Magic Quadrant for Endpoint Protection Platforms

Published 31 December 2022 - ID G00752236 - 55 min read

By Peter Firstbrook, Chris Silva

All vendors in this report have effective solutions for combating malicious attacks. Now that endpoint detection and response (EDR) is integrated into EPPs and evolving into extended detection and response (XDR), the main consideration for most buyers should be integration with security operations.

Strategic Planning Assumptions

By the end of 2025, 80% of Type C organizations will acquire endpoint detection and response (EDR) as a managed detection and response (MDR) service.

By the end of 2025, more than 50% of Type B organizations will consolidate EDR into a preferred vendor portfolio of security investments for more efficient security operations.

By the end of 2026, 80% of Type A organizations will be consuming EDR as part of a multitool extended detection and response (XDR) architecture.

Market Definition/Description

Note: Due to a pause in coverage of all Russian vendors by Gartner, there may be vendors that met the inclusion criteria described but were not evaluated. These vendors are not included in this research.

Endpoint protection platforms (EPPs) provide the facility to deploy agents or sensors to secure managed endpoints, including desktop PCs, laptop PCs, servers and mobile devices.

EPPs are designed to prevent a range of known and unknown malicious attacks. In addition, they provide the ability to investigate and remediate any incidents that evade protection controls.

The core capabilities of an EPP are:

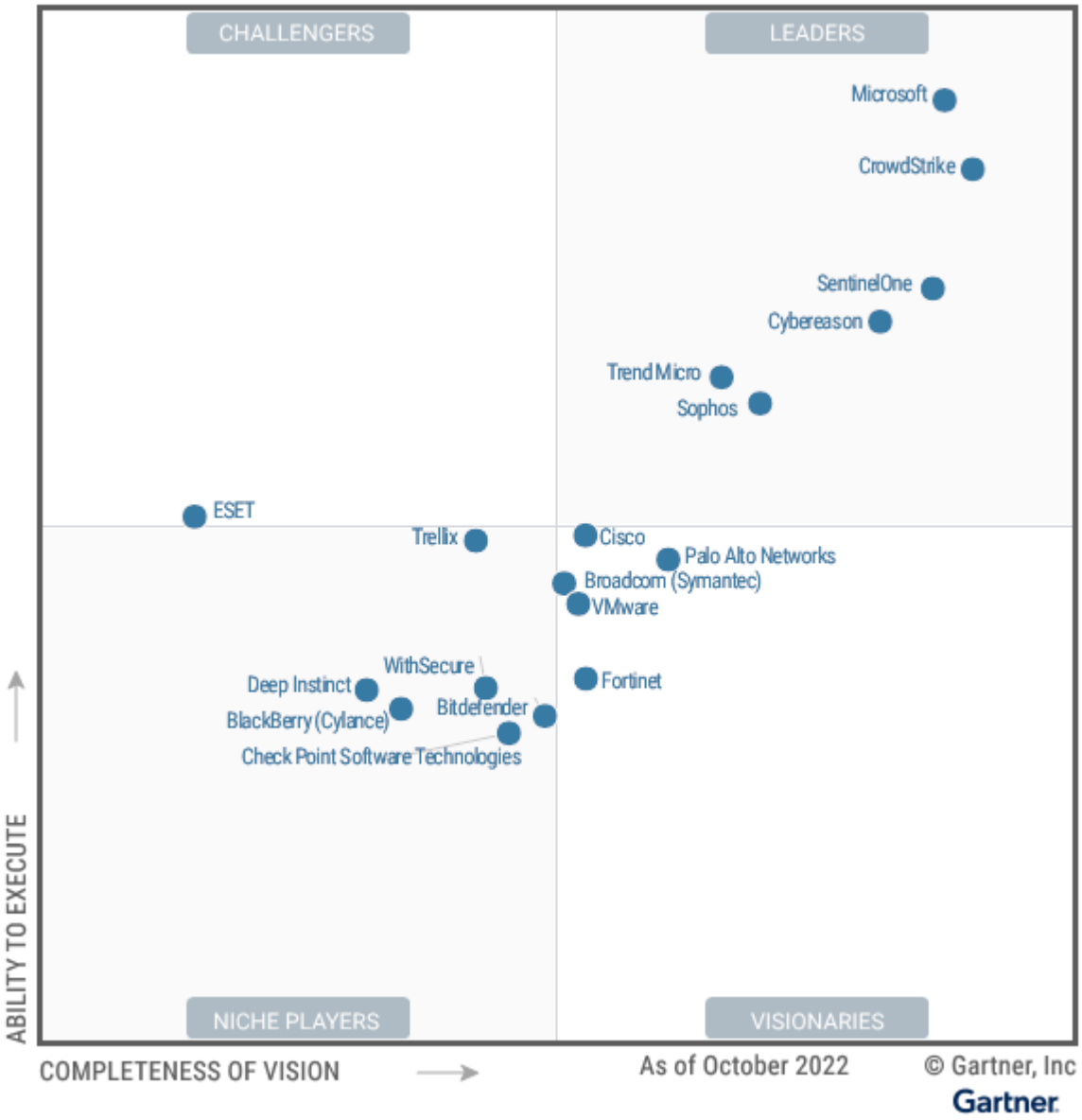
- Prevention of, and protection against, security threats, including malware that uses file-based and fileless exploits.
- The ability to control (allow/block) scripts and processes.
- The ability to detect and prevent threats using behavioral analysis of device activity, application, identity and user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

Optional capabilities often present in EPPs include:

- Risk reports based on inventory, configuration and policy management of endpoint devices.
- Management and reporting of operating system (OS) security control status, such as disk encryption and local firewall settings or substitute functionality.
- Facilities to scan systems for vulnerabilities and report on or manage the installation of security patches.
- Endpoint detection and response (EDR).
- Extended detection and response (XDR).
- Managed services.
- Extended OS compatibility with mobile, containers, virtual instances, and end-of-life and rare OSs.

Magic Quadrant

Figure 1: Magic Quadrant for Endpoint Protection Platforms
Source: Gartner (December 2022)



Vendor Strengths and Cautions

Bitdefender

Bitdefender is a Niche Player in this Magic Quadrant.

Its flagship product, the GravityZone platform, provides integrated EPP, EDR and now XDR capabilities, which are managed from the cloud. All other endpoint security products are provided as add-ons. Bitdefender also offers a rapidly expanding managed detection and response (MDR) service.

Bitdefender is best suited to Type B and C organizations in North America and EMEA that want easy-to-use and effective protection capabilities.

Strengths

- Bitdefender has a strong protection capability. It is consistently a top performer in file-based and fileless malware protection tests.
- Bitdefender offers a modular agent for physical, virtual and cloud platforms, which is managed by a SaaS console for all endpoint/server security administration. It also offers complementary security tools for midsize enterprises, email filtering, storage protection, mobile threat defense (MTD), file sandboxing and vulnerability management.
- Bitdefender's EDR capability is easy to use, partly due to excellent on-screen guidance and contextualization, such as MITRE ATT&CK mapping. Sandbox data and external data sources on file reputation are also well-integrated. Automated response actions ease remediation efforts.
- GravityZone XDR gathers telemetry from third-party applications, such as Microsoft Active Directory, Microsoft Office 365 and Amazon Web Services applications.

