been assessed in public testing. However, Fortinet has participated in the Phase 3 evaluations, although the results were not available at the time of this research.

F-Secure

F-Secure is a Niche Player in this Magic Quadrant.

F-Secure has a track record providing endpoint protection with expert managed services, adding EDR and its Countercept MDR service in 2018 and introducing threat hunting from 1Q20.

Recent investment has included development of advanced ML models and anomaly detection via its Blackfin AI research stream and new threat hunting capabilities.

F-Secure's main market is the EMEA region, with a presence in all other global regions. F-Secure customers are typically Type B and Type C midsize and smaller enterprises, while Countercept MDR service and Consulting customers are commonly large enterprises.

Strengths

- F-Secure made incremental improvements to Linux protection, agent resource utilization and deployment options in its cloud solution. Windows and Mac agents now have added response options including automation, broader detections for Mac and Linux, and improved patch management.
- Protection of servers has also been enhanced, providing application control, anti-tamper and ransomware resilience in the DataGuard facility, and flexible usage-based monthly subscriptions.
- Threat hunting is now part of the EDR solution together with newly developed Blackfin device-level AI to detect anomalous activity and provide more automated response opportunities.

- Scoring well for innovation in this year's Magic Quadrant, F-Secure's EDR product is easy to set up and consume, and has a unique option to elevate alerts to F-Secure's threat hunters directly from the console, with a two-hour SLA.

Cautions

- F-Secure has more limited third-party SIEM and SOAR integration opportunities than the leading solutions in this research. While its XDR platform is limited to EPP/EDR and Microsoft 365 telemetry today, broader capabilities are on the roadmap. These points lead to a low Completeness of Vision rating.
- Though F-Secure is targeting expansion into the North American market primarily with its Consulting and MDR business, there are more established competing EDR solutions for customers in this region.
- F-Secure has been slow to develop native cloud workload protection and container and serverless solutions, and is therefore not a preferred option for organizations deploying these workloads.
- F-Secure does not have the global reach or breadth of some of the leading vendors in this research and consequently scores lower for geographic coverage.

Kaspersky

Kaspersky is a Visionary in this Magic Quadrant.

Kaspersky has a good reputation for its protection capabilities and performs well in traditional third-party tests. The Kaspersky Anti Targeted Attack (KATA) Platform solution adds more comprehensive detection and response capabilities, including at the network and gateway level.

Recent investment has included a new cloud (SaaS) management console for enterprise customers, and significant improvements in detection of fileless malware and attribution of advanced persistent threats.

Kaspersky has global coverage, but it has a significant presence in Latin America (LATAM), and Middle Eastern and African regions, and it suits Types A, Type B and Type C organizations.

Strengths

- Kaspersky has a broad range of endpoint protection capabilities including device control, firewall management and URL filtering. It also covers a wide variety of platforms, including integration with cloud workloads.
- Kaspersky's reputation for protection is very high, and the vendor has consistently led in third-party detection tests for many years.
- Compared to other vendors that use signatures, as well as more advanced techniques, Kaspersky has less impact on the operating system.

- Kaspersky now offers a range of managed services directly to customers as well as providing the tools for partners to provide those services.

Cautions

- The EDR emphasis is very much on protection and automated response; as a result, Kaspersky doesn't provide response capabilities that are as extensive as other vendors in this research. For example, it does not offer prebuilt playbooks (other than automatic remediation) or the ability to create response playbooks.
- Kaspersky Anti Targeted Attack, a separate product, is required to carry out more extensive threat hunting actions involving analysis of network activity.
- Despite a wide range of products covering cloud workloads, email and operational technology (OT), there is more limited correlation of information between these solutions and XDR capabilities than is provided by the leading vendor solutions in this research.
- Kaspersky products were involuntarily not represented in the last MITRE ATT&CK evaluations (Enterprise 2020 and ICS 2020 evaluations). During the finalization stage of the Enterprise 2020 evaluation, Kaspersky says MITRE notified it that its participation had been discontinued. MITRE has not publicly explained why.

McAfee

McAfee is a Leader in this Magic Quadrant.

McAfee has developed its new MVISION strategy to tie the McAfee portfolio into an XDR solution. McAfee's standard endpoint offering combines advanced protection capabilities like ransomware rollback, with native OS capabilities. McAfee's premium MVISION EDR package now includes MVISION Insights, which prioritizes threats and countermeasures, and directs responders accordingly.

Mainly present in North America and EMEA, products suit Type A and Type B organizations, with options for Type C organizations without security staff.

Strengths

- McAfee MVISION Insights is a welcome addition to its core platform offering, and allows users to manage their attack surface and preempt attacks before they occur. This provides a differentiated feature set not seen in other solutions.
- MVISION EDR now maps threats against the MITRE ATT&CK Framework and this helped McAfee to identify techniques consistently in MITRE evaluations; additionally, the automated AI-guided investigation capabilities use the MITRE ATT&CK Framework to drive faster, easier alert triage.
- MVISION EDR includes an extensive remediation capability plus an advanced SOC workflow feature. The user interface is easy to use and EDR features now match those of market-leading counterparts.

