Magic Quadrant for Endpoint Protection Platforms

23 September 2024 - ID G00808300 - 44 min read

By Evgeny Mirolyubov, Franz Hinner, and 3 more

Learn how Gartner can help you succeed.

Become a Client

All solutions in this Magic Quadrant offer effective protection against most common attacks. Buyers should evaluate the included EPP vendors in the context of a comprehensive workspace security strategy and broader security operations modernization projects.

Strategic Planning Assumptions

By 2028, 30% of enterprises will adopt preventative endpoint security, endpoint detection and response, and identity threat detection and response from the same vendor, up from approximately 5% in 2024.

By 2029, 50% of organizations will evaluate endpoint protection platforms as part of a comprehensive workspace security strategy, up from approximately 20% in 2024.

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 endpoints — including desktop PCs, laptop PCs, mobile devices and, in some cases, server endpoints — against known and unknown malicious attacks. 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 consoles.

EPPs provide a defensive security control to protect end-user endpoints against known and unknown malware infections using a combination of security techniques (such as static and behavioral analysis) and system controls (such as device control and host firewall management). EPP prevention and protection 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.

Must-Have Capabilities

The must-have capabilities for this market include:

- 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 endpoint, application and end-user activity.

Standard Capabilities

The standard capabilities for this market include:

- Management and reporting of operating system security controls, such as host firewall, device control and endpoint encryption.
- Assessment of endpoints for vulnerabilities and risk reporting based on inventory, configuration, patch and policy of endpoint devices.
- Integrated endpoint detection and response (EDR) functionality enabling raw telemetry collection, detection customization, postincident investigation and remediation.
- Partner- and vendor-delivered service wrappers, such as managed detection and response (MDR) and co-managed security monitoring.

Optional Capabilities

The optional capabilities for this market include:

- Security configuration management capabilities enabling continuous assessment against configuration best practices.
- Workspace security integrations with email security, security service edge, identity protection and data security controls.
- Integrated extended detection and response (XDR) enabling telemetry collection, investigation, and remediation across multiple security controls.
- Patch management capabilities or activation of compensating security controls for unpatched vulnerabilities.
- Extended support for end-of-life, uncommon operating systems, or legacy server workloads.

Magic Quadrant

Figure 1: Magic Quadrant for Endpoint Protection Platforms

Vendor Strengths and Cautions

Bitdefender

Bitdefender is a Visionary in this Magic Quadrant. Bitdefender GravityZone is the flagship EPP product. In addition to the core EPP, Bitdefender offers email security and emerging human risk analysis, cloud security and extended detection and response (XDR) capabilities.

Bitdefender recently released unified incident management capabilities for its endpoint detection and response (EDR) and XDR alerts, extended security analysis to cloud and human identity risks, and integrated its mobile threat defense product into XDR. Bitdefender has also extended its patch management support to macOS. Bitdefender has also completed its acquisition of Horangi Cyber Security, extending its security technology and services portfolio, as well as its geographic reach in Southeast Asia.

Bitdefender's flagship EPP product is well-suited for small and midsize businesses that prioritize ease of use and protection efficacy, as well as those seeking managed detection and response (MDR) services augmentation. This vendor also caters to organizations looking for cloud-delivered, hybrid or on-premises (including air-gapped) deployment of EPP.

Strengths

- **Product strategy:** Bitdefender has a strong product roadmap that aligns with the requirements of its target small and midsize customers.
- **Customer experience:** Customers generally rate the support they receive from Bitdefender as good.
- **Sales execution:** Bitdefender's pricing is generally lower than average compared to other vendors in this Magic Quadrant.

Cautions

- **Market responsiveness and track record:** Bitdefender's share of the EPP market remains significantly lower than that of Leaders and Challengers in this Magic Quadrant.
- **Operations:** Bitdefender is a smaller company and its operations are less diversified when compared to the EPP market Leaders.
- **Overall viability:** Bitdefender is growing more slowly compared to the EPP market Leaders in this Magic Quadrant.

Broadcom

Broadcom is a Niche Player in this Magic Quadrant. Postacquisition of VMware, Broadcom offers two EPP products as part of its Enterprise Security Group — Symantec Endpoint Security (SES) Complete and Carbon Black Cloud EPP. In addition to the core EPP capabilities, Broadcom offers a broad suite of loosely integrated products across its security portfolio. Gartner expects rationalization in Broadcom's EPP product portfolio to occur due to overlaps in existing product capabilities.

Broadcom recently released multiple incremental enhancements to its EPP products. Symantec Endpoint Security Complete improved network integrity policy enforcement, role-based access controls for response actions, policy and exception management workflows, integration of mobile security with endpoint management tools. Carbon Black Cloud enhancements included design improvements to alert triage page, improved agent update status tracking, greater policy customization, a new version of the Splunk App, and enhanced endpoint telemetry collection.

Broadcom's EPP products are historically well-suited for large global enterprises that are familiar with the vendor's offerings, have the expertise to manage the solution in-house, and prefer enterprise agreements to simplify procurement. The vendor has recently publicly stated a shift in go-to-market strategy expanding its focus to mid-market and SMB segments through channel partners and distributors. This vendor also caters to organizations looking for cloud-delivered (including GovCloud), hybrid or on-premises (including air-gapped) deployment of EPP.

