Magic Quadrant for Endpoint Protection Platforms

31 December 2023 - ID G00789052 - 51 min read

By Evgeny Mirolyubov, Max Taggett, **and 2 more**

All solutions in this research offer strong protection against most common attacks. Advanced EDR features, managed services, identity threat detection and response, broader workspace security, security configuration management, and emerging XDR capabilities are the most significant differentiators.

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.

Gartner defines an endpoint protection platform (EPP) as security software designed to protect managed end-user endpoints — including desktop PCs, laptop PCs, and mobile devices — against known and unknown malicious attacks. Additionally, EPPs provide capabilities for security teams to investigate and remediate incidents that evade prevention controls. EPP products are delivered as software agents deployed to endpoints and connected to centralized security analytics and management interfaces.

EPPs provide a defensive security control to protect end-user endpoints against known and unknown malware infections. EPP prevention capabilities are deployed as a part of a defense-in-depth strategy to help reduce the attack surface and minimize the risk of endpoint compromise. EPP detection and response capabilities are used to uncover, investigate, and respond to endpoint threats that evade security prevention, often as a part of broader security operations platforms.

The standard capabilities of an EPP are:

- Prevention of, and protection against, security threats, including malware that uses file-based and fileless attack techniques
- The ability to detect and prevent threats using behavioral analysis of device activity, application, identity and user telemetry

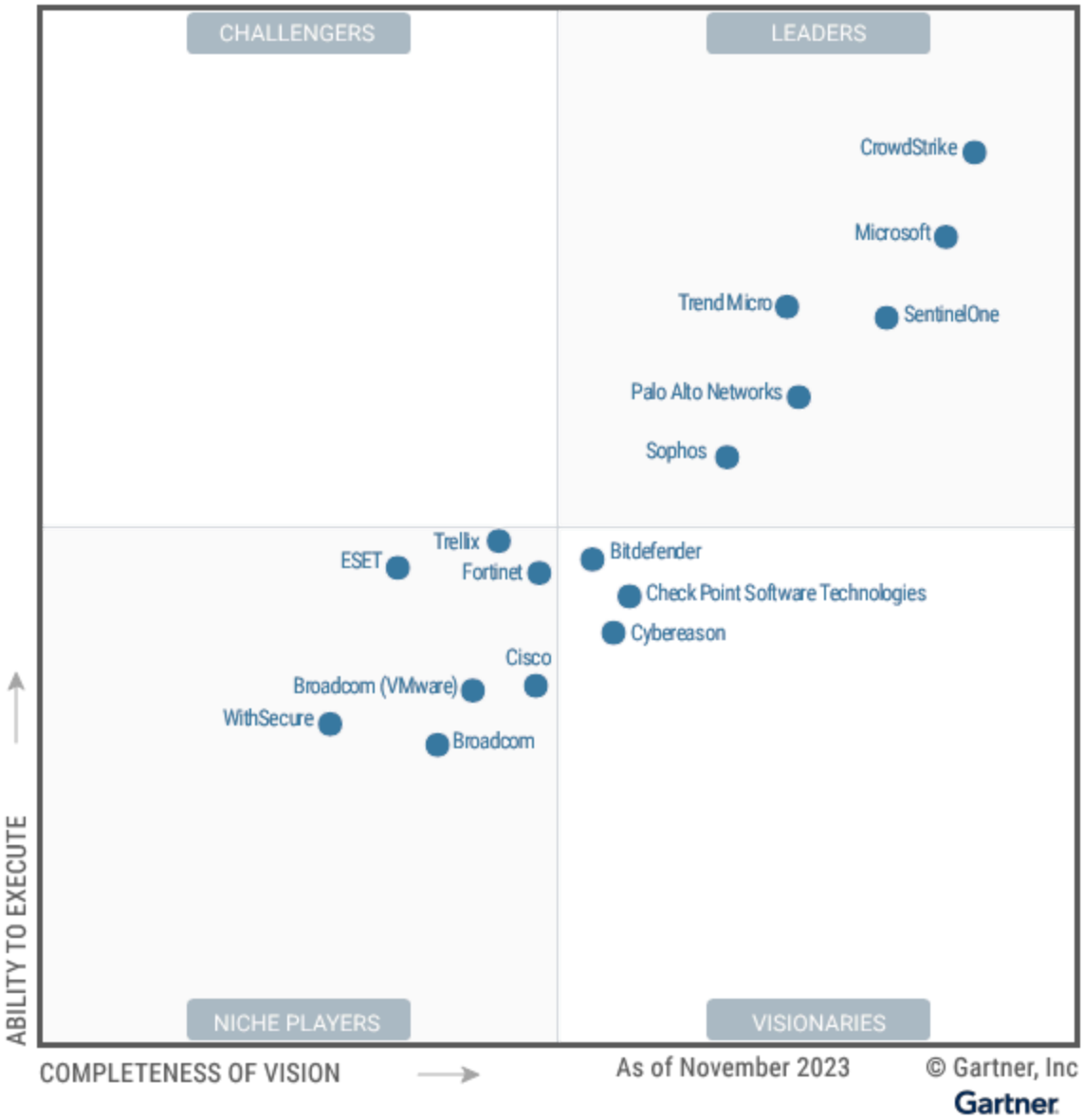
- Facilities to detect and investigate incidents and to obtain guidance for remediation when threats evade prevention controls
- Management and reporting of operating system security controls, such as host firewall and device control
- Integrated endpoint detection and response (EDR) functionality

The optional capabilities often present in EPPs include:

- Risk reports based on inventory, configuration and policy management of endpoint devices
- Facilities to assess endpoints for vulnerabilities and report on or manage the installation of patches or mitigating security controls
- Natively integrated extended detection and response (XDR) functionality with add-on modules such as identity protection, email security, server and workload protection
- Vendor-managed service wrappers, such as threat hunting, managed detection and response (MDR) and digital forensics and incident response (DFIR) retainer
- Extended support for end-of-life or uncommon operating systems

Magic Quadrant

Figure 1: Magic Quadrant for Endpoint Protection Platforms



Source: Gartner (December 2023)

Vendor Strengths and Cautions

Bitdefender

Bitdefender is a Visionary in this Magic Quadrant. Bitdefender GravityZone is the flagship EPP product with integrated prevention, protection, detection and response capabilities. Software add-ons include mobile security, patch management, full disk encryption, storage security and other components centrally managed through the GravityZone management console. Bitdefender is also a recognized OEM vendor supplying its AV, URL inspection and other protection engines to numerous security vendors.

Bitdefender's flagship EPP product suits small and midsize businesses, prioritizing ease of use, protection efficacy and flexibility to deploy in the cloud or network-constrained environments.

Strengths

- Bitdefender's product benefits from its relative ease of use, enhanced incident contextualization and remediation guidance, broad support for legacy and rare OSs, and strong protection efficacy. Recent improvements include protection against ransomware attacks launched from unmanaged devices over shared folders.