- McAfee continues to provide broad OS support, especially for those customers that still need agents for older and legacy OSs and/or still require an on-premises solution or add-ons like application control. A good score for operations in 2021 is awarded for the wide range of customer support and training facilities in all regions.

Cautions

- McAfee has been slow to convert its legacy installed base to MVISION. Many of its clients are still using the on-premises version of McAfee ePolicy Orchestrator (ePO) and McAfee Endpoint Security (ENS).
- The upgrade from older versions of McAfee ePO and McAfee VirusScan Enterprise to McAfee ENS is still ongoing for some McAfee customers. R&D effort and sales focus are on cloud solutions, and on-premises customers should upgrade ASAP.
- McAfee has announced general availability of its XDR solution. However, the products contributing to the XDR don't yet include network traffic analysis, a cloud access security broker (CASB) or user and entity behavior analytics (UEBA).
- The Managed Detection and Response solution was launched last year and hasn't seen much adoption from customers yet.

Microsoft

Microsoft is a Leader in this Magic Quadrant.

Microsoft Defender for Endpoint (MDE) provides an integrated and comprehensive set of EPP, EDR and threat hunting capabilities from a single cloud-hosted console and data lake. The native protection and prevention provided by Defender Antivirus in Windows OS is widely used and popular with customers, and is also leveraged by other vendors in this Magic Quadrant.

Microsoft invested in its OS coverage in 2020, introducing significant new macOS and Linux protection capabilities as well as developing threat and vulnerability management and attack surface reduction enhancements. Microsoft also added coverage for Android and iOS devices.

Microsoft appeals to all organization types on a global footing, especially large enterprises.

Strengths

- Microsoft continues to score highly for market understanding and innovation this year. Both Defender for Endpoint and the protection engines built into Windows 10 have evolved exponentially throughout the year, along with the addition of new capabilities in each release of Windows to create a holistic set of security layers.
- macOS and Linux operating systems also now have endpoint protection and threat and vulnerability management options fully integrated into the same management and reporting console.

- All Defender products share a common cloud-hosted console, underlying data lake and API, allowing for unified threat hunting, excellent automation and creating a true XDR platform.

- Microsoft has unified the Defender 365 console with coordinated prevention, automatic remediation and threat hunting across all Defender products. Other new additions include threat intelligence reports and a learning hub that makes finding product training much simpler.

Cautions

- Microsoft does not provide support for Windows legacy systems that have reached the end of their support life cycle, despite many organizations still owning significant numbers of these. The lack of legacy support means scoring for market responsiveness is lower for Microsoft.

- For organizations that maintain air-gapped networks and/or do not directly connect (e.g., server or workstation) workloads to the internet, a cloud-hosted solution is impractical since there is no option to host the console on-premises.

- There is a large gulf in capability and cost between SKUs providing MDE and those that do not, and some organizations are consequently unable to justify the cost premium of Microsoft Defender for Endpoint. Licensing Microsoft Defender individually outside of security bundles is also not cost-effective for these customers. This led to a lower score than the leading vendors in this Magic Quadrant for Sales Execution/Pricing for 2021.

- The (E5) central Threat Experts facility is not the equivalent of the more tailored and customized MDR services of competing vendors, and the Kusto query language, developed to ease the complexity of threat hunting, does not live up to this promise as it is complex to learn and use.

Panda Security

Wholly owned by WatchGuard, Panda Security is a Niche Player in this Magic Quadrant.

Panda's rebranded Cytomic Covalent is a full EDR solution including modules for encryption and patching, and Cytomic Insights for enhanced monitoring and reporting. Other functionalities included are device control, web access control, data loss prevention (DLP) and system management.

Panda has invested in richer EDR capabilities across its Cytomic EDR and Orion products as well as important SIEM integration and other API connectivity with third-party security tools. Integration of Panda's endpoint solutions into a WatchGuard unified cloud platform is expected in summer 2021.

Best for Type B and Type C organizations in EMEA, Panda plans expansion into North America for 2021.

Strengths

- Panda has an EDR and MDR service combination with additional tools for a variety of security needs beyond endpoint protection, such as encryption, vulnerability and patch management, and device control. These are better integrated in the rebranded Cytomic and Orion packages than the earlier

Adaptive Defense 360 they replace, giving Panda a higher score for its products than in the previous Magic Quadrant.

- Panda supports a comprehensive range of OSs, and includes coverage for virtualized systems and virtual desktop infrastructure (VDI) desktops, with the addition of Android mobile device security.
- Panda provides 100% attestation of the small percentage of unidentified or unknown items via a specialist team, reducing the likelihood of false positives and missed detections.
- Parent security company WatchGuard has a ready-to-go reseller channel in the U.S. and elsewhere, greatly expanding the reach of Panda's products but also providing an interesting opportunity to combine endpoint and network security telemetry for analytics and hunting.