Cautions

- On the Completeness of Vision axis, Bitdefender ranks poorly compared to some competitors for its marketing strategy, which is aimed at midsize enterprises.
- Bitdefender's market share and market share growth in the EDR market remain low.
- Although Bitdefender has an easy-to-use EDR capability and an emerging XDR capability (released in the first quarter of 2022), advanced features desired by large enterprises are often missing or late to arrive.
- Application control and MTD are not available on the cloud console.

BlackBerry (Cylance)

BlackBerry (Cylance) is a Niche Player in this Magic Quadrant.

BlackBerry's EPP product suite includes CylancePROTECT (EPP), CylanceOPTICS (EDR) and CylanceGUARD (MDR).

BlackBerry's product improvements in 2022 have so far focused on simplification of investigation, MITRE ATT&CK mappings and sensitive-data policies.

BlackBerry is a good option for organizations looking for converged endpoint security and management, as well as those seeking a suite of MDR services.

Strengths

- BlackBerry's XDR capabilities expanded in 2022 through a partnership with Exabeam and the launch of direct managed services. This enabled integration with Exabeam's Fusion security information and event management (SIEM) solution and granted access to other products and services integrated with it for more expansive detection.
- BlackBerry's Cylance Endpoint Security product set offers protection tools that span PC endpoints, servers and mobile devices. BlackBerry integrates

its CylancePROTECT and CylanceOPTICS products with its unified endpoint management (UEM) capability to operationalize remediation or reconfiguration at scale.
- In addition to MDR, BlackBerry offers a broad suite of services within the CylanceGUARD family, including incident response, security assessment and forensic analysis capabilities that extend beyond managed-EDR-centric services.
- BlackBerry has integrated continuous authentication into its solution via the CylancePERSONA capability, to detect identity-related threats.

Cautions

- After downplaying the better-known Cylance brand in favor of BlackBerry, the company has reversed course and revived the Cylance branding. Although this is a good move, it is confusing for prospective customers.
- BlackBerry's opportunity for cross-selling with its UEM products to manage PC and mobile devices is tempered by its small market share in the UEM market.
- Customers still report a high level of false-positive detections when using versions of Cylance Endpoint Security prior to version 3. We recommend that clients upgrade as soon as possible.
- CylanceOPTICS has a low overall market share and low CylancePROTECT attach rate. Recent improvements in performance, role-based access control and telemetry optimization, and CylanceGUARD should help accelerate adoption of BlackBerry's EDR, however.

Broadcom (Symantec)

Broadcom (Symantec) is a Visionary in this Magic Quadrant.

Its principal EPP is Symantec Endpoint Security Complete (SESC), which includes the company's full EDR and XDR capabilities.

This vendor aims its solutions at very large global Type A and Type B enterprises that want an integrated portfolio of security solutions and enterprisewide licensing agreements. Symantec recently launched a new program to better serve and support small and midsize business (SMB) customers via local distributors.

Broadcom recently announced its intention to acquire the outstanding shares of VMware. At the time of evaluation, however, both Broadcom (Symantec) and VMware met the inclusion criteria for this Magic Quadrant and operated separately. Gartner will provide further insight as more detail becomes available about the future roadmap for these vendors' existing portfolios.

Strengths

- Broadcom (Symantec) achieves its best scores in this Magic Quadrant for the scale and reach of its operations. SESC can be deployed in a hybrid

fashion — that is, partly in the cloud and partly on-premises. It can aggregate logs and alerts from either deployment site.
- Broadcom (Symantec) provides a wide range of additional EPP components, including Active Directory defense, personal firewall, device/application control, and data security. Some solutions also include comprehensive mobile device protection.
- Broadcom (Symantec)'s product benefits from the newly introduced Adaptive Protection, which provides automated and customized execution restrictions for commonly abused application behaviors employed in "living off the land" attacks.
- Enterprise agreements can lower the cost of a portfolio of Broadcom (Symantec) products.

Cautions

- Broadcom (Symantec) receives a low score for marketing execution as it has reduced the size of its sales channel and refocused its efforts exclusively on the largest enterprises. Although Symantec is still a significant player in the overall market, it is losing market share and its customer engagement lags behind that of the Leaders.
- Broadcom (Symantec)'s product score is lowered by our evaluation of its MITRE ATT&CK Phase 4 results, which were lower than the average for this Magic Quadrant.
- Broadcom (Symantec) receives low scores for innovation, due to its limited XDR strategy, beyond integration of the XDR platform into existing enterprise SIEM/security orchestration, automation and response (SOAR) solutions.
- Broadcom (Symantec)'s customer satisfaction score is below average, with very mixed signals coming from different market segments. Gartner clients often raise concerns about Symantec's support and service. Symantec's larger enterprise customers appear more satisfied.

Check Point Software Technologies

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

Check Point Harmony Endpoint provides protection and detection capabilities, including machine learning (ML), behavioral analysis, sandbox analysis and automated remediation of detected threats. Check Point Harmony Endpoint integrates with Check Point Infinity for XDR capabilities across Check Point's endpoint, mobile, Internet of Things (IoT), network, email and cloud workload security products. The company recently launched early availability of Horizon XDR/XPR for networks, endpoints, cloud, email and IoT, and general availability of a Horizon MDR/MPR managed service. Horizon XDR/XPR was not evaluated for this Magic Quadrant but will be considered for evaluation in the next edition.

Check Point is present in all the world's regional markets. Its products suit all types of organizations, especially those that are existing Check Point customers.

Strengths

- Check Point scores well for market understanding and products, as its wide range of integrated security products provides opportunities for consolidation and integration to simplify operations and security.
- Check Point Harmony Endpoint includes a wide variety of nonstandard protection technologies, such as a native (non-OS) personal firewall, USB port control, data loss prevention (DLP), encryption, email phishing protection, content disarm and reconstruction, and the Harmony Endpoint enterprise browser.
- Check Point Harmony Endpoint also covers mobile OSs, such as Android and iOS, as part of an integrated solution.
- Check Point scores highly for customer experience. It emphasizes ease of use for the less mature security organizations, with features such as automated analysis of the attack chain, automated remediation and predefined searches for common threats, such as the Log4j vulnerability and the type of attack to which SolarWinds customers fell victim.

Cautions

- Check Point's scores for Ability to Execute are reduced by its poor market responsiveness, as evidenced by low levels of EPP market penetration and mind share, despite having the resources of a large, respected security vendor.
- Check Point has not developed the deep EDR workflow and custom playbooks or behavioral rules that would appeal to organizations with large, complex security operations centers (SOCs).
- Check Point's EDR capability would benefit from more prescriptive remediation guidance and automation.
- Check Point Harmony Endpoint has a larger "footprint" than many solutions, in terms of both memory and number of services and processes used when all components are installed. Check Point is investing in reducing the Harmony Endpoint footprint.

Cisco

Cisco is a Visionary in this Magic Quadrant.

Cisco Secure Endpoint comes in three tiers — Essentials, Advantage and Premier — each of which adds more EDR and threat-hunting capability. Secure Endpoint is integrated with the other Cisco network and identity security products in Cisco SecureX, a cloud-native XDR platform provided at no extra cost. In early 2022, Cisco launched Cisco Secure Endpoint Pro, a service that provides telephone support, playbooks and defined investigations directly from the Cisco Talos Intelligence Group.

Cisco's focus is on the North American and EMEA markets, but it is also present in Asia/Pacific and Japan, and in South America. Most Cisco customers are Type A or Type B enterprises.