- Bitdefender shows strong market understanding and innovation, with an early focus on endpoint and human risk analytics — integrated tools that help identify and remediate endpoint OS weaknesses, and identity attacks.

- Bitdefender's product benefits from its EDR capability that records a comprehensive set of raw endpoint telemetry used for detection and investigation purposes. A network attack defense sensor provides embedded DPI technology for deep network visibility.

- Bitdefender's sales execution benefits from generally lower-than-average prices compared to other vendors in this Magic Quadrant.

Cautions

- Bitdefender's below-average market responsiveness and track record are attributed to its low share of the EPP market and slow adoption of EDR capabilities.

- Bitdefender's product XDR capability is limited and may be insufficient for experienced analysts looking for custom response automation. It also has fewer third-party integration options compared to Leaders in this Magic Quadrant.

- Bitdefender's geographic strategy is impacted by the limited cloud hosting options it offers and a lack of solid presence in regions such as the Asia/Pacific, Middle East, Africa and Japan.

- Its product requires a separate administration console for mobile security management of iOS, Android and Chromebook devices. Mobile security features are yet to be integrated with the vendor's XDR solution.

Broadcom

Broadcom is a Niche Player in this Magic Quadrant. Symantec Endpoint Security (SES) Complete is the flagship EPP product available as a fully cloud-based, hybrid or on-premises deployment. In 2023, Broadcom focused its product strategy on improving ease of use through better alert quality and incident visualization, Adaptive Protection customization features, and AI-assisted threat investigation and hunting capabilities.

Broadcom's flagship EPP product mostly suits large global enterprises familiar with the vendor's offering that have expertise in operating the solution in-house, have a preference for enterprise agreements, and require flexibility to deploy in the cloud or in network-restricted environments.

In November 2023, Broadcom completed the acquisition of VMware. At the time of this evaluation, both Broadcom and VMware met the inclusion criteria for this Magic Quadrant and operated as

separate entities. Gartner will provide further insight as more details become available.

Strengths

- Broadcom's product benefits from improved incident visualization capabilities, which provide a better experience for security analysts performing threat investigations.
- Broadcom's product includes continued advancements in its Adaptive Protection capabilities designed to restrict the execution of trusted applications running on the endpoint. Recent enhancements include configuring granular exceptions based on the prevalence of living-off-the-land behaviors in the customer environment.
- Broadcom's market understanding benefits from the Active Directory prevention capabilities it introduced to mitigate credential harvesting and lateral movement attack techniques.
- Broadcom's product strategy benefits from comprehensive mobile security included in its flagship EPP product. Recent improvements include protection against malicious URLs delivered in SMS messages as part of phishing attacks.

Cautions

- Broadcom's market responsiveness and track record are challenged as the vendor continues to lose market share and client engagement.
- Broadcom's customer experience assessment is impacted by the mixed signals coming from different market segments. Gartner clients often raise concerns about the vendor's customer support and service. Its larger enterprise customers have reported being more satisfied.
- Broadcom's product lacks credible MDR service and XDR product strategies. SES Complete XDR functionality is limited to integration with CloudSOC, Broadcom's CASB solution, in addition to third-party security information and event management (SIEM) and security orchestration, analytics and reporting (SOAR) integrations.
- Broadcom's geographic strategy assessment reflects a generally lower market penetration in regions outside North America. The vendor offers fewer cloud hosting points of presence than average among the vendors included in this Magic Quadrant.

Broadcom (VMware)

Broadcom (VMware) is a Niche Player in this Magic Quadrant. VMware Carbon Black Cloud is the flagship EPP product. It combines protection capabilities for endpoints, mobile devices and workload security capabilities under a unified management console. In 2023, Broadcom (VMware) focused its product strategy on expanding XDR capabilities to include agent-based network and identity visibility, and ecosystem integrations with IAM and email security providers. Broadcom (VMware) has also announced advancements in workload protection, including runtime protection for Linux containers and Kubernetes.

Broadcom (VMware)’s flagship EPP product suits enterprises looking for a mix of endpoint and cloud security capabilities, particularly in the VMware technology ecosystem.

In November 2023, Broadcom completed the acquisition of VMware. At the time of evaluation, both Broadcom and VMware met the inclusion criteria for this Magic Quadrant and operated as separate entities. Broadcom has publicly stated its intention to divest the Carbon Black product. Gartner will provide further insight as more details become available.

Strengths

- Broadcom (VMware)’s product benefits from a mature EDR capability. Recent enhancements include combining deep endpoint network visibility via embedded network IDS with endpoint identity, authentication, and application data in a single console.
- The vendor’s geographic strategy and operations are strong, given its extensive channel ecosystem and market penetration.
- Broadcom (VMware)’s product strategy includes expanded coverage of Carbon Black App Control to air-gapped and cloud environments.
- The vendor’s product benefits from the newly added capability to assess the security configuration of the Windows Server OS against the Center for Information Security (CIS) benchmarks for compliance purposes.

Cautions

- As of this writing, the acquisition of VMware by Broadcom is a continuing concern. In a recent survey of Gartner clients, most either view the future of VMware negatively or are taking a cautious approach to committing to its long-term future. Without insight into a product integration roadmap and the potential for two nearly identical products in the same portfolio, there is some uncertainty about the future.
- Broadcom (VMware)’s market responsiveness and track record are challenged due to its relatively low market share and growth.
- The vendor’s product strategy and innovation are impacted by a lag in the rollout of innovative EPP features and prevention capabilities such as host firewall management. Its XDR solution offers limited third-party security ecosystem integration compared to Leaders in this Magic Quadrant, and may be insufficient for experienced analysts looking for flexible detection and response customization across multiple security controls.
- Broadcom (VMware)’s product offers limited integration of the popular Carbon Black App Control with the vendor’s cloud-delivered flagship EPP product. Carbon Black App Control is only available as an on-premises product.

Check Point Software Technologies

Check Point Software Technologies is a Visionary in this Magic Quadrant. Check Point Harmony Endpoint is the flagship EPP product supporting cloud, on-premises and hybrid deployment options. In 2023, Check Point's product strategy focused on further integrating its solution portfolio, expanding data security controls and enhancing identity protection. Check Point also launched a generally available version of the Horizon XDR offering, integrating data from the vendor's endpoint, network, identity, data and email security products.

Check Point's flagship EPP product generally suits organizations prioritizing ease of use, deploying EDR capabilities for the first time and pursuing security vendor consolidation.

Strengths

- Check Point demonstrates a strong market understanding and industry/vertical strategy due to its wide variety of integrated workspace security products, providing opportunities for consolidation and appealing to clients across the industrial spectrum.
- Check Point's product benefits from the recent general availability of its Horizon XDR product and EDR enhancements, including improved correlation of alerts into incidents and features such as automatic analysis of the attack chain and automated remediation for common threats.
- Check Point's product has a generally intuitive management console emphasizing ease of use for less mature security organizations. Recent enhancements include a new managed security service provider (MSSP) portal that improves centralized tenant management capabilities.
- Check Point's sales execution benefits from generally lower-than-average prices compared to other vendors in this Magic Quadrant.