Cautions

- Panda has yet to develop cloud workload protection, and container and serverless security solutions, so it appeals primarily to customers with traditional server hosting.
- Integration of MITRE ATT&CK classifications into alerting and threat visualization is not as comprehensive as those of leading vendors in this research, who have already added these enhancements.
- Though its own sensors and telemetry are more integrated and threat hunting is available, the current platform does not feature the automation, analytics and extensibility of leading XDR systems. However, integration of more telemetry sources from the company's wider portfolio is expected in 2H21.
- Panda has limited appeal for Type A enterprise customers. Consequently, this year's overall viability score is lower; however, the vendor claims that this will improve as a result of its new ownership and associated opportunities.

SentinelOne

SentinelOne is a Leader in this Magic Quadrant.

SentinelOne's Singularity platform, its XDR solution, launched in 1H20. It adds third-party integrations to existing EDR and threat hunting hosted on a new cloud platform and data lake. Further enhancement of the XDR solution has been made via the recent acquisition of Scalyr.

Investment in 2020 included more automated mitigation options via the Storyline Active Response capability, as well as new IoT discovery and protection capabilities in its Ranger product.

North America and EMEA markets are a mainstay for SentinelOne, and expansion into India and the Middle East is targeted. It has options to suit all organization types in each of these regions.

Strengths

- SentinelOne customers cite ease of deployment, excellent timeliness and quality of customer support, and effective protection, all of which score highly in this analysis and are reflected in the rating for its products and service in this year's Magic Quadrant.
- As the solution has been reengineered to leverage a microservices architecture, this provides flexible hosting options to suit all customers and rapid/frequent functionality updates.
- SentinelOne added support for containers and serverless workloads, especially Kubernetes dynamic workloads, with additional runtime protection and simplified deployment for these.
- SentinelOne achieved a strong showing in the MITRE Phase 2 evaluations, with consistent identification of tactics and techniques as well as high detection rates with few misses.

Cautions

- While SentinelOne has focused on third-party integrations into the Singularity console, its own range of sensors is not as comprehensive as other XDR platforms, and SentinelOne does not have its own network security sources to add, though it has device discovery via Ranger.
- Though SentinelOne has its own Vigilance MDR solution, third-party managed service providers (MSPs) and an expanded network of resellers, SentinelOne does not yet score as highly as some of the Magic Quadrant Leaders in range and reach of its managed services.
- New SentinelOne customers migrating from other enterprise solutions will miss add-ons like fully featured DLP and other extras that are not offered.
- SentinelOne provides a hybrid mode for customers with air-gapped and on-premises management requirements; but unless the endpoint agents can forward telemetry to the cloud, the solution will lack advanced analytics and threat hunting.

Sophos

Sophos is a Leader in this Magic Quadrant.

In March 2020, Thoma Bravo, a private equity firm, completed the acquisition of Sophos.

Sophos Central is a single console for EPP, EDR and MTD, offering better visibility, easier management and increased threat detection across all endpoint types. It also manages disk encryption, server protection, firewall and email gateways.

Investment has primarily focused on the Sophos Central cloud-hosted solution and includes enhancements to Live Response, forensic and device discovery data.

Sophos is best suited to Type A and Type B organizations, with options for Type C organizations without security staff. Customers are mainly in North America and EMEA.

Strengths

- Sophos was one of the first vendors to offer XDR-style integration between security tools.
- Sophos' Managed Threat Response offers expanded capabilities to its MDR as a result of its acquisition of Rook Security in June 2019.
- Sophos added better threat hunting capabilities specifically focused for large enterprise clients.
- Intercept X clients continue to report strong confidence that the product protects against most ransomware, and in its ability to roll back the changes made by a ransomware process that escapes protection.

Cautions

- The on-premises capability lacks feature parity with the SaaS version, resulting in clients not getting the latest features unless they migrate to the cloud offering.
- The Intercept X agent has a large footprint, which is especially problematic under the new work-from-home reality resulting from the pandemic. Clients report users with low bandwidth struggle to install software updates.
- Live Discover uses a very detailed SQL-level-style interface that is too technical for some admins, but prebuilt queries are available in the interface and via a community forum. Some clients report problems with offline devices and the associated lag in data sync to the cloud.
- Sophos has not participated in the first and second series of MITRE ATT&CK evaluations.

Trend Micro

Trend Micro is a Leader in this Magic Quadrant.

Trend Micro has a broad range of capabilities delivered through the Apex One platform, and more advanced EDR capabilities can be added with an XDR add-on to integrate with other security tools in its portfolio. The vendor provides support for all current and many legacy operating systems, as well as providing on-premises, cloud and hybrid management options.

Recent investment has included the XDR platform used for detection and response and establishment of a comprehensive set of cloud workload and container security tools, unified and rebranded as Cloud One.

Trend Micro is most suited to Type B and Type C organizations. It has a global presence, but is most popular in Asia/Pacific, in particular Japan.

Strengths

- Broad platform coverage, including cloud workloads and containers, and integration through Apex One XDR into other security tools, such as email and network traffic analysis (NTA), provide increased visibility and response capabilities.