Strengths

- Cisco scores well for marketing strategy and execution. Its success in this regard is reflected in its strong market share.
- Cisco's product and innovation scores benefit from Cisco SecureX, an XDR platform that unites Cisco security capabilities with cross-product case management, search, investigation and remediation capabilities.
- In 2021, Cisco acquired Kenna Security, which provides risk-based vulnerability management to help prioritize patching.
- Cisco scores well for its geographic strategy, due to extensive global channel partner, service and support programs across regions and languages, as well as its extensive training resources.

Cautions

- Cisco Secure Endpoint does not provide native personal firewall or any data security capability.
- Cisco's portfolio of EDR, security service edge (SSE) and secure email gateway (SEG) products is integrated by Cisco SecureX for incident response, but management consoles and policy integration are lacking.
- Manual EDR remediation capabilities, such as remote shell, are not available from the SecureX console.
- Cisco SecureX does not store log data centrally, but fetches data on-demand from other log stores. The Orbital Advanced Search feature has a different interface from Cisco Secure Endpoint or SecureX.

CrowdStrike

CrowdStrike is a Leader in this Magic Quadrant.

The CrowdStrike Falcon Platform now includes a comprehensive set of CrowdStrike's own integrations, including ones for identity protection, cloud security and file integrity monitoring. These sit alongside the existing EDR, managed services, and extras like device control, firewall management, vulnerability management and patching.

In 2021, CrowdStrike acquired Humio, a SIEM solution provider, to build XDR integrations into the Falcon console. Humio technology is now the basis of CrowdStrike Falcon LogScale, which can be used as a long-term storage option. In addition, CrowdStrike recently acquired Reposify, which provides external attack surface management (EASM) capabilities. CrowdStrike has also established the CrowdXDR Alliance and it participates in the Open Cybersecurity Schema Framework (OCSF), both of which aim to develop deeper out-of-the-box integrations with early partners.

CrowdStrike competes globally, but its largest installed base is in North America. Its products suit Type A and Type B organizations. It also offers managed services to suit Type C organizations.

Strengths

- CrowdStrike's highest scores are for market understanding and innovation. These attributes are reflected in the broad scope of its offering, which now includes a growing set of cloud workload protection and container/serverless monitoring features, as well as full support for traditional server workloads.
- CrowdStrike scores consistently highly for customer experience, innovation and overall viability. It has continued to perform well in 2022, despite strong competition from newer entrants to the Leaders quadrant.
- CrowdStrike continues to deliver its own MDR and incident response services to a large percentage of its clients and MDR partners.
- The acquisition of Humio provides CrowdStrike with a strong base for XDR expansion.

Cautions

- CrowdStrike scores poorly for its pricing. Its list prices are generally higher than the average for vendors in this Magic Quadrant, and its discounts smaller, although we are seeing it price more aggressively in 2022.
- CrowdStrike's position in this Magic Quadrant takes account of its 2022 MITRE ATT&CK phase 4 test results, which show less tactic and technique coverage than other vendors in this Magic Quadrant.
- CrowdStrike does not provide an on-premises management option for "air-gapped" or low-bandwidth environments. Nor does it support the Microsoft Windows Server 2003 or Windows XP OSs.
- CrowdStrike's approach to XDR is immature, relative to the XDR approaches of other Leaders in this Magic Quadrant.

Cybereason

Cybereason is a Leader in this Magic Quadrant.

Cybereason offers a cloud-native solution, the Cybereason Defense Platform, with EPP, EDR and MTD capabilities. In 2022, Cybereason partnered with Google to integrate its analytics engine with the back-end SIEM/SOAR capabilities of Google's solutions. It did this to enable XDR deployments and digital forensics and incident response (DFIR) capabilities that help automate investigations.

Cybereason's solution is available from the cloud, and for on-premises or hybrid deployment. The company offers MDR both directly and through partners, with platform inclusion for MDR extending to mobile OSs.

Cybereason targets mainly EMEA, Japan and North America. Its solution is suitable for Type A and B organizations. Additionally, Cybereason's managed

services make it attractive to Type C organizations looking to outsource EDR operations.

Strengths

- Cybereason's presentation of threat data, using its MalOp event categorization to guide threat-hunting activity, can be helpful to organizations new to EDR and threat hunting.
- Cybereason offers broad OS coverage, including mobile OSs. It offers device control to manage removable media, (rogue) device isolation and personal firewall support on OSs, including Linux. Cybereason's Cloud Workload Protection offering provides protection for containerized workloads and specific detection and response capabilities for containerized workspaces.
- Cybereason offers broad platform coverage. It complements this with the ability to examine network traffic for potential indicators of attack (IOAs), email scanning and support for virtual patching.
- Some remediation options are automatically created and can be initiated from the console to address all affected machines. Manual remediations are aided by a remote shell. Quick triage actions, such as kill process, quarantine and isolate, can be taken manually or automated.

Cautions

- Cybereason's Ability to Execute score is impaired by publicly reported staffing reductions that took place in October 2022.
- Cybereason lacks a broad suite of tools beyond those focused on endpoints. For example, it lacks SEG, SSE, NDR and data protection products.
- Cybereason's score for geographic strategy is lowered by its limited language support (only English and Japanese).
- The Cybereason agent architecture installs a high number of processes that use a considerable amount of memory.

Deep Instinct

Deep Instinct is a Niche Player in this Magic Quadrant.

Deep Instinct is a private company based in Israel and the U.S. Its customers are primarily in North America, Europe and Japan.

Deep Instinct has developed a purpose-built, deep learning (DL) framework to automatically prevent malicious files and behaviors. The company's focus is on exploiting its DL expertise to provide autonomous and automated protection without analyst involvement.

Deep Instinct for Endpoint is suitable for organizations looking for a DL-based EPP companion to EDR tools or for more isolated (bandwidth-constrained or air-gapped) and automated use cases.

Strengths

- Deep Instinct scores highly for innovation because of its DL approach to prevention, with a light EDR capability. Behavioral detection mechanisms reside on the endpoint, which reduces dependency on internet connectivity and frequent updates.
- DL is a variant of ML algorithms. It uses multiple layers to solve problems by extracting knowledge from raw data and transforming it at every level, often outperforming traditional ML techniques.
- Recent improvements to Deep Instinct's product include MITRE ATT&CK framework classification of detected threats, reputation analysis, an "EDR-lite" behavioral engine for file-less attacks and registry rollback remediation.
- Deep Instinct provides a dedicated PowerShell DL model to detect malicious PowerShell scripts.

Cautions

- Deep Instinct's product score is reduced by its product's focus solely on prevention, as opposed to detection and response. Its EDR capability is constrained. It does not have detailed event logs. Threat hunting, custom behavioral rules and advanced remediation features are limited.
- Deep Instinct provides only malware prevention. It does not offer any additional endpoint security capabilities, such as a personal firewall, port and device control, or data security, such as encryption. Nor does it provide a broad portfolio of infrastructure security controls.
- Public test results from AV-TEST, SE Labs and MITRE, which use known malware samples, cannot demonstrate that Deep Instinct offers substantial improvement in accuracy over other methods of malware protection.
- For very large enterprises, Deep Instinct's management capabilities, such as role-based administration, are limited, with localization only in English and Japanese management consoles. Its product supports most Windows OSs, including embedded ones, but offers only limited support for macOS and Linux. Deep Instinct has not invested in cloud workload capabilities beyond prevention.