Cautions

- Check Point's below-average market responsiveness and track record are attributed to low market and mind share among EPP buyers, despite having the resources of a large, respected security vendor and an integrated security platform.
- Check Point's product lacks a graphical attack view and prescriptive remediation guidance, and has limited customization capabilities for detection and response rules. The vendor's secure access service edge (SASE), IoT, cloud and mobile security products are yet to be integrated with Horizon XDR/XPR.
- Check Point's product consumes more endpoint disk space than most other solutions evaluated in this Magic Quadrant, despite recent improvements to CPU utilization and more acceptable memory utilization rates.

- Check Point's operations are impacted by fewer certifications obtained for the solution, lagging behind other vendors in this research. For example, Check Point does not have a FedRAMP-certified product version.

Cisco

Cisco is a Niche Player in this Magic Quadrant. Cisco Secure Endpoint is the flagship EPP product, which includes prevention, protection, detection and response capabilities. In 2023, Cisco focused its innovation efforts on integrating its flagship EPP product as a native module in Cisco Secure Client, unifying its AnyConnect VPN and SSE security capabilities with EPP. Cisco released a new XDR solution in July 2023 and acquired Oort, an identity threat detection and response (ITDR) solution provider, in August 2023. These events did not meet the deadline for inclusion in Gartner's 2023 analysis of this vendor.

Cisco's flagship EPP product suits global organizations invested in the broader suite of Cisco security offerings looking to simplify integration, operations and procurement.

Strengths

- Cisco's product benefits from the broad workspace security suite, as its wide range of security products provide prospective clients with consolidation opportunities to reduce integration efforts and simplify operations.
- Cisco's product strategy benefits from integrating its flagship EPP product as a native module of Cisco Secure Client. Besides EPP, the unified agent provides additional capabilities such as VPN, SSE, network visibility and posture assessment.
- Cisco's sales strategy benefits from including its EPP product in wider enterprise agreements. Cisco's EPP prices are also generally lower than average for vendors in this Magic Quadrant.
- Cisco's product supports flexible on-premises EPP deployment options like air-gapped, connected stand-alone and connected proxy modes.

Cautions

- Cisco's market market responsiveness and track record are impacted by its small EPP market share and slow share growth relative to the vendor's overall security business. In 2023, a more detailed breakdown of market share was provided, resulting in a smaller reported EPP market share compared to 2022.
- As of the time of this writing, Cisco's product lacks advanced EDR capabilities such as mature raw endpoint telemetry collection, creation of custom detection rules, remote script execution and remote shell. It also does not include host firewall management.
- The vendor's innovation is held back by the generally slow pace of releasing new and innovative EPP capabilities and the re-establishment of its XDR strategy, lagging behind the Leaders in this

Magic Quadrant.

- Cisco's product requires multiple distinct administration consoles to operate a complete solution, creating a disorganized analyst workflow. The vendor recently released a new XDR solution; however, as of this writing, Gartner does not have sufficient client feedback on its ability to improve ease of use.

CrowdStrike

CrowdStrike is a Leader in this Magic Quadrant. CrowdStrike Falcon is the flagship EPP product, delivered as part of the cloud-native endpoint security platform and a unified security agent with add-on modules such as file integrity monitoring, cloud security, identity protection and others. In 2023, CrowdStrike focused its product strategy on further advancing its Falcon Insight XDR offering, which integrates events and detection logic across CrowdStrike's portfolio and an expanding list of third-party integrations via CrowdXDR Alliance. Recent partnerships include collaborating with Google to provide ChromeOS visibility and threat detection as part of CrowdStrike's XDR solution. The vendor now provides a Linux agent based on eBPF architecture, improving runtime visibility and protection and reducing performance impact across cloud and on-premises workloads. CrowdStrike also launched a new product bundle tailored to the needs of small and midsize businesses called Falcon Go.

CrowdStrike's flagship EPP product suits a broad range of organizations worldwide, especially those looking for cloud-delivered endpoint protection and MDR service augmentation.

Strengths

- CrowdStrike's strong market responsiveness and track record are due to its top market share and impressive growth rate. Gartner client interactions show evidence of a high degree of visibility for this vendor.
- CrowdStrike's product strategy benefits from its innovation in capabilities such as cloud security, attack surface management and ITDR, alongside advancements in XDR.
- The vendor's product benefits from the broad set of raw endpoint telemetry collected, mature and customizable EDR functionality, lightweight security agent, and app-store-like agent expansion capability.
- Its product also benefits from its vendor-managed MDR and threat-hunting services, addressing the needs of organizations with less mature security staff and expertise augmentation needs.

Cautions

- CrowdStrike's geographic strategy is challenged by generally lower market penetration in regions outside North America. The vendor's language support is limited to English and Japanese.

- The vendor's product lacks a comprehensive native workspace security suite compared to most other Leaders in this Magic Quadrant, despite having a broad ecosystem of integration partners.
- CrowdStrike's sales execution is impacted by generally higher-than-average prices and lower-than-average default endpoint telemetry retention compared to other vendors in this Magic Quadrant.
- CrowdStrike's product lacks hybrid and on-premises deployment options for its management console. CrowdStrike also has limited support for legacy OS compared to some of the other Leaders in this Magic Quadrant.

Cybereason

Cybereason is a Visionary in this Magic Quadrant. The Cybereason Defense Platform is the flagship EPP product that combines prevention, protection, detection, and response capabilities. In 2023, Cybereason's product strategy focused on further improving customers' operational efficiency through ease of use, expanding the portfolio of add-on capabilities such as endpoint in-memory protection and tightening integration with the Google security suite. Cybereason leads the market with MDR services delivered directly or through global channel partners. The product is available via cloud delivery or as an on-premises implementation.

Cybereason's flagship EPP product suits enterprises with either well-staffed security operations teams looking for deep EDR capabilities or midsize organizations looking for enterprise MDR service augmentation.

Strengths

- Cybereason's product has strong EDR functionality, particularly in terms of the real-time correlation of suspicious events into prioritized MalOps, improving ease of use and addressing alert fatigue.
- The vendor's product strategy benefits from consistent improvements to its threat detection capabilities. Recent enhancements include predictive ransomware protection, in-memory variant payload detection and behavioral document protection.
- Cybereason's product provides MSSP tenant management capabilities, including centralized endpoint, policy and alert management across multiple customer organizations.
- Cybereason's sales execution benefits from generally lower-than-average prices compared to other vendors in this Magic Quadrant.