- Vulnerability management includes prioritized guidance and virtual patching, which can mitigate vulnerabilities before patching, combined with support for a broad range of older platforms means it is a good choice for organizations that need to support legacy systems.

- Trend Micro has shown a strong commitment to its cloud offerings and has made good progress to move its existing clients to the cloud solution to get the benefits associated with the new platform.

- Trend Micro has a comprehensive set of application control capabilities that goes beyond simple block listing and allows administrators to define their own controlled applications.

Cautions

- The endpoint agent has one of the larger footprints and unlike other vendors requires regular updates to detection data and rules to maintain protection.

- Apex One has only limited response capabilities at present, and more advanced threat hunting tools require the EDR add-on. Integration into cloud workload protection and network traffic analysis tools in XDR have only recently been added. The automation and workflow functionality is not as strong as the other leading solutions in this Magic Quadrant and relies on integration to SOAR tools through its APIs.

- The XDR platform has a different workflow and user interface from the main EPP management console and, unlike some other XDR solutions, storage of data from other products has different retention periods.

- Despite a long history in the market and global coverage, Trend Micro is still seen as a legacy vendor by some Gartner clients despite being one of the earliest vendors to combine detection and response capabilities, leading to slow adoption of the latest solutions and less growth in seat numbers than other Leaders in this research.

VMware Carbon Black

VMware Carbon Black is a Visionary in this Magic Quadrant.

VMware finalized its acquisition of Carbon Black in 2019. With this addition it has security coverage across endpoints, network and cloud workloads. VMware also made significant progress on its partner ecosystem, including its advanced Next-Gen SOC Alliance with SIEM and SOAR vendors.

Investment has focused on incorporating Carbon Black into existing VMware virtualization solutions, as well as integrating Carbon Black with VMware's expanding portfolio of security tools based around a single cloud-hosted console and data lake.

Mainly in North America, products suit Type A and Type B organizations and are gaining a strong foothold in the managed security service provider (MSSP) and incident response (IR) markets. VMware

Carbon Black also appeals to vSphere, NSX and Workspace ONE customers with cloud workloads and managed endpoints.

Strengths

- VMware Carbon Black Cloud provides all four core EPP capabilities in a single agent, with customers appreciating the easy-to-use management console and simplified deployment experience.
- VMware Carbon Black provides a cloud-native console and single-agent approach that meet multiple use cases to include EPP, EDR, endpoint query and remediation. It is used for advanced EDR in incident response. Carbon Black is rated high for viability and operations under the new ownership of parent VMware
- The acquisitions of Lastline (sandboxing and intrusion detection system [IDS]) and Octarine (cloud workload protection platform [CWPP]) help build out its cloud workload protection capability.
- VMware Carbon Black achieved positive results in the MITRE Phase 2 evaluations with good telemetry and consistent identification of techniques.

Cautions

- VMware's range of products, especially with the latest acquisitions, are not as long-established as the equivalent platforms of the leading solutions in this research.
- VMware has recently added coverage for virtualized workloads and also added container support. Plans to cover serverless workloads are not yet announced.
- On-premises versions of the Carbon Black products are less advanced than the latest cloud-hosted solutions, and VMware is still in the process of migrating the few remaining customers from these.
- Customers looking to use VMware Carbon Black Cloud without Workspace ONE, will experience missing management and protection capabilities, such as discovering unprotected devices, managing host firewall settings/internet URL filtering and automated playbooks.

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

Cybereason is a new entrant for the 2020 Magic Quadrant and has placed in the Niche Players section based on its 2021 scoring, survey and demos.

Dropped

Malwarebytes and Palo Alto Networks were both unable to meet the inclusion and exclusion criteria stipulated by Gartner for this year's research.

Inclusion and Exclusion Criteria

For Gartner clients Magic Quadrant and Critical Capabilities research identifies and then analyzes the most relevant providers and their products in a market. Gartner uses, by default, an upper limit of 20 vendors to support the identification of the most relevant providers in a market. The inclusion criteria represent the specific attributes that Gartner analysts believe are necessary for inclusion in this research.

Magic Quadrant Inclusion Criteria

To qualify for inclusion, vendors needed to meet the following criteria at the commencement of initial research and survey process (as of 1 April 2020):

Core Criteria

All vendors must provide *at least 12* of the following:

1. The solution must protect against known and unknown malware without relying on daily agent/definition updates.

2. There must be a facility to detect malicious activity based on the behavior of a process.

3. The solution must store indicator of compromise (IOC)/indicator of attack (IOA) data in a central location for retrospective analysis.

4. The capability must be provided to detect and block fileless malware attacks.

5. The solution must be able to remove malware automatically when detected, i.e., delete/quarantine files/kill processes.

6. The solution must allow for false positives to be suppressed/ignored from the management console without excluding all protection techniques, e.g., suppress file detection, but still monitor behavior.

7. The primary EPP console must use a cloud-based, SaaS-style, multitenant infrastructure that is operated, managed and maintained by the vendor.