ESET

ESET is a Challenger in this Magic Quadrant.

ESET is a privately owned Slovakian company with 30 years' experience in the EPP industry and a well-recognized research lab. Since the previous edition of this Magic Quadrant, ESET has launched its cloud EDR module on its PROTECT Cloud platform, and Docker protection. The company also offers a malware sandbox and threat intelligence feeds, including new private advanced persistent threat (APT) reports.

ESET appeals mostly to midsize Type B and Type C organizations in the countries it supports, which are predominantly in EMEA and North America.

Strengths

- One of ESET's best scores is for product capability. ESET does well in public anti-malware and performance tests. It was an early adopter of ML techniques. Recent improvements include network brute-force attack protection for Remote Desktop Protocol (RDP), FTP and Server Message Block (SMB) protocol exploits, and improvements to parsing and processing scripts.
- For enterprise customers that require it, ESET provides a deployment architecture for air-gapped systems.
- ESET scores well for its operations capability. The ESET management console is available in 23 languages, which makes it a good fit for globally distributed enterprises and enterprises that require regional localization.
- ESET has introduced MDR and implementation services directly in some countries and via channel partners in others.

Cautions

- ESET scores poorly for market understanding and innovation, as it lagged behind competitors in the rollout of innovative features such as cloud delivery, EDR, direct MDR and XDR.
- Although ESET does well in public prevention tests, its MITRE ATT&CK Phase 4 test results show fewer technique-level detections and indicate the need for a larger than average number of configuration changes.
- ESET did not participate in the Linux portion of the latest MITRE ATT&CK tests, as it did not support Linux at the time of evaluation However, it introduced EDR Linux support in the first quarter of 2022.
- ESET's product scores are weakened by a lack of advanced EDR capabilities and of emerging capabilities such as vulnerability management and configuration management to proactively harden endpoints (due in the first half of 2023).

Fortinet

Fortinet is a Visionary in this Magic Quadrant.

Fortinet has focused its innovation efforts on introducing more artificial intelligence (AI)-trained investigation, automated remediation and support for custom rules, and on enhancing the integration of third-party security products into the FortiXDR console.

FortiXDR combines Fortinet's endpoint, IoT security, network, email, identity and cloud security capabilities, as well as network infrastructure, into one holistic solution. FortiEDR can trigger remediation actions across third-party infrastructure, including firewalls and zero trust network access infrastructure.

Fortinet has a global reach. Its products are well-suited to organizations seeking an integrated XDR security platform.

Strengths

- FortiXDR offers broad integration capability and automated and custom rules. Its EDR provides remote shell access for manual remediation.
- Fortinet can integrate with multiple data lakes and third-party SIEM and data analysis tools, allowing ingestion from cloud and third-party datasets for analysis of threat data.
- Fortinet maintains low resource utilization and broad OS support, despite the addition of new logic and agent capabilities. Its resource utilization is commendably low, in comparison with competing solutions.
- FortiEDR's MITRE ATT&CK test results have greatly improved in 2022.

Cautions

- Fortinet scores poorly for marketing execution. The company's market share and mind share among EDR and XDR buyers remains low, beyond its existing network security customers.
- Fortinet does not provide an integrated capability for MTD on mobile devices, in contrast to vendors with competing and comparably priced solutions.
- Although Fortinet has its own managed services, adoption of them is low, compared with competing services from other vendors.
- Fortinet plans to retire the ability to host its on-premises central manager in offline mode for air-gapped environments. Therefore, in future, all on-premises deployments will require an internet connection from the FortiEDR central manager.

Microsoft

Microsoft is a Leader in this Magic Quadrant.

Microsoft offers a collection of Defender-branded EPP/EDR capabilities across two license tiers in its Defender for Endpoint offering. The base Microsoft Defender Antivirus is included with Windows OS licenses. Threat and vulnerability management, attack surface reduction, EDR, and an increasing array of direct managed services are available in various licensing options.

Microsoft is expanding its security capabilities to macOS, Linux and mobile OSs, as well as solutions for IoT devices. The Microsoft Defender Security Center provides an out-of-the-box XDR capability across Microsoft's security products (EPP/EDR, SEG, cloud access security broker, IoT and Active Directory) complete with automated paybook actions. Microsoft's Sentinel SIEM/SOAR solutions can expand on the security center workflow through integration with third-party vendors. Both Sentinel and Defender for Endpoint solutions benefit from integration with Microsoft's UEM, and from Azure capability.

Microsoft Defender for Endpoint suits Type A, B and C organizations in all regions.

Strengths

- Microsoft's highest scores are for its market understanding and overall viability. This partly reflects the strong performance of its security business. It also reflects an early move to define and evolve the emerging XDR category, with deep integration and automation between Microsoft Defender for Endpoint and other Microsoft products, particularly Azure Active Directory, which enables an emerging identity threat detection and response (ITDR) capability.
- Microsoft Defender External Attack Surface Management is now generally available, which enables better vulnerability management.
- Microsoft provides generous log storage retention by default, and includes web browsing control, device control and network protection. Other vendors often charge separately for these things.
- Partnerships with, for example, AttackIQ and Illusive, and the open log integration capability of Microsoft Sentinel expand integration beyond just Microsoft products.

Cautions

- Microsoft offers numerous licensing and packaging variations and permutations that include Defender for Endpoint security capabilities. Buyers must ensure they get only the products and features they need, or combine their budgets with those of other corporate buyers to acquire broader portfolios of security and collaboration software.
- Microsoft provides only limited support for older OSs. Also, there is no option to host its Defender for Endpoint solution on-premises or to effectively manage systems that do not connect to the internet.
- Microsoft Defender for Endpoint is a complex tool for threat hunting and advanced proactive monitoring. It may not suit organizations without experienced security operations staff or managed security service provider (MSSP) partners.
- Microsoft Defender Experts is not a full MDR service. Additionally, although Microsoft announced Microsoft Security Experts, an MDR service, earlier in 2022, it was available only as a public preview at the time of analysis.

Palo Alto Networks

Palo Alto Networks is a Visionary in this Magic Quadrant.

Its Cortex XDR platform combines endpoint, network, and cloud protection and detection capabilities, as well as integrations with the company's broader infrastructure portfolio and third-party security providers. Cortex XDR is not available in an on-premises or self-hosted version. Palo Alto Networks' Unit 42 MDR service was publicly launched on 3 August 2022; it offers managed threat hunting, and supports initial implementation and tuning of the company's EDR tool.

Palo Alto Networks is appropriate for Type A and Type B organizations with critical assets that require network layer detection and defense.

Strengths

- Palo Alto Networks scores highly for innovation due to the introduction of XDR capabilities to its Cortex XDR platform. The Cortex XDR platform receives weekly updates to its ML, which are delivered efficiently, and can export data to third-party log management tools.
- Palo Alto Networks scores highly for the broad nature of its offering, which includes a combination of network, cloud, and endpoint detection technologies suited to customers with existing investments in its solutions.
- Palo Alto Networks performed well in both of AV-Comparatives' 2021 tests and in the MITRE ATT&CK Phase 4 evaluations in 2022.
- Palo Alto Networks' EPP is sold in eight regions of the world. Of the vendors evaluated in this Magic Quadrant, Palo Alto Networks offers the third-highest number of cloud hosting locations.