Broadcom did not respond to requests for supplemental information. Gartner's analysis is therefore based on other credible sources.

Strengths

- **Market understanding:** Broadcom has a good understanding of the EPP market and its competitors, with its historical focus on large global enterprises.
- **Vertical strategy:** Broadcom continues to offer a combination of cloud-delivered, hybrid and on-premises EPP deployments that appeals to certain industry verticals.
- **Sales strategy:** Broadcom has a focused sales strategy aligned with the vendor's objectives to sell into global large enterprises.

Cautions

- **Customer experience:** Customer feedback indicates that the technical support and account management they receive from Broadcom are variable, and the product may impact performance during scanning.
- **Product strategy:** Broadcom's recent, incremental enhancements to its EPP products are unlikely to shape the broader EPP market.
- **Market responsiveness and track record:** Broadcom's EPP market share growth is lower than that of market Leaders or Challengers in this Magic Quadrant.

Check Point Software Technologies

Check Point Software Technologies is a Visionary in this Magic Quadrant. Check Point Harmony Endpoint is the flagship EPP product. In addition to the core EPP, Check Point offers emerging XDR capabilities and a suite of integrated workspace security products.

Check Point recently released a browser-based data loss prevention (DLP) capability as part of Harmony Endpoint to improve data security controls, in addition to existing anti-phishing and URL filtering enabled by the browser extension. Check Point also added Domain Name System (DNS) inspection support as part of Harmony Endpoint and enhanced its offering with identity threat detection and response (ITDR) features. The vendor continued its work on reducing the footprint of the Harmony Endpoint agent. Check Point has also completed its acquisition of Perimeter 81, extending its reach in the security service edge (SSE) market.

Check Point's flagship EPP product caters to organizations that prioritize ease of use, prevention capabilities and the consolidation of the broader workspace security suite. This vendor also caters to organizations looking for cloud-delivered, hybrid or on-premises (including air-gapped) deployment of EPP.

Strengths

- **Market understanding:** Check Point has a good understanding of the EPP market direction, with a focus on workspace security consolidation.
- **Geographic strategy:** Check Point supports a higher-than-average number of geographic points of presence and languages compared to other vendors in this research.
- **Sales execution:** Check Point's pricing is generally lower than average compared to other vendors in this research.

Cautions

- **Market responsiveness and track record:** Check Point's share of the EPP market remains significantly lower than that of Leaders and Challengers in this Magic Quadrant.
- **Customer experience:** Harmony Endpoint consumes more resources compared to other vendors in this research, which may negatively impact system performance.
- **Overall viability:** Check Point is growing more slowly compared to the EPP market Leaders in this Magic Quadrant.

Cisco

Cisco is a Visionary in this Magic Quadrant. Cisco Secure Endpoint is the flagship EPP product. In addition to the core EPP, Cisco offers a broad suite of security products across its User Protection, Cloud Protection and Breach Protection suites.

Cisco recently released a generally available version of Cisco XDR, introduced a new remote scripts capability, added host firewall management features, and launched a common user experience (UX) design framework for its security products. Cisco is in the process of integrating Identity Intelligence (Oort acquisition) across its portfolio. Cisco has also completed its acquisition of Splunk, strengthening its competitive position in security operations and observability markets.

Cisco's flagship EPP product is well-suited for organizations invested in the suite of Cisco security tools, those seeking to simplify procurement, and those pursuing consolidation of workspace security capabilities. This vendor also caters to organizations looking for cloud-delivered, hybrid or on-premises (including air-gapped) deployment of EPP.

Strengths

- **Market understanding:** Cisco has a good understanding of the EPP market, with a focus on workspace security consolidation and security operations modernization.
- **Sales strategy:** Cisco's sales strategy benefits from the newly introduced User Protection suite, which combines EPP with other workspace security products, and the Breach Protection Suite, which combines EPP with XDR and other threat detection and response technologies.
- **Sales execution:** Cisco's pricing is generally lower than average compared to other vendors in this research, especially through purchasing programs, such as Enterprise Agreements.

Cautions

- **Market responsiveness and track record:** Cisco's share of the EPP market remains significantly lower than that of Leaders and Challengers in this Magic Quadrant.
- **Product:** Cisco still has distinct administration consoles for Secure Endpoint, Orbital and XDR products, which may hinder operational effectiveness using the product.
- **Overall viability:** Cisco Secure Endpoint is growing more slowly compared to the EPP market Leaders in this Magic Quadrant.

CrowdStrike

CrowdStrike is a Leader in this Magic Quadrant. CrowdStrike Falcon is the flagship EPP product. In addition to the core EPP, CrowdStrike offers a growing suite of integrated security products, including identity protection, cloud security, extended detection and response, among others.

CrowdStrike recently released its initial endpoint data protection offering. Additionally, the vendor has launched Falcon for IT solution for endpoint management, compliance and performance monitoring. CrowdStrike has also released Falcon NG-SIEM, enhancing the presentation of detections across its native product portfolio and third-party security controls. Falcon Flex is the new licensing model from the vendor. CrowdStrike has also completed its acquisitions of Bionic and Flow Security, strengthening its position in cloud and application security.