8. Reporting and management console views must display a full process tree to identify how processes were spawned and for an actionable root cause analysis.

9. Threat hunting must be provided including the facility to search for an IOC/IOA (e.g., file hash, source/destination IP, registry key) across multiple endpoints from the management console even if

machines are not connected.

10. The solution must identify changes made by malware and provide the recommended remediation steps or a rollback capability.

11. The option must be provided to integrate threat intelligence/reputation services into the management console.

12. The solution must implement protection against common application vulnerabilities and memory exploit techniques.

13. The solution must continue to collect suspicious event data when the managed endpoint device is outside of the corporate network.

14. The facility must be present to perform static, on-demand malware detection scans of folders, drives or devices, such as USB drives.

15. All capabilities must be delivered in a single agent/sensor or be directly integrated in the operating system.

Optional

All vendors must provide *at least four* of the following capabilities:

1. The solution should implement named vulnerability shielding (virtual patching) for known vulnerabilities in the OS and for non-OS applications (examples required).

2. Provision should be made for risk-based vulnerability reporting and prioritization.

3. The solution should implement configurable default deny approved listing (with trusted sources of change).

4. Provision of application isolation to separate untrusted applications from the rest of the system (container/sandbox or hardware-based hypervisor) should be included.

5. The capability should include access to a cloud or network-based sandbox for detonation that is virtual machine (VM)-evasion-aware.

6. The endpoint agent should include endpoint-based deception (lures) capabilities designed to expose an attacker.

7. The vendor itself should offer managed alerting and monitoring services, alerting customers to suspicious activity (with telephonic incident response advice).

8. The vendor itself should offer managed threat hunting, or managed IOC/IOA searching, for detection of threats (not via third party or channel) and provide direct incident response remotely.

9. The solution should support advanced queries against the database with operators and thresholds (i.e., “show all machines with new portable executable [PE] files less than one-week old and on less than 2% of machines or unknown”).

10. Reporting should include guided analysis and remediation based on intelligence gathered by the vendor, e.g., “the next steps needed to contain this threat are xyz.”

11. The capability should be provided to report attribution information and potential motivations behind attacks.

12. The vendor should provide a solution with the same capabilities as cloud managed for air-gapped or non-internet-facing systems.

13. The ability to automatically consolidate multiple alerts from multiple sources into a single incident should be provided.

14. The ability to correlate and enrich multiple weak events/alerts from multiple sources/sensors into strong detection should be present.

15. The solution should allow coordination of response across multiple security products, e.g., initiates a change.

Magic Quadrant Exclusion Criteria

- Vendors may be excluded if the majority of detection events are not from the vendor’s own detection agent and techniques are not designed, owned, and maintained by the vendor itself. Augmenting a solution with an OEM engine *is* acceptable provided the additional agent/sensor is not the *primary* method of detection.

- If a vendor has not participated in independent, well-known, public tests (e.g., Virus Bulletin, AV-TEST, AV-Comparatives, NSS Labs, SE Labs, MRG Effitas, MITRE, etc.) for accuracy and effectiveness within the 12 months prior to 30 June 2019 it will be excluded. A vendor will only be considered if it is a current participant in the VirusTotal public interface (other public test participation may be considered if it is the equivalent of those listed).

- The vendor must have more than 7 million enterprise active seats overall that use the vendor’s EPP as their sole EPP. Of these, more than 250,000 must be active installations with accounts larger than 500 seats. These account names can be kept confidential with Gartner and are not required to participate in the reference survey. Vendors with less than the requisite numbers of seats (as indicated previously) may not qualify for inclusion in the main analysis of the Magic Quadrant and Critical Capabilities.

- Candidate vendors can include *only* those solutions and services that have the combination of SMB and midsize solutions and services, coupled with enterprise-grade, highly scalable and extensible services that these customers demand. It is therefore a requirement that vendors included in the research are limited to those that can adequately service all target organization types at all scales (see the Use Case Definitions section).
- The definitions in the Critical Capabilities companion research also stipulate the availability of managed services, globally available localization and support/professional services facilities, and an array of resellers and comprehensive support for the list of operating systems and device types in use by Gartner clients. Failure to offer any one of these key capabilities would be a barrier to inclusion in this research.

Honorable Mentions

Malwarebytes

Malwarebytes, already well established in cyber protection, is a growing presence in the endpoint protection segment and is best-known for its malware removal capabilities It has recently expanded its protection portfolio to include EPP solutions scaled for SMBs through enterprise. Malwarebytes' core detection engines include machine learning, behavioral, and heuristic technologies, and an anti-exploit layer. Both EPP and EDR modules are delivered via a single agent and are managed through a cloud-based platform. Malwarebytes did not meet the following criterion in 2020/21 and thus does not feature in the main analysis in this research:

The vendor must have more than 7million enterprise active seats overall that use the vendor's EPP as their sole EPP, of these, more than 250,000 must be active installations with accounts larger than 500 seats.