Cautions

- Palo Alto Networks receives a low score for market responsiveness, due to its low share of the EPP market.
- Although Palo Alto Networks offers managed services, such as managed threat hunting, adoption is limited (adoption data for the newly launched MDR service was not available for evaluation).
- Although Palo Alto Networks' customer satisfaction scores on Gartner's Peer Insights platform are on par with those of other vendors in this Magic Quadrant, it has lower-than-average scores for ease of integration with standard APIs and tools.
- Palo Alto Networks did not participate in macOS and Microsoft Windows industry tests conducted by AV-TEST in 2022.

SentinelOne

SentinelOne is a Leader in this Magic Quadrant.

SentinelOne provides EDR and XDR capabilities to suit the needs and budgets of a wide range of clients. It also offers its own managed services and partners with leading third-party MDR providers. In 2021, SentinelOne acquired Scalyr, a security log and event management solution provider, to provide the basis of its XDR expansion. Additionally, in May 2022, SentinelOne acquired Attivo Networks for its IDTR capabilities and deception features.

SentinelOne's main markets are North America and EMEA, but this vendor also has a major presence in the Middle East. It has support service options to suit all organization types in each of these regions.

Strengths

- SentinelOne continues to expand its product portfolio based on acquisitions. Notably, it is bringing its Singularity Identity, Singularity Ranger AD and Singularity Hologram deception offerings to market as platform components.
- SentinelOne has continued to expand its network of MDR partners and seen the attach rate for its own managed services increase in the past year.
- Support for legacy Windows OSs, the Apple macOS and numerous versions of Linux is a particular strength. SentinelOne is quick to support the latest Apple chipsets and OSs as they are launched.
- SentinelOne achieved excellent results in the MITRE ATT&CK Phase 4 evaluations of the first quarter of 2022. This reaffirms its ability to detect all attacks and provide full details of the techniques and tactics used.

Cautions

- SentinelOne's marketing execution score is impacted by its lower brand awareness, compared with other Leaders.
- SentinelOne's ability to support on-premises deployments and systems that are not directly connected to the internet is partial. By contrast, it offers fully featured support for cloud-facing systems.
- SentinelOne's XDR product is still evolving, relative to competing solutions from other vendors evaluated in this Magic Quadrant.
- SentinelOne's customers would welcome deeper integrations with network security solutions from major network appliance vendors. These would provide zero trust and service mesh opportunities, and appeal to clients who want to make the most of existing investments.

Sophos

Sophos is a Leader in this Magic Quadrant.

Sophos has continued to expand its Adaptive Cybersecurity Ecosystem (ACE) platform, with three important acquisitions in 2021 and 2022 that jointly improve Linux support, automation and integrations for XDR, and visibility into cloud-hosting environments. Sophos has also addressed the growing need for flexible managed services and threat response options — these are now among the most successful parts of its portfolio. The ACE platform includes both endpoint security and network security features, as well as all the security operations tools needed to integrate and manage them.

Sophos' clients are mainly Type A and Type B organizations, but Type C organizations without security staff are also catered for via fully managed detection and incident response services.

Strengths

- Sophos scores highly for marketing strategy as an early exponent of a full XDR platform. It also scores well for the breadth of its portfolio, which

includes management tools, network and endpoint security products, and support for cloud workloads.
- Sophos offers an MDR service. Third-party services are also available from MSSP partners. Additionally, Sophos launched a fixed-cost Compromise Assessment tool in July 2022.
- In 2022, Sophos added integration with the Microsoft Graph Security API. It has also expanded its integrations with third-party security tools and focused on bringing efficiency gains to its endpoint agent.
- Sophos provides a useful rollback capability for protection against common ransomware and related malware.

Cautions

- Sophos' lowest score is for marketing execution. Its conservative approach to marketing does not generate enough of an opportunity to compete effectively against the other Leaders in this Magic Quadrant.
- Sophos lacks on-premises and private cloud deployment options, and is therefore inappropriate for organizations with these requirements.
- Sophos offers integration between third-party tools and its MDR offering but lacks integration of its own mobile product's data. It also lacks the capability to manage integrated third-party products.
- Sophos had disappointing results in the MITRE ATT&CK Phase 4 evaluations of the first quarter of 2022, compared with those of other Leaders. It had significant numbers of misses and telemetry detections that required expert analysis to detect the associated activity.

Trellix

Trellix is a Niche Player in this Magic Quadrant. Trellix is a new company formed around the combined products of McAfee Enterprise and FireEye.

Trellix is trying to establish its brand as a major competitor in the endpoint security market by undertaking expansive marketing campaigns. The combined products of McAfee Enterprise and FireEye are expansive, but display overlaps that have not yet been resolved. Trellix currently has two EDR offerings — namely the former MVISION and Helix offerings — both of which are separate agents and management consoles.

Trellix's products suit global Type B and C organizations that are prepared for product integration and consolidation.

Strengths

- Trellix scores well for attributes such as operations and viability, due to the depth and breadth of its combined corporate capabilities, its geographic reach, and its mature installed base of loyal customers.
- Trellix's scores for Completeness of Vision are improved by its broad range of security products and tools for legacy systems, as well as its improving

EDR capability with the combination of FireEye and McAfee Enterprise approaches.
- Trellix continues to support FireEye's network security appliances and SIEM/SOAR tools for customers that have invested in these and wish to retain them.
- Trellix is good at supporting customers that have invested in the broad range of McAfee Enterprise's technology and are familiar with its management tools.

Cautions

- Trellix's Completeness of Vision score is held back by the execution risk represented by consolidation of the two EDR products into a single agent and a single management console with consistent UI design.
- Trellix receives a low score for marketing execution as it works to replace two well-known brands with a new, unknown brand.
- Trellix offers a roadmap that includes continued consolidation and streamlining of its products, but the current mix of EDR features spread across two distinct offerings continues to confuse buyers.
- Although Trelix has a three-year agreement with Google (Mandiant) to provide MDR services while it develops its own native capabilities, Google competes with Trelix when it comes to XDR/SIEM capabilities.

Trend Micro

Trend Micro is a Leader in this Magic Quadrant.

Trend Micro has recently consolidated its cloud, server and endpoint security solutions, and has expanded its Vision One XDR brand. Trend Micro supports hybrid on-premises/cloud and pure cloud versions of its Vision One offering. The company has made migration of its existing customers to cloud products a major initiative. It offers rich support in its EPP and EDR products for a broad catalog of current and legacy platforms.

Trend Micro was early in establishing its full XDR platform, which it has expanded using a variety of SOAR, IT service management, and network security enhancements and integrations across the Trend One platform and third-party tools. It has a global presence.

Strengths

- Trend Micro scores very highly for the breadth of its offering and the fact that, as well as core EDR and XDR platforms, it provides device and application control, support for mobile and industrial control systems, DLP, storage security, and hosted network sandboxing services.
- Trend Micro supports a wide range of Linux variants and legacy server platforms. Additionally, it maintains integration with its TXOne joint venture, which focuses on protecting operational technology and IoT endpoints.

- Trend Micro has introduced an Attack Surface Management offering focused on identifying and contributing attack surface risk data to an organization-level quantified risk dashboard.
- Trend Micro scores highly for overall viability. This publicly traded company, listed on the Tokyo Stock Exchange, has a global reach, a consistent customer base and sustained financial performance.