CrowdStrike's flagship EPP product is well-suited for a broad range of organizations worldwide, especially those looking to modernize security operations or augment MDR services. This vendor caters to organizations looking for cloud-delivered (including GovCloud), hybrid or on-premises (including air-gapped) deployment of EPP.

On 19 July 2024, CrowdStrike's content update for Falcon client caused an outage affecting millions of Windows systems in various businesses around the world. CrowdStrike responded promptly by pulling back the faulty update, supporting customer's recovery efforts, and announcing improvements to software resilience and testing. Gartner considered this incident in the CrowdStrike evaluation. Gartner has also provided further analysis of this incident and implications for CrowdStrike customers and prospects in research published outside of this comparative evaluation.

Strengths

- **Market responsiveness and track record:** CrowdStrike's share of the EPP market and its rate of consideration by EPP buyers are significant.
- **Customer experience:** Customers generally rate technical support, account management and managed security services from CrowdStrike as strong.
- **Product strategy:** CrowdStrike's product strategy and security roadmap is aligned with emerging customer requirements.

Cautions

- **Operations:** CrowdStrike's Channel File 291 incident on 19 July 2024 revealed limitations in the vendor's quality assurance and security content testing practices.
- **Sales execution:** CrowdStrike's pricing is higher than average compared to other vendors in this research, and its growing set of product SKUs is becoming increasingly complex.
- **Geographic strategy:** CrowdStrike supports a lower-than-average number of languages and an average number of geographic points of presence compared to other vendors in this research.

Cybereason

Cybereason is a Niche player in this Magic Quadrant. Cybereason Defense Platform is the flagship EPP product. In addition to the core EPP, Cybereason offers emerging XDR capabilities.

Cybereason recently enhanced its anti-tampering capabilities in the Windows agent to safeguard the agent software against unwanted modification. The vendor also improved EPP exclusion management by shifting all exclusion-related configuration items to a single unified page. Cybereason has improved agent compatibility for server deployments, allowing organizations to update minor agent versions without upgrading the server OS. Cybereason continues to pursue its SIEM Detection and Response (SDR) strategy by overlaying detection and response capabilities on top of existing enterprise data lakes.

Cybereason's flagship EPP product is well-suited for enterprises with well-staffed security operations teams looking for deep EDR capabilities, as well as midsize organizations looking for MDR service augmentation. This vendor also caters to organizations looking for cloud-delivered, hybrid or on-premises (including air-gapped) deployment of EPP.

Strengths

- **Market understanding:** Cybereason has a good understanding of the EPP market and its competitors, with a focus on serving midsize enterprises with MDR services.
- **Sales execution:** Cybereason's pricing is generally lower than average compared to other vendors in this Magic Quadrant.
- **Product:** Cybereason's EDR functionality is generally well-regarded by customers for its efficacy and usability.

Cautions

- **Product strategy:** Cybereason's recent and planned product developments, such as unified exclusions management and vulnerability management, are rolled out more slowly compared to market Leaders in this Magic Quadrant.
- **Innovation:** Cybereason's recent innovations, such as the new mobile security offering and improved agent compatibility for server deployments, are less likely to shape the broader EPP market.
- **Sales strategy:** Based on Gartner end-user client inquiries and Peer Insights customer feedback, Cybereason is rarely included on competitive EPP provider shortlists compared to market Leaders in this Magic Quadrant.

ESET

ESET is a Challenger in this Magic Quadrant. ESET PROTECT is the flagship EPP product. In addition to the core EPP, ESET offers email security, multifactor authentication, DNS and web content filtering, network file storage, and other security capabilities.

ESET recently released ESET Connect, a REST API gateway to open up its solution to third-party integrations. ESET has also enhanced its Cloud Office Security with additional support for Google Workspace, providing protection for Gmail and Google Drive against malware, phishing and business email compromise (BEC) attacks. The vendor introduced a new MDR service tailored to the needs of its small and medium businesses. ESET has also repackaged and enhanced support for mobile OS, such as Android and iOS, and enhanced its automated remediation and incident management capabilities.

ESET's flagship EPP product is well-suited for small and midsize organizations in supported geographies, particularly those prioritizing ease of use and prevention efficacy. This vendor also caters to organizations looking for cloud-delivered, hybrid or on-premises (including air-gapped) deployment of EPP.

Strengths

- **Overall viability:** ESET has a long history and consistent revenue growth in the EPP market.
- **Customer experience:** Customers generally rate the support they receive from ESET as good.
- **Vertical strategy:** ESET has a well-diversified base of customers across most industry verticals and demonstrates a good understanding of unique vertical requirements.

Cautions

- **Product strategy:** ESET's planned and recently added product enhancements, such as mobile device support and ESET Connect, are less likely to shape the broader EPP market.
- **Sales strategy:** Based on Gartner end-user client inquiries and Peer Insights customer feedback, ESET is rarely included on competitive EPP provider shortlists compared to market Leaders in this Magic Quadrant.
- **Market understanding:** ESET's market understanding is focused on the needs of its small and midsize customers rather than the broader EPP market.