Palo Alto Networks

Palo Alto has both EPP and EDR capabilities with its Cortex XDR product. Cortex XDR provides cloud-hosted EDR, NTA and UEBA capabilities that are integrated with Palo Alto's firewalls and cloud offerings for endpoint attack prevention, alert triage, incident response, and threat hunting. Cortex XDR uses its integrated endpoint agent, next-generation firewall, and additional third-party sensors, including network and identity sources, to collect and analyze logs and telemetry data in the same console.

In April 2020, Palo Alto Networks notified Gartner that, due to its ongoing consolidation of its endpoint platform, it was unable to meet the inclusion criteria and was thus excluded from the main scoring and analysis in this research. Subsequent guidance from the vendor would suggest that market traction has advanced significantly since the original inclusion criteria were assessed.

Tanium

Tanium offers endpoint security and rapid response, vulnerability and patch management, plus system management tools. These tools can be either an on-premises deployment or leveraged directly from the cloud-hosted “Tanium as a Service.”

Tanium’s strength is incident response and has major customers in North America and Europe. Enterprises with resources and skills to use the complex capabilities of Tanium, are most suited to it. As are those that need unified endpoint management or unified endpoint security tools.

Customers usually deploy Tanium with Windows Defender or another antivirus/anti-malware solution. Deployed this way, Tanium will likely provide a full set of prevention, detection and response capabilities. Although invited to participate in this research, Tanium notified Gartner that it was unable to fully meet the inclusion criteria and was thus omitted from the main scoring and analysis in this year’s research.

Evaluation Criteria

The following tables show how all criteria are evaluated. This includes specific characteristics and their relative importance that support the Gartner view of the market and that are used to comparatively evaluate providers in this research. The two sections represent the X and Y axes of the Magic Quadrant graphic.

Ability to Execute

Gartner analysts evaluate vendors on the quality and efficacy of the processes, systems, methods or procedures that enable IT provider performance to be competitive, efficient and effective, and to positively impact revenue, retention and reputation within Gartner’s view of the market.

Product/Service: This criterion refers to core goods and services that compete in and or serve the defined market. This includes current product and service capabilities, quality, feature sets, skills, etc. This can be offered natively or through OEM agreements/partnerships.

Overall Viability (Business Unit, Financial, Strategy, Organization): Viability includes an assessment of the organization’s overall financial health, as well as the financial and practical success of the business unit. Views the likelihood of the organization to continue to offer and invest in the product, as well as the product position in the current portfolio.

Sales Execution/Pricing: This refers to the organization’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 and Track Record: This criterion evaluates the organization’s 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 to changing market demands.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message in order to influence the market, promote the brand, increase awareness of products and establish a positive identification in the minds of customers are evaluated. This "mind share" can be driven by a combination of publicity, promotional activity, thought leadership, social media, referrals and sales activities.

Customer Experience: This criterion evaluates products and services and/or programs that enable customers to achieve anticipated results with the products evaluated. Specifically, this includes quality supplier/buyer interactions, technical support or account support. This may also include ancillary tools, customer support programs, availability of user groups, service-level agreements, etc.

Operations: The ability of the organization to meet goals and commitments is evaluated. Factors include quality of the organizational structure, skills, experiences, programs, systems and other vehicles that enable

the organization to operate effectively and efficiently.

Ability to Execute

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	Low
Customer Experience	High
Operations	Medium

Source: Gartner (May 2021)

Completeness of Vision

Gartner analysts evaluate vendors on their ability to convincingly articulate logical statements. This includes current and future market direction, innovation, customer needs, and competitive forces and how well they map to Gartner's view of the market.

Market Understanding: This addresses a vendor's ability to understand customer needs and translate them into products and services. Scoring of this section focuses on three areas:

1. Matching of products to emerging threats and providing services to meet demand

2. Early moves to cloud hosting in response to industry and technology advances/changes

3. Response to market shifts and historic adjustment of roadmap to include EDR capabilities, combine agents into one.

Marketing Strategy: This refers to a vendor's history of and consistently clear, differentiated messaging communicated internally and externalized through social media, advertising, customer programs and positioning statements. This is scored using a combination of survey responses and external publicly accessible sources.

Offering (Product) Strategy: This criterion describes an approach to product development and delivery that emphasizes market differentiation, functionality, methodology, and features as they map to current and future requirements.

We look for vendors that provide educated guidance for customers to investigate incidents, to remediate malware infections and to 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 automation are given extra credit here. 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.

Innovation: The vendor's direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or preemptive purposes are evaluated.