Cautions

- Trend Micro's market responsiveness score reflects its relatively small share of the overall EDR market and of deals for over 500 seats.
- Although Trend Micro has prioritized efficiency in its agent, with major improvements to size and memory footprint, the agent remains larger than others, owing to its vast catalog of platform support.
- Although Trend Micro offers full management of its products via an MDR offering, this is used by only a minority of the company's existing customers.
- Trend Micro's XDR integration is richest among its own products — the company has only a modest number of third-party integrations.

VMware

VMware is a Visionary in this Magic Quadrant.

The VMware Carbon Black Endpoint offers EPP and EDR capabilities and MDR services across PCs, servers and cloud workloads. In 2022, VMware has invested in the rollout of a VMware-delivered MDR offering and the introduction of the Contexa threat intelligence product. Contexa combines network and email security data with endpoint telemetry from other VMware security tools for vulnerability and risk assessment with automated remediation.

VMware products suit Type A and Type B organizations, particularly those that have invested in VMware vSphere and VMware NSX.

Broadcom has announced an intention to acquire the outstanding shares of VMware, but, at the time of evaluation, both Broadcom (Symantec) and VMware met the inclusion criteria for this Magic Quadrant and continued to operate separately. Gartner will provide additional insight as more detail becomes available about the future roadmap for these vendors' existing portfolios.

Strengths

- VMware XDR powered by Contexa provides integration, qualification and correlation of threat intelligence from multiple VMware and third-party tools, and a platform for automating response and remediation.
- In 2022, VMware introduced a direct MDR offering, which it has expanded with automated containment.
- VMware scores very highly for operations, given its extensive channel and market penetration.

- VMware Carbon Black Cloud enhancements include integration of its data into ServiceNow security tools and integration with Proofpoint for identification, ingestion and cross-product remediation of email threats.

Cautions

- VMware receives a below average score for market responsiveness, due to its low market share relative to the execution potential of its sales channel.
- VMware's product score is impacted by a lower overall score in the MITRE ATT&CK WizardSpider+Sandworm 2022 tests relative to competitors in this analysis.
- VMware's innovation score is limited by the pace at which it introduces new functionality.
- The impact of the Broadcom acquisition on VMware's products cannot yet be determined, but we advise clients pursuing multiyear investments to increase their diligence.

WithSecure

WithSecure is a Niche Player in this Magic Quadrant.

WithSecure is a new company that was formed in June 2022 when F-Secure's corporate security business was demerged from F-Secure's consumer operations and rebranded. It is a publicly traded Finnish company. WithSecure Elements provides cloud-native EPP and EDR capabilities, as well as email, collaboration protection for Microsoft Office 365 and vulnerability management. WithSecure Countercept provides MDR services.

Most of WithSecure's customers are in EMEA, Asia/Pacific and Japan. WithSecure's Elements offering is appropriate for resource-constrained Type B and Type C organizations.

Strengths

- WithSecure's product score reflects recent improvements, including a memory scanner for deployment during an incident, chained EDR response actions and proactive administrator notifications of misconfigured endpoints.
- A premium EPP feature called DataGuard provides policy-based ringfencing for assigned files or folders as an extra layer of ransomware protection.
- WithSecure offers a General Data Protection Regulation (GDPR)-compliant MDR service for EU customers.
- WithSecure Elements' EDR capability is easy to set up and use. Additionally, it has a unique option to elevate alerts directly from the console to WithSecure's threat hunters, who offer a two-hour response time.

Cautions

- WithSecure’s efforts to serve more than mainly midsize enterprises have had mixed results. The rebranding of the company and its offerings could slow its growth into new areas.
- WithSecure’s XDR solution is immature and, out of the box, integrates with only Microsoft Office 365. WithSecure’s product portfolio lacks data security, network, SSE and SEG solutions.
- WithSecure’s EDR capability does not extend to custom detection rules or playbooks. Threat hunting is limited, and there is no ability to integrate with external threat feeds.
- WithSecure has performed well in tests run by AV-TEST, but its MITRE ATT&CK Round 4 test results reveal gaps in both analytic coverage and detection count, in comparison with Leaders in this Magic Quadrant.

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

- Deep Instinct
- Palo Alto Networks
- Trellix

Dropped

- FireEye (see Trellix)
- F-Secure (replaced by WithSecure)
- McAfee (see Trellix)
- Panda Security

Inclusion and Exclusion Criteria

For a Magic Quadrant, Gartner analyzes the most relevant providers in a market. Gartner sets an upper limit of 20 vendors per Magic Quadrant, these being the most relevant vendors in the market.

The following inclusion criteria represent the specific attributes that Gartner analysts deemed necessary for a vendor to be evaluated in this Magic Quadrant.

Inclusion Criteria

To qualify for inclusion in this Magic Quadrant, vendors had to meet the following criteria at the start of Gartner's research and survey process.

Core Inclusion Criteria

To be included in this Magic Quadrant, each vendor had to satisfy at least 12 of the following criteria using only its own nominated solution(s):

- The solution protects against known and unknown malware without relying on daily agent/definition updates.
- There is a facility to detect malicious activity based on the behavior of a process.
- The solution stores IOCs\IOAs in a central location for retrospective analysis for at least 30 days and allows subsequent forwarding to other long-term retention storage where required by the client.
- The capability to detect and block script-based attacks, "living off the land" attacks and other exploits that do not introduce new executable processes to the endpoint.
- The solution removes malware automatically, once it is detected (that is, it deletes or quarantines files, kills processes and automatically removes artifacts).
- The solution enables false positives to be suppressed or ignored from the management console without excluding all protection techniques (for example, it must be able to suppress file detection but still monitor behavior).
- The primary EPP console uses a cloud-based, SaaS-style, multitenant infrastructure that is operated, managed and maintained by the vendor.
- Reporting and management console views display a full process tree to identify how processes were spawned, for actionable root cause analysis.
- Threat hunting is provided, including the facility to search for an IoC/IoA (such as a file hash, source or destination IP address or registry key) across multiple endpoints from the management console.
- The solution identifies changes made by malware and provides recommended remediation steps or a rollback facility.
- There is an option to integrate threat intelligence and reputation services into the solution.
- The solution protects against common application vulnerabilities and memory exploit techniques (such as process injection and dynamic-link library sideloading).
- The solution continues to protect and collect suspicious event data when the managed endpoint device is outside the corporate network or offline.
- The solution performs scheduled static, on-demand malware detection scans of folders, drives or devices such as USB drives.
- The solution can detect misuse of identity and tokens, and lateral movement associated with this misuse.

Optional Inclusion Criteria

To be included in this Magic Quadrant, vendors also had to satisfy at least four of the following criteria:

- The solution implements named vulnerability shielding (also known as virtual patching) for known vulnerabilities in the OS of the protected endpoint device and for non-OS applications.
- Provision of risk-based vulnerability reporting and prioritization of remediation actions.
- The solution implements configurable default-deny allow/block listing (of applications, for example), with trusted sources of change.
- The ability to provide protection, detection and response capabilities for cloud workloads, including serverless workloads.
- The endpoint agent has identity and/or endpoint-based deception capabilities (lures) designed to expose attackers and track their activity.
- The vendor offers managed alerting and monitoring services that alert customers to suspicious activity and provide guided remediation advice (managed detect and respond services, for example).
- The vendor offers remote managed deployment, configuration services, and detection and removal of threats on behalf of the client.
- The solution supports advanced queries across multiple endpoints and combines multiple events into a single incident.
- The solution includes playbooks and guided analysis and remediation, based on intelligence gathered by the vendor (for example, “the next steps needed to contain this threat are XYZ”).
- Reporting capability for attribution information and potential motivations behind attacks, including mapping of events and alerts to MITRE ATT&CK tactics, techniques and procedures (TTPs).
- The vendor provides a hybrid solution with capabilities comparable to its cloud-managed principal capability for air-gapped or non-internet-facing systems.
- Integration of alerts and workflows from other security solutions, including those of third parties.
- The ability to correlate and enrich weak events or alerts, from multiple sources or sensors, into strong detections.
- The solution can coordinate responses across multiple security products (for example, It can initiate a change in configuration, detection, blocking or removal using two-way API integration with other tools).
- The ability to show the overall security posture of the managed estate and give insights into exposure to the latest threats.