Fortinet

Fortinet is a Niche Player in this Magic Quadrant. FortiEDR is the flagship EPP product. In addition to the core EPP, Fortinet offers a broad suite of integrated products across its security portfolio.

Fortinet recently released incremental improvements to FortiEDR's user interface (UI), integrated FortiEDR with FortiClient into a unified security agent for protection and remote access, and improved vulnerability prioritization in its product. Fortinet has also released host firewall management and full disk encryption features, as well as introduced support for mobile OS, such as Android and iOS. Fortinet continues to pursue ease-of-use improvements and feature parity across non-Windows OS.

Fortinet's flagship EPP product is well-suited for organizations invested in the broader suite of Fortinet security offerings, as well as those seeking MDR services augmentation. This vendor also caters to organizations looking for cloud-delivered, hybrid or on-premises (excluding air-gapped) deployment of EPP.

Strengths

- **Geographic strategy:** Fortinet supports a higher-than-average number of geographic points of presence compared to other vendors in this research.
- **Sales execution:** Fortinet's pricing is generally lower than average compared to other vendors in this Magic Quadrant.
- **Overall viability:** Fortinet's revenue growth in the EPP market is higher than that of other Niche Players.

Cautions

- **Market responsiveness and track record:** Fortinet's share of the EPP market remains significantly lower than that of market Leaders and Challengers in this Magic Quadrant.
- **Product strategy:** Fortinet's recent and planned product enhancements, such as improved UI, feature parity across non-Windows OS, appear to focus on closing technical gaps rather than driving innovation.
- **Innovation:** Fortinet's recent innovations, such as FortiRecon integration with FortiEDR for common vulnerability and exposure (CVE) prioritization and mobile security, are less likely to shape the broader enterprise EPP market.

Microsoft

Microsoft is a Leader in this Magic Quadrant. Microsoft Defender for Endpoint is the flagship EPP product. In addition to the core EPP, Microsoft offers a broad suite of security products across various product bundles.

Microsoft recently consolidated Defender XDR with Microsoft Sentinel, unifying the user experience across these security operations tools. Microsoft has also released settings management capabilities directly in its EPP product, reducing administration dependency on Microsoft Intune. The vendor released an Extended Berkeley Packet Filter (eBPF) version of its Linux agent in an attempt to improve manageability, resource utilization and protection efficacy on Linux OS. Microsoft is also in the process of unifying its endpoint agents to simplify the deployment experience and operations.

Microsoft's flagship EPP product is well-suited for a wide range of organizations worldwide, especially those invested in the Microsoft technology ecosystem and those pursuing security vendor consolidation. This vendor caters to organizations seeking cloud-delivered (including GovCloud) deployment of EPP.

On 12 January 2024, the Microsoft security team detected an attack on its corporate systems. Microsoft responded promptly by activating its internal response procedures and mitigating the impact of the incident. The vendor incorporated lessons from the incident into its Secure Future Initiative (SFI), which had launched in November 2023. Gartner has provided further analysis of this incident and implications for Microsoft customers and prospects in research published outside of this comparative evaluation.

Strengths

- **Market responsiveness and track record:** Microsoft's share of the EPP market and rate of consideration by EPP buyers are significant.
- **Product strategy:** Microsoft's product strategy and security roadmap are aligned with emerging customer requirements around consolidating security operations.
- **Sales strategy:** Microsoft has an effective sales strategy and a large, established customer base that presents opportunities to continue expanding its EPP product reach.

Cautions

- **Customer experience:** Indications from customers are that the technical support and account management support they receive from Microsoft is variable.
- **Sales execution:** Customers report that Microsoft's licensing model is complex and difficult to understand.
- **Vertical strategy:** Microsoft offers limited industry-specific product packaging, pricing or discounting options, and does not support on-premises EPP deployments.

Palo Alto Networks

Palo Alto Networks is a Leader in this Magic Quadrant. Cortex XDR is the flagship EPP product. In addition to the core EPP, Palo Alto Networks offers a broad suite of integrated security products across network security, cloud security and security operations.

Palo Alto Networks recently introduced a unified endpoint agent that combines its cloud workload protection platform (CWPP) solution and EDR, and improved forensics capabilities in its XDR platform. The vendor also added advanced security modules to enhance its protection capabilities, which include unified extensible firmware interface (UEFI) protection against preboot attacks and on-write protection for Windows. Palo Alto Networks has also completed its acquisition of Talon, an enterprise browser company, to strengthen its secure access service edge (SASE) offering.

Palo Alto Networks' flagship EPP product is well-suited for mature, well-staffed security operations teams, less mature security organizations seeking MDR service augmentation, and those pursuing security vendor consolidation. This vendor caters to organizations looking for cloud-delivered EPP deployment, including on GovCloud.

Strengths

- **Sales strategy:** Palo Alto Networks has an effective sales strategy and a large, established customer base, presenting opportunities to continue expanding its EPP product reach.
- **Customer experience:** Customers generally rate technical support, account management and managed security services from Palo Alto Networks as strong.
- **Market responsiveness and track record:** Palo Alto Networks has been rapidly acquiring a bigger share in the EPP market in the past year.