We look at the vendor's current roadmap and historic performance/leadership in:

1. Delivering alternative approaches and new technologies

2. Additional protection and capabilities, and for contributing positively to the infosec community

3. Following others' lead (delivering catch-up or tick-box features can expect a neutral or low rating)

Geographic Strategy: This criterion addresses 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. This includes each of:

1. In-country/regional R&D and professional services facilities and resources
2. Local and regional training and managed services and whether these are provided by the vendors or partners
3. Full localization of the customer products including coverage of right-to-left alphabets and double-byte character sets

Table 2: Completeness of Vision Evaluation Criteria

Evaluation Criteria ↓	*Weighting* ↓
Market Understanding	High
Marketing Strategy	High
Sales Strategy	NotRated
Offering (Product) Strategy	High
Business Model	NotRated
Vertical/Industry Strategy	NotRated
Innovation	Medium
Geographic Strategy	Medium

Source: Gartner (May 2021)

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. Increasingly, leaders provide holistic XDR platforms that allow customers to consolidate their other tools and adopt a single-vendor solution. 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 not a match for best-of-breed solutions and aren't pursuing clients' individual and particular needs. Leaders may be less able to quickly 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 that will be significant in the next generation of products, and will give buyers early access to improved security and management. These features include automation, advanced analytics, cloud workload and container protection, customizable managed services, automated detection or protection capabilities, and real-time incident response workflows. Visionaries can affect the course of technological developments in the market, but may not yet demonstrate consistent execution and may yet lack 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 a 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

Endpoint protection is a commonly deployed layer of malware prevention and is considered basic security hygiene for all organizations. Despite the advent of sophisticated, stealthy attacks, a well-configured and maintained EPP product can still significantly lower the risk of malware and targeted attacks. However, all industry sectors and scales of organization must reexamine their endpoint protection approach and invest in additional capabilities and layers of protection for the endpoint to address more advanced attack techniques that can evade EPP detection.

Endpoint detection and response is now a mainstream part of any endpoint security strategy and, as such, received increased emphasis in this analysis. Roughly 30% of endpoints are now protected by EPP and EDR. Increasingly, EDR deployment is no longer limited to organizations with mature security operations. EDR adoption is driven primarily by protection against advanced threats, but also the added appeal of automation, orchestration and managed EDR features. EDR innovation, such as behavior-based detection and basic threat hunting, is increasingly included in endpoint protection platforms. This convergence also came from the EDR side of the market, where EDR vendors added protection capabilities to their core detection and response functions.

EDR solutions provide capabilities to detect and investigate security events, contain the attack and produce guidance for remediation. EDR solutions must identify and analyze activity and device configuration. Visibility and reporting of user and device activity are combined with direct intervention when abnormal activity is detected. Automated response and rollback of threats are highly desirable EDR features. Integration and automation with other tools such as ticketing and system management are key.

In this year's analysis, we also evaluated the extended detection and response capability of vendors. XDR is a new approach that delivers a single solution combining threat detection and incident response tools, unifying multiple security products into a security operations system. For example, XDR offerings can combine firewalls, sandboxes, secure web and email gateways, and identity tools in a common incident response capability. XDR solutions allow pragmatic security organizations to gain more operational efficiency without complex manual integration in a SIEM or SOAR tool (see Innovation Insight for Extended Detection and Response).

Cloud delivery is becoming mainstream. Roughly 65% of the enterprise EPP market is currently using a cloud-delivered solution; however, approximately 95% of new licenses are cloud-delivered. Services such as full and light incident response support are also receiving more attention from buyers.

Use-Case Definitions

Type A

Type A organizations, also referred to as “lean forward” organizations, adopt new technologies very early in the adoption cycle.

Type A organizations represent the smallest group of organizations. They have the budgeting and staffing resources to configure and implement new technologies and solutions rapidly within their environments. These organizations tend to focus on best-of-breed solutions that address their business, technology and security needs and that have the capacity to integrate, develop or build custom-made components as required. They see the use of technology as a competitive differentiator. Their tolerance for risk is high and their approach to technology change is to run projects in parallel, having multiple teams working on technology and business changes simultaneously. For EPP, these organizations focus on best-of-breed prevention, detection and response, and rarely require managed security service (MSS)/MDR capabilities.

Type B

Type B organizations aim to stay relatively current on technology without getting too far ahead or behind their competition.

Type B organizations represent the largest group of organizations. They typically experience budgeting and staffing resource constraints and, as a result, focus on overall value by weighing the risks of the early use of new technology against the benefits. Their focus is on technology deployments that improve their organization’s productivity, product quality, customer service and security. Type B organizations typically wait for a technology to become mainstream before considering implementation. They tend to be moderate in their approach, frequently using benchmarks within their industry to justify their investments in technology. Type B organizations balance innovation with reasonable caution when selecting new solutions. For EPP, these organizations focus on a blended approach between prevention, detection and response capabilities that can be complemented with managed services where needed.

Type C

Type C organizations typically view technology as an expense or operational necessity and use it as a means to reduce costs.

Type C organizations represent the second-largest group. These organizations experience severe budgeting and staffing resource constraints and, as a result, prefer simply to deploy and use integrated solutions with managed service add-ons that can best complement their minimal staff. These organizations wait for technologies to become stable and for costs to acquire and operate to reach the lowest quartile before committing to purchase. For EPP, these organizations focus on prevention, rather than on integrated detection and response capabilities and solutions that offer a complement of managed services.