Exclusion Criteria

- If a vendor did not satisfy at least 12 of the core inclusion criteria, and four optional capabilities overall, it did not qualify for inclusion in this Magic Quadrant.

- A vendor could be excluded if the majority of detection events did not come from its own detection agent and the techniques used were not designed, owned and maintained by the vendor itself. However, vendors were permitted to augment their solution(s) with an OEM engine, provided the OEM or third-party agent/sensor was not the primary means of detection. Vendors also had to provide their EPP independently of any other solution or service.
- If a vendor had not participated in independent, well-known, public tests of accuracy and effectiveness — such as those of AV-TEST, AV-Comparatives, MITRE, MRG Effitas and SE Labs — within the 12 months prior to 30 June 2021, it was considered for evaluation only if it was a current participant in the VirusTotal public interface. (Participation in other public tests was considered if they were equivalent to those listed above.)
- A vendor had to have more than 7 million enterprise active seats using its EPP as their sole EPP, as of 28 January 2022. Of these, more than 500,000 had to be active installations with accounts larger than 500 seats. The proportion of enterprise customers in a single region outside North America could not exceed 60% of the total number.
- Due to a pause in coverage of all Russian vendors by Gartner, there may be Russian vendors that meet the inclusion criteria described but were not evaluated. These vendors are not included in this research.

Evaluation Criteria

Ability to Execute

Gartner analysts evaluate vendors on the quality and efficacy of the processes, systems, methods and procedures they use to be competitive, efficient and effective, and to improve their revenue, retention and reputation.

Product or Service: Core goods and services offered by the vendor that compete in/serve the defined market. This includes current product/service capabilities, quality, feature sets, skills etc., whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the MQ/CC inclusion criteria.

Overall Viability (Business Unit, Financial, Strategy, Organization): Viability includes an assessment of the overall organization’s financial health, the financial and practical success of the business unit and the likelihood of the individual business unit to continue to invest in the product, continue offering the product and advancing 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 in order 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, 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, etc.

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.

Table 1: Ability to Execute Evaluation Criteria

Enlarge Table

Evaluation Criteria	We
Product or Service	Hig
Overall Viability	Lov
Sales Execution/Pricing	Me
Market Responsiveness/Record	Hig
Marketing Execution	Lov

Evaluation Criteria	We
Customer Experience	Hig
Operations	Me

Source: Gartner (December 2022)

Completeness of Vision

Gartner analysts also evaluate vendors on their ability to convincingly articulate logical statements relating to current and future market direction, innovation, customer needs, and competitive forces. We evaluate how well these statements correspond to Gartner's view of the market.

Market Understanding: This criterion addresses a vendor's ability to understand customers' needs and to translate that understanding into products and services. Scoring focuses on three areas:

1. Matching of products to emerging threats and providing services to meet demand.
2. Cloud-native hosting and use of own and third-party integrations in response to advances and changes in the industry and in technology.
3. Responses to market shifts and historic adjustments of the roadmap to include EDR capabilities and combine separate agents into one.

Marketing Strategy: The vendor's ability to provide 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: This criterion looks for an approach to product development and delivery that emphasizes market differentiation, functionality, methodology, and features that relate to current and future requirements.

Data submitted by vendors via a questionnaire, as well as videos they submitted to demonstrate their products using a Gartner-supplied script, were used to determine current functionality and how it has been improved. These sources of information also identified strategic product plans that will lead to enhanced capabilities in future.

Innovation: This criterion addresses a vendor's ability to create direct, related, complementary and synergistic layouts of resources, expertise or capital, for investment, consolidation, defensive or preemptive purposes.

We assess each vendor's current roadmap and historical performance and leadership in terms of:

1. Delivery of alternative approaches and new technologies.
2. Additional protection and capabilities, and positive contributions to the information security community.
3. Following others' lead (merely delivering catch-up or tick-box features attracts a neutral or low score).

Geographic Strategy: This criterion addresses a vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside its "home" or native geography, either directly or through partners, channels and subsidiaries, as appropriate for the geography and market. Assessment includes:

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 vendor itself or by partners.
3. Localization of the products, including coverage of right-to-left alphabets and double-byte character sets.

Table 2: Completeness of Vision Evaluation Criteria

Enlarge Table

Evaluation Criteria	Weightin
Market Understanding	High
Marketing Strategy	Medium
Sales Strategy	NotRated
Offering (Product) Strategy	High

Evaluation Criteria	Weightin
Business Model	NotRated
Vertical/Industry Strategy	NotRated
Innovation	Medium
Geographic Strategy	Low

Source: Gartner (December 2022)

Quadrant Descriptions

Leaders

Leaders demonstrate balanced and consistent progress and effort in relation to all Ability to Execute and Completeness of Vision criteria. They have broad capabilities in advanced malware protection, and proven management capabilities for large enterprise accounts. Increasingly, leaders provide holistic XDR platforms that enable customers to consolidate their other tools and adopt a single-vendor solution. However, a Leader should not be a default choice for every buyer. Clients should not assume that they must buy only from a Leader.

Leaders may be less able to quickly react when Visionaries challenge the status quo in the market.

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 strong sales and visibility, which add up to a better Ability to Execute than Niche Players have. Challengers, however, are often late to introduce new capabilities, lack some advanced capabilities, and lack a fully converged strategy. This affects their positions for Completeness of Vision, when compared with Leaders. Challengers are solid, efficient and expedient choices.

Visionaries

Visionaries deliver the leading-edge features that will be significant in the next generation of products, and that 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 lack market share. Clients pick Visionaries for best-of-breed features.

Niche Players

Niche Players offer solid products, but rarely lead the market in terms of features and functions. Some vendors are Niche Players because they serve a specific region or customer type. Others are Niche Players because they focus on excellence in a specific feature. Niche Players can be a good choice for existing customers, conservative organizations in supported regions, and organizations looking to augment an existing EPP for a “defense in depth” approach.

Context

Endpoint protection is the most commonly deployed layer of malware prevention and is considered an aspect of basic security hygiene for all organizations. Although there are some use cases that justify continuing with on-premises management, according to Magic Quadrant vendor surveys 82% of EPPs are now cloud-delivered. Providers that can accommodate on-premises hosting are now rare.

EDR is a required component of a mature endpoint security strategy and, as such, receives emphasis in this analysis. EDR solutions provide capabilities that detect and protect against advanced attacks, investigate security events, contain attacks and produce guidance for remediation. Roughly 42% of corporate endpoints have EDR, and this number increased by 40% between 2020 and 2021.

MDR usage is increasing rapidly. More than 20% of EPPs are managed by third parties. Increasingly, vendors are delivering direct management services for their products.