Cautions

- **Sales execution:** Palo Alto Networks' pricing is higher than average compared to other vendors in this research.
- **Product:** Palo Alto Networks' product customization requires a steep learning curve and may be less suitable for lean security teams and those pursuing ease of use.
- **Vertical strategy:** Palo Alto Networks does not publicly offer industry-specific product packaging, pricing or discounting options.

SentinelOne

SentinelOne is a Leader in this Magic Quadrant. SentinelOne Singularity is the flagship EPP product. In addition to the core EPP, SentinelOne offers integrated identity protection, cloud security, extended detection and response, and other security products.

SentinelOne recently released Singularity Operations Center, unifying security alert management across detections from native and third-party security controls. The vendor has also enhanced its vulnerability assessment and prioritization capabilities, introducing asset inventory, assessment of third-party and OS vulnerabilities, and asset graph views to identify and address managed and unmanaged assets. SentinelOne has also completed its acquisition of Krebs Stamos Group (KSG) and PingSafe, strengthening its advisory services and cloud security capabilities, respectively.

SentinelOne's flagship EPP product is well-suited for a broad range of organizations worldwide, especially those seeking ease of use, broad OS support and MDR service augmentation. This vendor caters to organizations looking for cloud-delivered (including GovCloud), hybrid or on-premises (including air-gapped) deployment of EPP.

Strengths

- **Market responsiveness and track record:** SentinelOne's share of the EPP market and its rate of consideration by EPP buyers are significant.
- **Product strategy:** SentinelOne's product strategy and security roadmap are aligned with emerging customer requirements.
- **Customer experience:** Customers generally rate technical support, account management and managed security services from SentinelOne as strong.

Cautions

- **Sales execution:** SentinelOne's pricing is higher than average compared to other vendors in this research.
- **Geographic strategy:** SentinelOne supports a lower-than-average number of languages and an average number of geographic points of presence compared to other vendors in this research.
- **Sales strategy:** SentinelOne's sales strategy is yet to result in significant market share and market visibility in product categories adjacent to the vendor's core EPP solution.

Sophos

Sophos is a Leader in this Magic Quadrant. Sophos Intercept X Endpoint is the flagship EPP product. In addition to the core EPP, Sophos offers emerging XDR capabilities and a suite of integrated workspace security products.

Sophos recently released a new Critical Attack Warning capability that delivers urgent notifications to customers when an active, persistent threat is detected in their environment. The vendor has also enhanced its Adaptive Attack Protection feature, enabling the exemption of specific device groups from dynamic policy changes and adding additional response capabilities. Sophos continues to strengthen its workspace security suite through agent integration across endpoint protection and secure access. The vendor continued its work on reducing the footprint of its endpoint agent. Sophos has also launched new partnerships with Tenable and Veeam focused on exposure management, and backup and recovery, respectively.

Sophos' flagship EPP product is well-suited for small and midsize businesses prioritizing ease of use, organizations seeking to consolidate workspace security capabilities, and those seeking for MDR services augmentation. This vendor caters to organizations seeking for cloud-delivered deployment of EPP.

Strengths

- **Product strategy:** Sophos' recent product enhancements, such as Adaptive Attack Protection, focus on serving resource-constrained customers with prevention-focused features and MDR services, and its product roadmap is aligned with the needs of its target customers.
- **Sales strategy:** Sophos has been effective at selling its EPP product bundled with MDR services to small and midsize organizations with managed services augmentation needs.
- **Overall viability:** Sophos has a long history and consistent revenue growth in the EPP market.

Cautions

- **Product:** Sophos Intercept X Endpoint offers fewer product customization options compared to other Leaders in this Magic Quadrant.
- **Vertical strategy:** Sophos' market penetration is skewed toward the services industry, and the vendor does not support the on-premises EPP deployments required by some verticals.
- **Customer experience:** Indications from customers are that the technical support they receive from Sophos is variable, and the product may impact performance during scanning.

Trellix

Trellix is a Challenger in this Magic Quadrant. Trellix Endpoint Security Suite is the flagship EPP product. In addition to the core EPP, Trellix offers a broad suite of integrated products across its security portfolio.

Trellix continues to focus on product and UX unification efforts by integrating EPP, EDR, XDR, and now Forensics with Trellix XConsole. The vendor has also enhanced its endpoint agent deployment experience by offering a unified installer and package manager across its endpoint application portfolio. Trellix is pursuing the addition of exposure management and security configuration management capabilities to help customers assess and optimize the configuration of their EPP deployments. The vendor has launched Trellix Thrive to extend its customer success service offerings.

Trellix flagship EPP product is well-suited for enterprises with well-staffed security teams that require a comprehensive set of endpoint protection capabilities and customization options. This vendor caters to organizations seeking cloud-delivered (including GovCloud), hybrid or on-premises (including air-gapped) deployment of EPP.

Strengths

- **Market responsiveness and track record:** Trellix's share of the EPP market is significantly higher than that of Niche Players and Visionaries.
- **Operations:** Trellix has continued to grow its employee headcount despite the challenging economic environment.
- **Geographic strategy:** Trellix has a global presence of technical and sales resources and supports a higher-than-average number of languages in its administration console compared to other vendors in this research.