Cautions

- Cybereason's market responsiveness and track record are impacted by low market share and a slowdown in market share growth.
- Cybereason's overall viability and operations assessments are impacted by its recent organizational structure and leadership changes. In addition to reductions in workforce that

figured into Gartner's 2022 analysis of this vendor, in the ensuing time period, recent changes in the executive leadership and additional investment from investor Softbank demonstrate an organization in transition. [1]

- The vendor's product lacks a comprehensive native workspace security suite compared to some other vendors in this Magic Quadrant, despite having an ecosystem of integration partners.

- Cybereason's product relies on its managed services to deliver and create custom XDR detection rules, which requires end users to interact with the services team instead of making changes directly to the Cybereason console.

ESET

ESET is a Niche Player in this Magic Quadrant. ESET PROTECT is the flagship EPP product combining prevention, protection, detection and response in a single management console available across cloud delivery, on-premises or air-gapped deployment methods. Product add-ons include endpoint encryption, multifactor authentication, email security and managed security services. In 2023, ESET launched its XDR offering, threat intelligence with premium APT reports, and a 180-day telemetry and detection event retention add-on for ESET's XDR solution.

ESET's flagship EPP product mostly suits small and midsize businesses in supported geographies prioritizing ease of use, protection efficacy, flexibility to deploy in the cloud or on-premises, and product language localization.

Strengths

- ESET's product benefits from its ease of use, generally low performance impact and high protection efficacy. Recent improvements include enhancements to the vendor's software-based detection technologies with Intel Threat Detection Technology to deliver better ransomware protection and efficacy on Intel-based PCs.

- The vendor's strong overall viability and operations are attributed to its consistent performance and 30-plus years of experience in the EPP space.

- ESET's product provides on-premises EPP support, including hybrid and air-gapped options, which may be required in high-security environments, critical infrastructure and organizations with strict data residency requirements.

- ESET's innovation manifests in tighter integration of its workspace security components, improving protection and ease of use for the vendor's existing clients and target buyers.

Cautions

- ESET's performance in the market responsiveness and track record evaluation criterion is impacted by the generally low levels of adoption of its cloud-delivered offering and the low attach rate of EDR capabilities.

- ESET's product EDR capability assessment indicates gaps in the recorded real-time raw endpoint telemetry. For example, driver modification and unload events, device mount and unmount events, and scheduled task events aren't recorded, despite the indirect investigative evidence available in the product.
- The vendor's product includes a custom detection rule builder that relies on text-heavy editing mechanisms and does not extend to telemetry collected outside the endpoint.
- ESET's product strategy is impacted by XDR capabilities that are currently restricted to the vendor's product portfolio and are evolving slower than average among the vendors in this Magic Quadrant.

Fortinet

Fortinet is a Niche Player in this Magic Quadrant. FortiEDR is the flagship EPP product, part of the FortiXDR platform, providing real-time visibility, protection, detection, automation and remediation across the Fortinet Security Fabric to detect and respond to attacks. In 2023, Fortinet's product strategy focused on integrating FortiEDR with its Fortinet Security Fabric to converge XDR, zero-trust network access (ZTNA) and SASE into a unified security mesh. Fortinet supports on-premises, cloud and hybrid deployment options for its EPP solution.

Fortinet's flagship EPP product suits enterprises and midsize organizations invested in the Fortinet technology ecosystem and looking to consolidate security vendors.

Strengths

- Fortinet's strong geographic and industry/vertical strategies are attributed to its dedicated resources in relevant industry verticals, a global market presence and an ongoing expansion of cloud hosting locations across different geographies.
- Fortinet's overall viability benefits from sustained financial performance, strength in adjacent cybersecurity markets and above-average relative share growth in the EPP market.
- Fortinet's sales strategy includes competitive displacement programs and dedicated sales resources for specific industry verticals. FortiEDR is attractive to organizations pursuing security vendor consolidation with Fortinet Security Fabric.
- Fortinet's product benefits from its on-premises deployment option, support for legacy OS and generally low endpoint performance impact.

Cautions

- Fortinet's performance in the market responsiveness and track record evaluation criterion is impacted by its low EPP market share. Despite accelerated relative share growth, the expansion is limited beyond existing Fortinet network security customers.

- Fortinet's EDR product capability assessment indicates that custom behavioral detection rules execute on a predefined query schedule, which could potentially result in delayed detection and response for custom rules.

- Fortinet's customer experience assessment reflects below-average ease of use based on analyst and end-user impressions of the console UX. The FortiEDR user interface requires a steep learning curve and expertise investments to operate despite the vendor's ongoing efforts to improve product usability.

- Fortinet's performance in the innovation evaluation criterion is impacted by a lack of prevention capabilities such as host firewall management and device control on non-Windows OSs and a lack of FortiEDR integration with FortiClient, the vendor's fabric agent. FortiXDR relies on data lake integrations such as FortiSIEM for detection customization, thus impacting end-user administration experience.

Microsoft

Microsoft is a Leader in this Magic Quadrant. Microsoft Defender for Endpoint is the flagship EPP product, available both stand-alone and as part of broader Microsoft bundles with varying sets of capabilities. In 2023, Microsoft launched its vendor-managed MDR service, called Microsoft Defender Experts for XDR, which includes alert triage, investigation, response and threat hunting. As of this writing, native Defender for Endpoint settings management remains in preview, providing the capability to manage security policies from the Microsoft 365 Defender management console, independent of Microsoft UEM.

Microsoft's flagship EPP product suits a wide range of organizations worldwide, especially those looking to consolidate security vendors and those with investments in the Microsoft technology ecosystem.

Strengths

- Microsoft's strong market responsiveness, track record and overall viability are attributed to its substantial market share and share growth in its security business. Gartner client interactions show evidence of a high degree of visibility for this vendor.

- Microsoft's strong product strategy and innovation are reflected in the breadth of its workspace security suite and the tight coupling with Microsoft Sentinel SIEM. Recent enhancements include automatic attack disruption capabilities for high-confidence incidents.

- Microsoft's product benefits from security configuration management capabilities, providing continuous posture assessment and recommended remediation suggestions to address vulnerabilities and misconfigurations.

- The vendor's product includes generous default endpoint telemetry and detection event retention that is higher than average among the vendors in this Magic Quadrant.

Cautions

- Microsoft's product is challenged by limited support for older OSs and generally uneven support across non-Windows OSs. Support for and performance on Linux-based systems are among Gartner clients' complaints.
- Microsoft's sales execution is impacted by a general focus on selling security bundles, which often creates shelfware and redundant spending, as reported by Gartner clients. In addition, products such as Microsoft Defender for Servers or Microsoft Sentinel SIEM are not fully represented in popular packages such as E3 or E5.
- Microsoft's customer experience assessment reflects below-average ease of use based on analyst and end-user impressions of the console UX and the current need to use separate dashboards for endpoint protection settings and security event management, despite the in-progress consolidation into a unified experience.
- Microsoft's product is impacted by a lack of on-premises deployment options for its EPP management console, making it unsuitable for organizations without a cloud-first strategy.