Market Overview

- Ransomware is currently the biggest risk for all organizations. Recent changes in ransomware include the expansion of affiliate programs, data theft and doxing threats, and the expansion of human-operated ransomware; all of which elevate the business impact of ransomware infections. Some EPP solutions are offering cyber insurance policies for ransomware to demonstrate confidence in ransomware defense.

- Remote work has significantly accelerated the adoption of cloud-managed offerings, which now represent 60% of the installed base and 95% of all new deployments. Hybrid deployment offerings are desirable for buyers that cannot commit to 100% cloud deployments. However, buyers should look for indicators that solutions are truly designed for cloud delivery and not simply management servers shifted to the cloud.

- Fileless attacks are now a common component of all malware types, making the behavioral protection of EDR tools a critical capability. Advanced adversaries targeting the organization can evade any protection solutions, making detection and hunting critical to fast incident response. EDR should now be a mandatory key capability; however, EDR capabilities are deployed to only 40% of endpoints.

- The biggest barrier to adoption of EDR tools remains the skills required to operate them and the increased total costs, particularly as later adopters deploy EDR. On average, EDR capabilities will add an extra 37% to initial costs, and adoption of EDR must be accompanied by investment in training to be effective.

- To alleviate the skills gap, MDR services that provide monitoring and alert triage are becoming much more popular. MDR services are increasingly being offered by the solution providers themselves rather than through partners.

- The recent SolarWinds supply chain attacks illustrated both the value of EDR and the drawbacks. We have little evidence that EDR solutions detected the breach in real time. However, EDR solutions were very useful postevent to detect compromise and to block newly discovered malicious behavior. However, EDR data storage periods should anticipate attack techniques that stretch the attack timeline to several weeks.

- SolarWinds attacks also illustrated the need for better integration of telemetry data from identity and email at a minimum and the need for effective tamper protection to ensure agents are not disabled.

- Extended detection and response capabilities are emerging as the newest key capability for EPP solutions. XDR provides a threat detection and incident response tool that unifies multiple security products into a common incident response and hunting toolset.

- All organizations need better-prioritized hardening guidance. EPP solutions are increasingly offering vulnerability analysis, with some more advanced solutions also including endpoint configuration guidance.

- EPP solutions may also add mobile threat defense and integration with unified endpoint management to reduce the overall administration burden and allow further consolidation of security operations and

IT operations tools.

Acronym Key and Glossary Terms

AI	Artificial intelligence (especially when used to identify and alert on unknown threats)
EDR	Endpoint detection and response (for postinfection stages of an attack or exploit)
EPP	Endpoint protection platform (provides prevention of malware and exploits)
MDR	Managed detection and response (a managed service for EDR tools)
ML	Machine learning (e.g., where agents use mathematical determination of threats)
MSSP	Managed security service provider
SIEM	Security information and event management (gathers and analyzes device logs)
SOAR	Security orchestration, analytics and reporting (joins solutions with workflow)
SOC	Security operations center (or also the team that works in it)
XDR	Extended detection and response (a unified system combining telemetry sources and integrating multiple tools into a single console usually with automation and AI-powered analytics for faster and more accurate detection and response)

Evidence

The Magic Quadrant team relied on data from the following sources:

- Gartner analysts responded to more than 5,300 client inquiries since January 2019.
- Data from more than 5,000 Peer Insights reviews on gartner.com.
- Data from a 630-question survey and 30-minute demonstrations provided by each vendor conducted in 2Q20 and 1Q21

Note 1. Kaspersky

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.

Kaspersky launched its Global Transparency Initiative (GTI) and established data centers in Switzerland to relocate customer data processing functions as well as launching transparency centers in Switzerland and Spain to allow external review of its internal processes and source code of its products. The company has undergone a SOC 2 Type 1 audit by a Big 4 firm and obtained ISO/IEC 27001:2013 certification, and increased bug bounty awards up to $100,000 for security researchers.

Kaspersky is continuing to migrate North America and Europe customers and plans to open additional transparency centers in Kuala Lumpur, Malaysia, and São Paulo, Brazil. Gartner clients who work directly with U.S. federal agencies should consider this information in their vendor selection and continue to monitor this situation for updates.

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.

Recommended by the Authors

Hype Cycle for Security Operations, 2020

Hype Cycle for Endpoint Security, 2020

Market Guide for Endpoint Detection and Response Solutions

Top Security and Risk Management Trends 2021

Innovation Insight for Extended Detection and Response

Defend Against and Respond to Ransomware Attacks

Market Guide for Security Threat Intelligence Products and Services

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	Low
Customer Experience	High
Operations	Medium

Source: Gartner (May 2021)

Table 2: Completeness of Vision Evaluation Criteria

Evaluation Criteria ↓	*Weighting* ↓
Market Understanding	High
Marketing Strategy	High
Sales Strategy	NotRated
Offering (Product) Strategy	High
Business Model	NotRated
Vertical/Industry Strategy	NotRated
Innovation	Medium
Geographic Strategy	Medium

Source: Gartner (May 2021)