Cautions

- **Product strategy:** Trellix's recent product enhancements, such as unification of EDR with Forensics, XConsole integration and product roadmap items evaluated for this Magic Quadrant, are less likely to shape the broader EPP market.
- **Sales strategy:** Based on Gartner end-user client inquiries and Peer Insights customer feedback, Trellix Endpoint Security Suite is included on competitive EPP provider shortlists less frequently if compared to Leaders in this Magic Quadrant.
- **Product:** Trellix administration consoles are loosely integrated, providing only moderate improvements to ease-of-product use over the prior product versions.

Trend Micro

Trend Micro is a Leader in this Magic Quadrant. Trend Vision One — Endpoint Security is the flagship EPP product. In addition to the core EPP, Trend Micro offers a broad suite of integrated workspace security products, including email, security service edge and others.

Trend Micro continues to enhance its single console experience and capabilities, ranging from attack surface management and security configuration management to extended detection and response. Trend Micro also improved vulnerability prioritization with attribution of actively exploited CVEs. The vendor continued its ongoing agent optimization efforts, extended OS support and added new forensics capabilities. Trend Micro released improvements to its identity threat detection and response capability set, helping assess security posture of identity systems and broker automated mitigation and response actions.

Trend Micro's flagship EPP product is well-suited for a broad range of organizations worldwide, especially those pursuing consolidation of the broader workspace security suite and looking for broad OS support. This vendor caters to organizations looking for cloud-delivered, hybrid or on-premises (including air-gapped) deployment of EPP.

Strengths

- **Market understanding:** Trend Micro demonstrates a strong understanding of EPP market competitors and market direction with a focus on comprehensive workspace security.
- **Product strategy:** Trend Micro has a product roadmap that is aligned with emerging EPP market requirements.
- **Overall viability:** Trend Micro has a long history and consistent revenue growth in the EPP market.

Cautions

- **Sales strategy:** Based on Gartner end-user client inquiries and Peer Insights customer feedback, Trend Micro appears on competitive EPP provider shortlists less frequently than other market Leaders in this Magic Quadrant.
- **Sales execution:** Trend Micro's sales execution lags behind other market Leaders, with comparatively slower revenue growth in the EPP space.
- **Geographic strategy:** Trend Micro's market penetration outside Europe and Japan is limited compared to other Leaders in this Magic Quadrant.

WithSecure

WithSecure is a Niche Player in this Magic Quadrant. WithSecure Elements Endpoint Security is the flagship EPP product. In addition to the core EPP, WithSecure offers email and collaboration protection, cloud security and emerging XDR, and exposure management capabilities.

WithSecure recently released the first iteration of its ITDR capabilities as part of Elements XDR solution. WithSecure has also released outbreak control functionality that can dynamically adjust security policy settings based on the changing risk score of the endpoint device and its location. The vendor has also expanded its Broad Context Detections, enhancing alert management across its security portfolio, and enhanced Elements API, opening up the product to more prebuilt third-party integrations.

WithSecure's flagship EPP product is well-suited for small and midsize businesses in supported geographies, those prioritizing ease of use and seeking MDR services augmentation. This vendor caters to organizations looking for cloud-delivered or on-premises (including air-gapped) deployment of EPP.

Strengths

- **Sales execution:** WithSecure's pricing is generally lower than average compared to other vendors in this Magic Quadrant.
- **Customer experience:** Customers generally rate the support they receive from WithSecure as good.
- **Market understanding:** WithSecure demonstrates a good understanding of the EPP market and its target buyers with EU-specific MDR service localization.

Cautions

- **Market responsiveness and track record:** WithSecure's share of the EPP market remains significantly lower than that of Leaders and Challengers in this Magic Quadrant.
- **Sales strategy:** Based on Gartner end-user client inquiries and Peer Insights customer feedback, WithSecure appears on competitive EPP provider shortlists less frequently than market Leaders in this Magic Quadrant.
- **Geographic strategy:** In our assessment, WithSecure's geographic strategy lags behind competitors, and most of the vendor's customers are in Europe.

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

- Broadcom (VMware) and its Carbon Black Cloud EPP product is now analyzed under the combined Broadcom vendor name.

Inclusion and Exclusion Criteria

Magic Quadrant and Critical Capabilities research identify and analyze 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. Gartner did not define any exclusion criteria for this research.

To qualify for inclusion, providers had to meet the definition of the EPP market and satisfy all of the inclusion criteria using their flagship EPP product as of the start of Gartner's research and survey process (on 29 April 2024). Products and capabilities had to be generally available to be considered in the evaluation. Requirements included:

- The solution supports Windows, macOS and Linux operating systems.
- The solution combines all security prevention, protection, detection and response functionality in a single agent.
- The solution enforces agent-based protection using a combination of security techniques, such as static and behavioral analysis, and system controls, such as device control and host firewall management.
- The solution includes built-in endpoint detection and response functionality, enabling collection of raw, real-time endpoint telemetry, detection customization, postincident investigation and response.
- 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 a cloud-based, SaaS-style, multitenant security analytics and management infrastructure that the EPP vendor maintains.
- The solution offers tight coupling with partner- or vendor-delivered service wrappers, such as managed detection and response or co-managed security monitoring.
- A vendor must sell EPP software and licensing independently of other products or services.
- A vendor must design, own and maintain most of its detection content and threat intelligence in-house. OEM augmentation is acceptable if the OEM is not the primary protection method.
- A vendor must have participated in at least two enterprise-focused, well-known public tests (for example, MITRE Engenuity, AV-Comparatives, AV-TEST, SE Labs and MRG Effitas) for detection efficacy within 12 months before 1 April 2024.
- A vendor must have over 7.5 million licensed endpoints protected and actively under management using its EPP as of 29 April 2024. More than 500,000 must be 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 exceed 60% of the total number.