EDR has made maturing SOCs hungry for more integrated investigation and remediation capabilities that are easier to use and deploy than traditional tools. As a result, buyers are increasingly looking for XDR capabilities. XDR is a vendor-specific threat detection and incident response tool that unifies multiple security products into a security operations system. Primary functions include security analytics, alert correlation, incident response and incident response playbook automation.

Many of the vendors in this report offer extended endpoint protection tools that offer more than malware protection. These include personal firewalls, USB port protections, and encryption and DLP tools. Others provide an expansive set of infrastructure security controls, such as email and network gateways, data security and cloud controls.

According to the 2022 Gartner CISO Security Vendor Consolidation XDR and SASE Trends Survey, most buyers (approximately 75%) have security solution consolidation efforts underway. To future-proof their EPP investments, buyers must consider how well a solution fits in with consolidation efforts, managed services needs and the future direction of the SOC, in addition to the EPP's technical features.

Market Overview

EDR is now a common and mature feature of EPP solutions. Recent MITRE tests have illustrated EDR's strength in detecting complex attacks.

As EDR becomes mature and mainstream, the key issue for EPP buyers will be how well a solution fits in with their plans for SOC operations.

Fileless attacks are now a common part of all malware types, which makes the behavioral protection of EDR tools a critical capability. Advanced adversaries can evade any protection solution, which makes detection and hunting essential for a fast incident response. EDR should now be considered a mandatory capability, but only 42% of enterprise endpoints have it.

XDR is emerging as the newest capability for EPP solutions. The 2022 Gartner Security Vendor Consolidation XDR and SASE Trends Survey found that 21% of respondents had already acquired an XDR capability. These organizations are predominantly in the 1,000-to-10,000-seat midsize-enterprise sector in North America and EMEA.

XDR provides a threat detection and incident response tool that unifies multiple security products into a common incident response and hunting toolset. Recent attack trends illustrate the need for integration with identity access management tools and SEGs at minimum, as phishing and credential misuse are involved in the majority of breaches.

Although some organizations may want the endpoint agent to be only a source of telemetry for their existing integrated security operations (SIEM/SOAR), others are considering EDR a basis for XDR integration.

All organizations need better-prioritized hardening guidance. EPPs are increasingly offering vulnerability analysis, with some more advanced solutions also including endpoint configuration guidance. However, misconfiguration of EPP/EDR solutions is a common root cause of recent breaches. We expect further improvements to preincident risk assessments and hardening guidance as peri- and post-incident capabilities become less differentiated across vendors.

Ransomware remains the biggest malware risk for all organizations. Recent changes in ransomware include the use of alternative system calls to acquire files, the acceleration of human-operated ransomware, the expansion of affiliate attacks, and an increase in data theft and "doxing" threats. We expect data theft to increase as extortion-based attacks move to cloud data repositories by exploiting stolen

credentials. Destructive attacks (also known as wipers) may also spill out of the Russian invasion of Ukraine. These emerging threats are driving parallel innovation in the detection and response techniques used by EPP and EDR vendors.

Effective tamper and bypass protection to ensure agents are not disabled is critically important to withstand attacks by the more skilled adversaries.

The biggest barrier to adoption of EDR tools remains the skills required to operate them and the increased total cost. On average, EDR capabilities add an extra 37% to initial costs, and adoption of EDR must be accompanied by investment in training to be effective. XDR will further increase training requirements.

To alleviate the skills gap, MDR services that provide monitoring and alert triage are becoming much more popular. Currently, 18% of EDR endpoints are managed by a third party, and 50% of managed services are delivered by EPP solution providers directly, rather than through channel partners. Several large vendors evaluated in this Magic Quadrant recently launched new MDR programs. We expect MDR adoption to increase dramatically.

Remote working has significantly accelerated adoption of cloud-managed offerings, which now represent 80% of the installed base. Buyers should look for indicators that solutions are truly designed for cloud delivery and not simply management servers shifted to the cloud. Hybrid deployment offerings are less common and should be a high priority for buyers that have regulatory issues, low bandwidth, or air gaps that make cloud adoption difficult.

EPP solutions may also gain MTD capabilities and integrate with UEM 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 the postinfection stages of an attack or exploit)
EPP	endpoint protection platform (provides prevention of malware and exploits)

MDR	managed detection and response (capabilities focused on quickly detecting, investigating and actively mitigating incidents)
ML	machine learning (used, for example, 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 the team that works in it)
XDR	extended detection and response (a unified system combining telemetry source and integrating multiple tools into a single console usually with automation and AI-powered analytics for faster and more accurate detection and response)

Evidence

Gartner's Magic Quadrant team used data from the following sources:

- More than 3,000 client inquiries since January 2022
- More than 4,500 Peer Insights reviews on gartner.com
- Vendors' answers to a survey containing over 500 questions about product and service capabilities and enhancements through 4Q22, as well as 30-minute demonstrations by each vendor
- The 2022 Gartner CISO Security Vendor Consolidation XDR and SASE Trends Survey

2022 Gartner CISO Security Vendor Consolidation XDR and SASE Trends Survey

This survey was conducted to determine how many organizations are pursuing vendor consolidation efforts, what the primary drivers are for consolidation, the expected or realized benefits of consolidation, and how those that are consolidating are prioritizing their consolidation efforts. Another key aim of this survey was to collect objective data on XDR and secure access service edge (SASE) for consolidation of megatrend analysis.

The survey was conducted online during March and April 2022, with 418 respondents from North America (the U.S. and Canada; n = 277), Asia/Pacific (Australia and Singapore; n = 37) and EMEA (France, Germany and the U.K.; n = 104). Each respondent represented an organization with $50 million or more in 2021 enterprisewide annual revenue. Industries covered included manufacturing, communications and media, IT, government, education, retail, wholesale trade, banking and financial services, insurance, healthcare providers, services, transportation, utilities, natural resources, and pharmaceuticals, biotechnology and life sciences.

Respondents were screened for job title, company size, job responsibilities (which included those of information security/cybersecurity and IT roles), and primary involvement in information security.

Disclaimer: The results of this survey do not represent global findings or the market as a whole. They reflect the sentiments of the respondents and companies surveyed.

Note 1: Definitions of Type A, Type B and Type C Organizations

Type A Organizations

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

Type A organizations are 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 technological change is to run projects in parallel, with multiple teams working on technology and business changes simultaneously. With regard to EPPs, these organizations focus on best-of-breed prevention, detection and response, and rarely require managed security service (MSS)/MDR capabilities.

Type B Organizations

Type B organizations aim to stay relatively current in terms of technology without getting too far ahead or behind their competitors.

Type B organizations are 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 and benefits of early use of new technology. Their focus is on technology deployments that improve their productivity, product quality, customer service and security.

Type B organizations typically wait for technologies 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 solutions. In terms of EPPs, these organizations focus on a blended approach involving prevention, detection and response capabilities that can be complemented with managed services where needed.

Type C Organizations

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

Type C organizations are the second-largest group. They experience severe budgeting and staffing resource constraints and, as a result, prefer simply to deploy and use integrated solutions with the managed service add-ons that can best complement their minimal staff.

These organizations wait for technologies to become stable and for acquisition and operation costs to reach the lowest quartile before committing to purchase. In terms of EPPs, these organizations focus on prevention, rather than on integrated detection and response capabilities and solutions that offer managed services.

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.