Palo Alto Networks

Palo Alto Networks is a Leader in this Magic Quadrant. Cortex XDR Pro is the flagship EPP product, integrating its endpoint protection with the vendor's workspace security portfolio and third-party integrations, including network, workload, cloud, identity and other security controls. In 2023, Palo Alto Networks' product strategy focused on simplifying the build-out of automation workflows, customizable incident risk scoring enhancements, and expansion and integration of its workspace security suite into Cortex XDR and Cortex XSIAM.

The vendor's flagship EPP product suits mature, well-staffed security operations teams, less mature security organizations looking for MDR service augmentation and clients pursuing security vendor consolidation opportunities.

Strengths

- Palo Alto Networks has a strong product strategy based on its growing workspace security suite and ongoing efforts to integrate these capabilities into Cortex XDR. Recent examples include the release of a new ITDR capability that expands the Cortex XDR offering.
- Palo Alto Networks' product benefits from high levels of customization, interoperability, automation and scoring logic tuning available through its administration console and often requested by mature security operations teams and MSSPs.
- The vendor's high overall viability assessment is attributed to its strength in adjacent cybersecurity markets, sustained financial performance and high relative share growth in the EPP market.

- Palo Alto Networks has a strong geographic strategy due to its global reach and multilingual product localization. The vendor supports more cloud hosting points of presence than average among the vendors included in this Magic Quadrant.

Cautions

- Palo Alto Networks' market responsiveness and track record are impacted by its market share, which remains significantly lower than that of the other Leaders in this Magic Quadrant, despite demonstrable progress over the past year.
- Palo Alto Networks' extensive functionality impacts its customer experience with a below-average ease of use based on analyst and end-user impressions of the console UX, highlighting the platform's steep learning curve.
- The vendor's product is impacted by its lack of fully on-premises or air-gapped deployment support, despite supporting hybrid use cases with the help of a Broker VM.
- Palo Alto Networks' sales execution is impacted by pricing that is higher than average among the vendors included in this Magic Quadrant.

SentinelOne

SentinelOne is a Leader in this Magic Quadrant. SentinelOne Singularity is the flagship EPP product, with three different software packages and multiple add-on modules, including deception, endpoint forensics, identity protection and others. The product can be deployed in cloud, hybrid or air-gapped network scenarios. In 2023, SentinelOne's product strategy focused on expanding the add-on portfolio to include attack surface management and gradually introducing new forensics capabilities called RemoteOps. The vendor is also in the process of unifying endpoint and identity protection agents and dashboards. SentinelOne has broadened its Marketplace XDR platform integrations to include endpoint, ticket and identity management.

SentinelOne's flagship EPP product suits a broad range of organizations worldwide, especially those prioritizing ease of use, comprehensive OS support and MDR service augmentation.

Strengths

- SentinelOne's strong market responsiveness and track record are attributed to above-average market share and share growth. Gartner client interactions show evidence of a high degree of visibility for this vendor.
- SentinelOne's product benefits from the intuitive design of its console UX combined with configuration granularity and customization, balancing ease of use and capability depth.
- SentinelOne's innovation manifests in the rapid pace of introducing new features, such as ITDR and Windows kernel real-time monitoring and protection.

- SentinelOne offers broad platform support, including for legacy systems such as Windows XP and Windows Server 2003. The vendor supports eBPF for numerous Linux families and introduced support for NetApp ONTAP in 2023.

Cautions

- SentinelOne's geographic strategy is impacted by limited language localization (English and Japanese only). The vendor demonstrates a smaller presence in regions outside of North America and Europe; however, new cloud hosting points of presence that are being introduced may broaden its appeal.
- The vendor's performance in the overall viability evaluation criterion is impacted by the challenging macroeconomic environment, which manifested in a small reduction in workforce. [2]
- SentinelOne's product lacks a comprehensive workspace security suite compared to other Leaders in this Magic Quadrant. The vendor relies on ecosystem integrations to cover the gaps in its portfolio.
- SentinelOne's product lacks managed security service support for the vendor's identity protection and extended detection and response products, despite supporting MDR for the endpoint.

Sophos

Sophos is a Leader in this Magic Quadrant. Sophos Intercept X is the flagship EPP product, with Sophos Central as the core administration platform enabling endpoint management, policy configuration, threat investigation and response across Sophos EPP and XDR solutions. Sophos' workspace security suite includes endpoint encryption and network, email and cloud security. The vendor has continued its focus on a protection-first strategy, enabling more robust default protections in standard deployments to improve ease of use. Sophos completed third-party integrations into Sophos XDR and MDR offerings in 2023, and launched an ecosystem of technology integrations, called Sophos Marketplace. Notably, Sophos extended MDR service coverage to Microsoft security solutions.

Sophos' flagship EPP product suits small and midsize businesses looking to consolidate multiple workspace and endpoint security capabilities, organizations looking for MDR service augmentation, and organizations with an existing Sophos investment.

Strengths

- Sophos has a strong market understanding due to the broad scope of its endpoint, workspace, networking and XDR offerings.
- Sophos' product benefits from recent improvements such as Active Adversary Protection, which dynamically enables heightened endpoint protection settings when a severe endpoint attack is detected.

- The vendor's product strategy benefits from the newly introduced Account Health Check tool, which helps continuously identify and remediate misconfigured Intercept X settings.

- Sophos' product benefits from MDR services supporting third-party integrations and includes incident response services as part of its higher-tier service package. In 2023, Sophos extended its MDR coverage to Microsoft security solutions.

Cautions

- Sophos' market responsiveness and track record assessment indicates the slow adoption of EDR capabilities in the vendor's installed base.

- Sophos' product lacks advanced EDR functionality, such as the ability to define granular custom detection rules, customize detection severity levels and assign MITRE ATT&CK classifications in the console. Sophos offers fewer built-in automated response actions for custom detection than other Leaders in this Magic Quadrant.

- Sophos' overall viability evaluation criterion performance is impacted by the challenging macroeconomic environment, which manifested in recent organizational structure changes and a small reduction in workforce. [3]

- Sophos' product is impacted by an evolving XDR capability that lacks a coherent analyst workflow for threat investigation and response, relying on cut-and-paste and navigation across multiple tabs for parts of the workflow. Sophos Factory, the part of the Sophos XDR offering used to create automation pipelines, is a separate interface from Sophos Central.

Trellix

Trellix is a Niche Player in this Magic Quadrant. The Trellix Endpoint Security suite includes Trellix Endpoint Security, Trellix Endpoint Detection and Response, Trellix Endpoint Forensics, and other capabilities such as application and device control. In 2023, Trellix focused its product strategy on combining the management capabilities for EPP, EDR and forensic capabilities into a single administration console, Trellix XConsole. Trellix has also recently announced new strategic MDR partnerships that augment its solutions with security monitoring and response capabilities.

The Trellix Endpoint Security suite fits enterprises with well-staffed security teams requiring a comprehensive set of endpoint protection capabilities with flexible deployment options, including cloud-delivery, hybrid and on-premises.