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 core product and service capabilities, the depth and breadth of functionality, and the availability of security add-ons.

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 overall financial health and EPP's contribution to 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 the execution of presales activities, the competitiveness of product and service pricing, and Gartner end-user client proposal reviews.

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 responsiveness to endpoint protection market trends, market share and relative share growth rate.

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 and Gartner client 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 development, certifications, internal security and end-user training programs.

Table 1: Ability to Execute Evaluation Criteria

Enlarge Table

Evaluation Criteria	*Weighting*
Product or Service	High
Overall Viability	Medium
Sales Execution/Pricing	Medium
Market Responsiveness/Record	High
Marketing Execution	NotRated
Customer Experience	High
Operations	Medium

Source: Gartner (September 2024)

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 endpoint protection market trends and understand their buyers and competitors.

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 the attractiveness of product licensing and packaging options, deal strategies, vendor-supplied new client logo wins, and Gartner end-user client interactions and consideration rates.

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 differentiated product functionality, execution against the roadmap over the past year and 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 12 months and past innovations older than 12 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 performance in international markets, product localization and geographic expansion strategies.

Table 2: Completeness of Vision Evaluation Criteria

Enlarge Table

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

Source: Gartner (September 2024)

Quadrant Descriptions

Leaders

Leaders demonstrate balanced and consistent progress in relation to all Ability to Execute and Completeness of Vision criteria. They offer broad, tightly integrated workspace security capabilities, deep EDR functionality, vendor-delivered service wrappers (such as MDR), and proven management capabilities for enterprise customers. Increasingly, leaders provide holistic XDR platforms that enable customers to consolidate or converge their security tools and incident management capabilities. Leaders have a strong momentum in the market in terms of sales and mind share. However, a Leader is not a default choice for every buyer. Customers 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 mature endpoint protection products that can address the security needs of the market. They also have strong sales and visibility in the market, which adds up to a better Ability to Execute than Niche Players have. Challengers, however, are often late to introduce new and emerging capabilities, lack advanced functionality and customization, lack ease of product use, lack a tightly integrated product and service strategy. Challengers may lack alignment with the market's direction. This affects their positions for the Completeness of Vision when compared with Leaders. Challengers are solid, efficient and practical choices, especially for customers that have established strategic relationships with them.

Visionaries

Visionaries deliver leading-edge capabilities that will be significant in the next generation of solutions, giving buyers early access to improved security and management. For example, Visionaries often have some of the following capabilities: extended detection and response, identity threat detection and response, workspace security capabilities, security configuration management, vendor-delivered service wrappers, advanced EDR features, data security, and generative AI (GenAI) capabilities. Visionaries can affect the course of technological developments in the market but may not yet demonstrate a consistent track record of execution, may lack visibility in the market, and often lack market share. Customers 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 capabilities. Some vendors are Niche Players because they focus on a specific geographic region or specific market segment. Others are Niche Players because they excel in a specific use case, industry or a specific technical capability set. Niche Players can be a good choice for existing customers, customers in the vendor's target market segment, change-averse organizations in supported regions, or organizations looking to augment their existing EPP for a defense-in-depth approach.

Context

EPPs focus on securing end-user endpoints (laptops, workstations, mobile) through a mix of prevention, protection, detection and response capabilities delivered via a single agent. Increasingly, vendors offer EPPs as part of security operations platforms, such as XDR and security information and event management (SIEM), enabling the path for modernizing security operations. At the same time, vendors increasingly bundle and integrate EPPs as part of their broader workspace security product portfolios focused on securing modern hybrid work.

According to Gartner Magic Quadrant vendor surveys and client inquiries, the growth in adoption of cloud-delivered EPP solutions and EDR capabilities has flattened out, with only a moderate increase in adoption compared to the previous year's research. However, interest in tightly integrated XDR and ITDR capabilities is increasing, with an estimated adoption rate of 14% and 9% (as of May 2024) among EPP buyers, respectively. Despite the wave of announcements and general availability of GenAI assistants and incident summarization capabilities, most organizations remain cautious, with limited interest from Gartner's EPP customers.

EPP customers increasingly contemplate the benefits and drawbacks of acquiring multiple security products and services from the same vendor. Vulnerability and exposure management, identity threat detection and response, email security, cloud workload protection, extended detection and response, and managed detection and response are increasingly part of the purchase decision. Therefore, this Magic Quadrant goes beyond evaluating a vendor's ability to deliver core EPP products to assist buyers looking to achieve a holistic approach to workspace security and security operations modernization.

Market Overview

Product Evolution

Despite the maturity of the EPP market, there are no perfect solutions. The year 2024 illustrates that even the most sophisticated solution providers are subjected to unpredictable events. No vendor is completely immune. Therefore, organizations must prepare for the possibilities of major disruption by focusing on resilience as with any other third-party risk.