Strengths

- Trellix has a strong marketing strategy based on its renewed focus on XDR, integration strategy and customer security outcome-based promotional campaigns.

- Trellix's product benefits from custom prevention capabilities and a generally broad set of raw endpoint telemetry collected for investigation purposes. Recent improvements include the

expansion of behavioral detection coverage for privilege escalation, lateral movement, credential access and persistence.
- Trellix's above-average geographic strategy is attributed to its global presence, multilingual product localization and the broad availability of geographic points of presence.

- Trellix's product benefits from a broad range of security capabilities and add-ons, support for legacy systems, and a significant ecosystem of XDR integration partners.

Cautions
- Trellix's product strategy is held back by the current mix of endpoint protection products, which are not fully integrated and can confuse prospective buyers and complicate the purchasing process.

- Trellix's customer experience assessment indicates below-average ease of use based on analyst and end-user impressions of the console UX and a lack of fully integrated management capability. The vendor recently released XConsole; however, as of this writing, Gartner does not have sufficient client feedback on its ability to improve ease of use.

- Trellix's product is not built on a modern unified endpoint security agent architecture. The vendor deprioritized the integration of its EPP and EDR agents.

- Trellix's product lacks vendor-managed MDR services, despite offering other expert and staff augmentation services to assist with deployment optimization, and relies on a channel partner network to deliver MDR.

Trend Micro

Trend Micro is a Leader in this Magic Quadrant. Trend Vision One — Endpoint Security is the flagship EPP product, which can be combined with the vendor's extensive suite of network/IoT, email, cloud, identity and workload security products. It can also be combined with select third-party security tools integrated into Trend Vision One, the vendor's XDR and attack surface risk management (ASRM) platform. In 2023, Trend Micro's product strategy focused on blending attack surface management, security configuration management, identity protection and XDR capabilities into the Trend Vision One platform. Trend Micro acquired security operations center (SOC) technology provider Anlyz in February 2023, enhancing its MSSP console capabilities.

Trend Micro's flagship EPP product suits a broad range of organizations worldwide, including clients pursuing security vendor consolidation and looking for integrated workspace security capabilities, as well as organizations requiring support across cloud, hybrid and internet-restricted environments.

Strengths
- Trend Micro's innovation manifests in its integrated attack surface management, security configuration management and XDR capabilities in the Trend Vision One platform to aid in proactive risk reduction and security operations.

- Trend Micro's product benefits from the breadth and integration of its workspace security suite components. Recent enhancements include an integrated ITDR capability within the Trend Vision One platform.

- Trend Micro's sales execution benefits from its flexible credit-based licensing model and generally lower-than-average prices compared to other Leaders in this Magic Quadrant.

- Trend Micro's product offers depth and granularity in its administration console, and broad support for legacy and rare OSs. Trend Micro is one of the few vendors supporting flavors of IBM AIX, Oracle Solaris, Red Hat OpenShift and others.

Cautions

- Trend Micro's marketing execution is challenged by lower levels of brand recognition compared to other Leaders in this Magic Quadrant, particularly in North America, where the vendor has a comparatively smaller client base.

- Trend Micro's product has gaps in raw endpoint telemetry collected for the EDR functionality. Also, despite recent optimizations, its agent still consumes more disk space than average among the vendors included in this Magic Quadrant.

- Trend Micro's geographic strategy is impacted by generally lower market penetration in regions outside Europe and Japan. Recent marketing activities, partner programs and sales hiring may broaden its appeal in other geographies.

- Trend Micro's product lacks centralized configuration and policy management capabilities across multiple subtenants in its MSSP console, while providing centralized threat detection and response.

WithSecure

WithSecure is a Niche Player in this Magic Quadrant. WithSecure Elements Endpoint Protection is the flagship EPP product, incorporating software packages that include EDR functionality, application control, endpoint encryption management and enhanced ransomware protection with policy-based ringfencing for files and folders. WithSecure offers workspace security capabilities, such as email and collaboration protection for Microsoft Office 365, as well as vendor-managed MDR services. In 2023, WithSecure launched its Cloud Security Posture Management (CSPM) module in WithSecure Elements and a new Co-Monitoring Service for its Elements EDR component.

WithSecure's flagship EPP product mostly suits small and midsize businesses in supported geographies looking for ease of use, protection capability and MDR service augmentation.

Strengths

- WithSecure's market responsiveness and track record benefit from higher-than-average market share growth compared to other Niche Players in this Magic Quadrant.

- WithSecure's product strategy benefits from an on-demand incident escalation capability, called "Elevate to WithSecure," that is built into the management console, allowing clients to receive investigation support from the vendor's threat hunting team. The vendor has also recently introduced Co-Monitoring Service for EDR.

- WithSecure's product offers solid core endpoint protection capabilities, which were recently extended with endpoint encryption, dynamically adjustable security configurations reacting to heightened risk, ransomware rollback and patch management for macOS.

- WithSecure's product benefits from the vendor's investment in an EU-specific MDR service delivery mode, where the data is stored and accessible only from within the EU, making it attractive to customers in that geography.

Cautions

- WithSecure's product lacks a robust EDR capability, indicating gaps in the recorded raw endpoint telemetry collection and a lack of functionality to create custom detection rules and assign corresponding response actions.

- WithSecure's geographic and vertical/industry strategies lack a differentiated approach to addressing the needs of specific industry verticals and geographies. Most WithSecure clients are located in Europe, lacking a balanced global representation.

- WithSecure's product XDR capability is limited, only integrating with Microsoft 365 Email, Teams, OneDrive and SharePoint, and lacking in third-party integrations. WithSecure's overall security suite is limited to EPP, CSPM and Microsoft Office 365 protection.

- WithSecure's innovation is held back by a lack of seamless and complete EDR capability integration in its console UX compared to Visionaries 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

- No vendors were added to this Magic Quadrant.

Dropped

- Deep Instinct offers an endpoint protection product focused on security prevention through deep learning. However, it has been excluded from this Magic Quadrant due to not meeting Gartner's

updated EPP market definition for this year's research.

- BlackBerry (Cylance) offers its CylanceENDPOINT product, delivering endpoint protection capabilities and managed security services. However, it has been excluded from this Magic Quadrant due to not meeting Gartner's inclusion and exclusion criteria for this year's research.