Since the last report, most vendors have only made incremental changes to their EPP products. Most vendors have fully integrated prevention, protection, detection and response capabilities into a unified EPP solution configured and operated from a single console and enabled with a single unified endpoint agent. However, buyers should be wary of vendors relying on multiple consoles for various functions or requiring multiple endpoint applications, even if tied together via single sign-on (SSO) or deployed using centralized agent deployment mechanisms.

In 2024, vendors made incremental improvements to user experience and administration capabilities, enhancing the overall ease of product use. Most vendors released embedded GenAI capabilities or AI assistants that aim to improve incident explainability, provide onboarding and configuration guidance, and support security teams with detection engineering, threat hunting queries and response script creation. Most vendors refrain from claiming full security policy, configuration or alert management automation. Despite vendors' progress with generative AI, the adoption of GenAI capabilities among EPP customers remains low.

Additional focus areas for EPP vendors included enhanced asset, vulnerability and exposure management capabilities. Several vendors are pursuing improvements to feature parity and product quality of non-Windows OS, such as macOS, and Linux. Additionally, we've seen a renewed focus of EPP providers on endpoint forensics, endpoint data loss prevention and streamlined security configuration management.

Enterprise Integration

Enterprise integration continues in areas such as XDR and workspace security. Several vendors released unified incident management capabilities as part of their XDR solutions to help correlate alerts from native and third-party security controls into a single incident view. Most vendors have also fully collapsed their EPP and XDR offerings into a single console UX. However, buyers should be aware of those still offering EPP and XDR as two separate products with distinct consoles, configurations and alert views, even if the products are integrated via SSO and APIs. ITDR and email security integrations into XDR are increasingly critical, as the use of stolen credentials and phishing are involved in most breaches.

Hybrid work drives the need for comprehensive workspace security strategies that integrate security across device, identity, email, data and application access into cohesive, modular solutions. Several broad portfolio security providers continue their unification efforts to bring together EPP with SSE and DLP agents. Examples of integrations between EPP and SSE tools include endpoint posture assessment for conditional access, common administration dashboards with reusable policy elements, security alert correlation, custom detection logic creation and dynamic secure access policy enforcement. Email security benefits from integrating user identity data that helps gauge user risk, identify signs of account takeover and initiative mitigation actions. Additionally, several vendors now offer a bundle of security products under a single SKU tailored to secure the hybrid workspace. Small and midsize organizations often prefer such single-vendor workspace security offerings.

Vendor Differentiation

Vendors in this market display various maturity levels regarding the breadth and depth of their prevention and protection functionality, detection and response capabilities, forensics features, data security, security configuration management, and OS support. While all vendors attempt to optimize their endpoint agents for minimal system performance impact, there's a significant differentiation in the resource consumption of different tools. Additionally, the quality and depth of ecosystem integration and support for various on-premises deployment scenarios differ.

Capabilities such as behavioral analysis, host firewall management and device control are common among most providers, and therefore, are not seen as differentiating by most Gartner customers. Built-in vulnerability, exposure management and patching are present in an increasing number of products. Some vendors cater their products to mature and fully staffed security teams, while others provide easier-to-use solutions with fewer customization options and more contextual guidance. Most vendors offer partner- and vendor-delivered service wrappers, such as MDR, to aid end users in 24/7 monitoring, triage, investigation and response.

Market Drivers

Broad market trends driving the adoption of EPP offerings include:

- **Consolidation:** Organizations need to manage complexity and increase the effectiveness of their limited security staff. Complex infrastructure security stacks lead to complexity of security configuration management and security control gaps that may expose organizations to threats. Security platforms, which provide a modular set of integrated security product capabilities, are becoming increasingly available to fill these needs. See Innovation Insight for Security Platforms and Simplify Cybersecurity with a Platform Consolidation Framework.
- **Hybrid work:** Endpoint protection tools only address part of the issues in securing hybrid workers, focusing on protecting managed endpoints from malware attacks. Identity theft, phishing and data exfiltration are workspace security risks that require further attention. To address these issues, organizations need a holistic workspace security strategy that places the worker at the center of protection and integrates security across device, email, identity, data and application access controls. See Securing Hybrid Work: Adopting the Right Workspace Security Strategy and Hype Cycle for Endpoint and Workspace Security, 2024.
- **Security operations:** The availability and expertise of security teams, coupled with the need for 24/7 coverage, remain the most significant barriers to success in security operations. Modern proactive exposure management and reactive incident management technologies, alongside investment in personnel and training, enable more organizations to modernize their security operations. For less mature organizations, MDR services provide customers with remotely delivered, human-led, turnkey, modern security operations center (SOC) functions. See Market Guide for Managed Detection and Response.

Evidence

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

- More than 2,000 Gartner client inquiries since January 2024.
- More than 4,000 Gartner Peer Insights reviews on gartner.com.
- Vendor responses to a Magic Quadrant survey, with over 230 questions about product and service and enhancements through 2Q24 as well as 60-minute live product demos by each vendor.

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.

© 2024 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by Gartner's Usage Policy. Gartner prides itself on its reputation for independence and objectivity. Its 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.