Inclusion and Exclusion Criteria

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

Inclusion Criteria

To qualify for inclusion, vendors had to meet the definition of the EPP market and satisfy at least seven of the eight inclusion criteria using their flagship EPP product as of the start of Gartner's research and survey process (on 15 June 2023). Products and capabilities had to be generally available to be considered in the evaluation:

- The solution implements agent-based protection using multiple security techniques, such as static and behavioral analysis and attack surface reduction.
- The solution implements all its prevention, detection, and response functionality using a single agent installed on the endpoint.
- The solution can automatically invoke a native malware response action, such as deleting or quarantining files, blocking or killing processes, and isolating compromised endpoints.
- The solution provides a severity rating, a process tree, and a mapping of events and alerts to MITRE ATT&CK tactics, techniques and procedures to aid root cause analysis and remediation.
- The solution provides support for new versions of major operating systems, including Windows, macOS and Linux, within 90 days of the OS release.
- The solution provides a cloud-based, SaaS-style, multitenant security analytics and management infrastructure that is required to be maintained by the EPP vendor.
- The solution stores endpoint telemetry and detection events in its management infrastructure for at least 30 days, with the ability to extend or forward to other long-term storage.
- The solution natively integrates with vendor-owned or third-party security controls, such as identity protection, email security, security service edge and workload protection.

Exclusion Criteria

- A vendor would be excluded if it did not provide EPP software and licensing independently of other products or services in its portfolio.

- A vendor would be excluded if more than 60% of its detection content did not come from the vendor's own threat intelligence team and if the protection techniques are not designed, owned,and maintained by the vendor itself. Augmenting a solution with an OEM engine is acceptable, provided that the OEM or third-party agent/sensor is not the primary method of detection.

- A vendor would be excluded if it had not participated in at least two enterprise-focused, well-known public tests (for example, AV-TEST, AV-Comparatives, SE Labs, MRG Effitas and MITRE Engenuity) for accuracy and effectiveness within the 12 months before 1 March 2023. Participation in the VirusTotal public interface and other public tests will be considered if they are equivalent to those listed above.

- A vendor had to have more than 7.5 million endpoints protected and actively under management using its EPP as of 15 June 2023. Of these, more than 500,000 must have been active production installations with accounts larger than 500 seats. The proportion of enterprise customers in a single region outside North America or Europe must not have exceeded 60% of the total number. Vendors with less than the requisite number of seats in the relevant geographies defined above may not have qualified for inclusion in the main analysis of the Magic Quadrant and Critical Capabilities research.

- 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 were 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: This criterion assesses a vendor's core goods and services that compete in and or serve the defined market. It includes current product and service capabilities, quality, feature sets, skills, etc. These can be offered natively or through OEM agreements/partnerships as defined in the Market Definition/Description section and detailed in the subcriteria. Evaluation factors include product capabilities, the range and quality of add-on modules, and availability and scope of managed service offerings.

Overall Viability: This criterion assesses a vendor's overall financial health, as well as the financial and practical success of the business unit. It also looks at the likelihood of the organization to

continue to offer and invest in the product, as well as the product's position in the current portfolio. Evaluation factors include financial health, investments in the EPP product and EPPs' contribution to overall revenue growth.

Sales Execution/Pricing: This criterion addresses a vendor's capabilities in all presales activities and the structure that supports them. It includes deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel. Evaluation factors include execution of presales activities, packaging options, and the competitiveness of EPP product pricing.

Market Responsiveness/Record: This criterion assesses a vendor's ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. Also considered is the provider's history of responsiveness to changing market demands. Evaluation factors include general market responsiveness, market share and relative growth rate.

Marketing Execution: This criterion addresses the clarity, quality, creativity and efficacy of programs designed to deliver a vendor'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. This mind share can be driven by a combination of publicity, promotional activity, thought leadership, social media, referrals and sales activities. Evaluation factors include marketing activities and messaging, brand awareness and visibility, and publicly accessible and vendor-supplied new client logo wins.

Customer Experience: This criterion assesses a vendor's 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. It may also include ancillary tools, customer support programs, availability of user groups, service-level agreements, etc. Evaluation factors include customer relationship management, Gartner Peer Insights data and Gartner customer interactions.

Operations: This criterion addresses a vendor's ability to meet goals and commitments, including the quality of the organizational structure, skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently. Evaluation factors include resources dedicated to EPP product R&D and threat research, organizational structure, certifications and processes, and end-user training programs.

Table 1: Ability to Execute Evaluation Criteria

Evaluation Criteria ↓	*Weighting* ↓
Product or Service	High

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

Source: Gartner (December 2023)

Completeness of Vision

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

Market Understanding: This criterion addresses a vendor's ability to understand customer needs and translate them into products and services. It looks at whether a vendor shows a clear vision of its market — listens to and understands customer demands, and can shape or enhance market changes with its added vision. Evaluation factors include how vendors identify static and dynamic market trends and understand their buyers and competitors.

Marketing Strategy: This criterion assesses a vendor's ability to present clear, differentiated messaging consistently communicated internally, and externalized through social media, advertising, customer programs and positioning statements. Evaluation factors include marketing communications, use of media and the size of the marketing organization.

Sales Strategy: This criterion assesses a vendor's ability to offer a sound strategy for selling that uses the appropriate networks, including direct and indirect sales, marketing, service, and communication. It also looks at partners that extend the scope and depth of market reach, expertise, technologies, services and the customer base. Evaluation factors include deal strategies, sales programs, incentives, and sales organization.

Offering (Product) Strategy: This criterion looks at a vendor's ability to offer an approach to product development and delivery that emphasizes market differentiation, functionality, methodology and features as they map to current and future requirements. Evaluation factors include product development, execution against the roadmap over the past year and the future roadmap.

Vertical/Industry Strategy: This criterion assesses a vendor's strategy to direct resources (sales, product, development), skills and products to meet the specific needs of individual market segments, including verticals. Evaluation factors include performance in specific industries and strategies for vertical expansion.

Innovation: This criterion addresses a vendor's ability to offer direct, related, complementary and synergistic layouts of resources, expertise or capital, for investment, consolidation, defensive or preemptive purposes. Evaluation factors include differentiated technical and nontechnical innovations made in the last 18 months and past innovations older than 18 months.

Geographic Strategy: This criterion assesses a 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. Evaluation factors include vendor presence in international markets, geographic expansion strategies and product localization.

Table 2: Completeness of Vision Evaluation Criteria

Evaluation Criteria ↓	*Weighting* ↓
Market Understanding	High
Marketing Strategy	Medium
Sales Strategy	Low
Offering (Product) Strategy	High

Evaluation Criteria ↓	*Weighting* ↓
Business Model	NotRated
Vertical/Industry Strategy	Low
Innovation	Medium
Geographic Strategy	Low

Source: Gartner (December 2023)

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, tightly integrated workspace security capabilities; deep EDR functionality; and proven management capabilities for enterprise accounts. Increasingly, leaders provide vendor-managed MDR, ITDR and holistic XDR platforms that enable customers to consolidate their other tools and adopt a single-vendor solution. However, a Leader is not a default choice for every buyer. Clients should not assume that they must buy only from a Leader. Leaders may be less able to react quickly 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 adds up to a better Ability to Execute than Niche Players have. Challengers, however, are often late to introduce new capabilities, lack advanced functionality, or lack a fully converged product and service strategy. This affects their positions for the Completeness of Vision when compared with Leaders. Challengers are solid, efficient and practical choices.

Visionaries

Visionaries deliver leading-edge features that will be significant in the next generation of products, giving buyers early access to improved security and management. For example, Visionaries often have some of the following capabilities: identity threat detection and response, security configuration management, customizable vendor-managed service wrappers, converged workspace security capabilities, automated detection or response capabilities, advanced EDR features, 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 early access to innovative 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 geographic region or customer type. Others are Niche Players because they focus on excellence in a specific use case. Niche Players can be a good choice for existing customers, change-averse 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 a foundational aspect of basic security hygiene for all organizations. Although some use cases justify continuing with on-premises management, according to the Magic Quadrant vendor survey, 90% of organizations use cloud-delivered EPP solutions.

EDR is a required element of a mature endpoint security strategy and an integral component of EPPs; as such, it receives significant emphasis in this analysis. According to the Magic Quadrant vendor survey, roughly 57% of organizations have EDR capabilities deployed, which is a 15% increase since 2022. MDR adoption continues to grow rapidly, with increasing numbers of vendors delivering such services for their products. Approximately 17% of organizations subscribe to vendor-managed service wrappers to provide or augment their security operations functions.

The EPP market is no longer limited by vendors only offering EPP and EDR capabilities, and buyers are increasingly looking for fewer vendors to deliver a wider array of capabilities. [4] Email security, identity threat detection and response and XDR are increasingly part of the purchasing decision. This Magic Quadrant goes beyond evaluating a vendor’s ability to deliver core EPP/EDR products and services as organizations seek to consolidate into fewer vendors providing a more holistic approach to workspace security.

Market Overview

As attacker techniques evolve, endpoint protection providers are challenged to keep pace. Behavioral EDR capabilities are now standard; however, endpoint protection must be integrated with contextual information from the entire security infrastructure stack to address evolving threats. The increased complexity of EPP, EDR and now XDR solutions, combined with the cybersecurity skills gap, drives

increased demand for managed services. Concurrently, vendor consolidation efforts place increased emphasis on comprehensive workspace security solutions rather than point products. As a result, endpoint protection products are increasingly evaluated in the context of these broader security strategies.

In 2023, vendor innovation mainly focused on detection efficacy improvements, identity threat detection and response, security configuration management, and the broader set of integrated workspace security platform features. Most vendors in this research offer additional workspace security controls and XDR solutions that aid with security vendor consolidation efforts. However, the breadth and depth of those auxiliary controls, the quality of ecosystem integration, and the overall end-user experience differ between providers.

Vendors are also working to improve ease of use, advance the level of integration of their offerings and reduce the endpoint performance impact of their solutions to provide a more seamless administration experience. Some vendors cater their products to mature and fully staffed security operations teams, while others provide easier-to-use solutions with more contextual guidance and suggestions. Most vendors have now released their vendor-managed MDR services to aid end users in 24/7 monitoring, triage, investigation and response. Many vendors are also trialing or announcing generative-AI-guided investigation capabilities in 2023. However, as of this writing, they are not generally available and Gartner did not have sufficient feedback on their efficacy for evaluation in this research.

Endpoint protection market leaders continue to focus on evolving protection for modern infrastructure. Organizations that continue to secure legacy infrastructure or those requiring on-premises deployments due to data residency often struggle to find vendors that can still support air-gapped and architecturally constrained environments, offer on-premises deployment options, or support a broad spectrum of legacy OSs.

Broad market trends that are driving the adoption of EPP offerings include:

- **Cybersecurity platform consolidation:** Organizations want to reduce complexity, improve security posture and increase staff efficiencies. XDR solutions provide a unified incident response and hunting toolset that integrates event and alert data from multiple security products. ITDR and email security solution integrations are increasingly critical elements, as phishing and employee account takeover are involved in most breaches. Organizations also need prioritized configuration and hardening guidance to improve security posture by reducing misconfigurations across their security controls.

- **Vendor-managed service wrappers:** The most significant barrier to adopting EDR capabilities remains the availability of expertise and 24/7 coverage required to operate them effectively. Adoption of EDR must be accompanied by investment in personnel and training to be successful. To alleviate these gaps, MDR services that provide alert monitoring and triage are becoming much

more popular. According to the Magic Quadrant vendor survey, approximately 17% of organizations subscribe to managed services delivered by EPP solution providers directly, rather than through channel partners.

- **Ransomware and threat defense:** Ransomware remains the most significant threat to all organizations. Ransomware operators are shifting from relying solely on encryption to other forms of cyber extortion, including nonrecoverable data corruption, hardware corruption, data theft and data mining. In addition, most modern attacks exploit credential misuse and living-off-the-land techniques to bypass signature-based solutions, making robust behavioral protection, EDR and file restore capabilities mandatory for an EPP solution.

- **Remote working and cloud adoption:** Remote working has significantly accelerated the adoption of cloud-delivered offerings, which now represent 90% of the installed base, according to the Magic Quadrant vendor survey. Prospective buyers should look for indicators that solutions are truly designed for cloud-native delivery and do not represent management servers that were simply shifted to the cloud. Hybrid and on-premises deployments are less common and should only be considered by buyers with regulatory and data residency requirements, architecturally-constrained or air-gapped environments, or other restrictions making cloud adoption problematic.

Acronym Key and Glossary Terms

EPP	endpoint protection platform (a platform construct combining prevention, protection, detection, and response functionality)
EDR	endpoint detection and response (functionality used for the post-infection stages of an attack or exploit)
ITDR	identity threat detection and response (a security capability used for implementing detection mechanisms, investigating suspect posture changes and activities, and responding to attacks to restore the integrity of the identity infrastructure)
MDR	managed detection and response (managed services focused on monitoring, triage, investigation, and response to security incidents)
MSSP	managed security service provider
SIEM	security information and event management (gathers and analyzes logs from diverse types of systems)

SOAR	security orchestration, analytics and reporting (joins solutions with automation and orchestration workflows)
SOC	security operations center (or the team that works in it)
XDR	extended detection and response (a unified system combining telemetry and alerts 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 2,000 Gartner client inquiries since January 2023
- More than 4,500 Gartner Peer Insights reviews on gartner.com
- Vendor answers to a Magic Quadrant survey containing over 450 questions about product and service capabilities and enhancements through 2Q23, as well as 45-minute demonstrations by each vendor
- The 2022 Gartner CISO Security Vendor Consolidation XDR and SASE Trends Survey

[1] **From $3 Billion to $300 Million in One Year: Cybereason's Hard Landing**, CTech.

[2] **SentinelOne Cuts Annual Revenue Forecast, Laying Off Around 100 Employees**, CTech.

[3] **Sophos to Lay Off 450 Employees Globally**, TechCrunch.

[4] **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 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:* Results of this survey do not represent global

findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.

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.

research is produced independently by its research organization without input or influence from any third party. For further information, see "**Guiding Principles on Independence and Objectivity**." Gartner research may not be used as input into or for the training or development of generative artificial intelligence, machine learning, algorithms, software, or related technologies.