Gartner. Licensed for Distribution

Magic Quadrant for Endpoint Protection Platforms

14 July 2025 - ID G00823512 - 45 min read

By Evgeny Mirolyubov, Deepak Mishra, and 1 more

Customer experience and vendor trust are key drivers for provider selection due to the maturity and mainstream adoption of EPPs. Buyers should assess solutions in the context of a broader integrated workspace security strategy as part of their cybersecurity technology optimization efforts.

Strategic Planning Assumptions

By 2029, 30% of midsize organizations will converge workspace, data security and identity security capabilities into a workspace security platform, enabling holistic protection and centralized policy management.

By 2030, 25% of enterprises will adopt a continuous assessment and optimization process to assess and remediate workspace security controls in a targeted fashion to reduce the attack surface.

Market Definition/Description

Gartner defines an endpoint protection platform (EPP) as security software designed to protect managed endpoints — including desktop PCs, laptop PCs, virtual desktops, mobile devices and, in some cases, servers — 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 and file-less attacks using a combination of security techniques (such as static and behavioral analysis) and attack surface reduction capabilities (such as device control, host firewall management and application control). EPP prevention and protection capabilities are deployed as a part of a defense-in-depth strategy to help reduce the endpoint attack surface and minimize the risk of compromise. EPP detection and response capabilities are used to uncover, investigate and respond to endpoint threats that evade security protection, often as a part of broader threat detection, investigation and response (TDIR) capable products.

Mandatory Features

- Protection against malware and file-less attacks using endpoint real-time scanning and anti-malware techniques
- Endpoint attack surface reduction capabilities, such as device control, host firewall, exploit protection or application control
- Detection and blocking of endpoint threats using behavioral analysis of endpoint, application and end-user activity

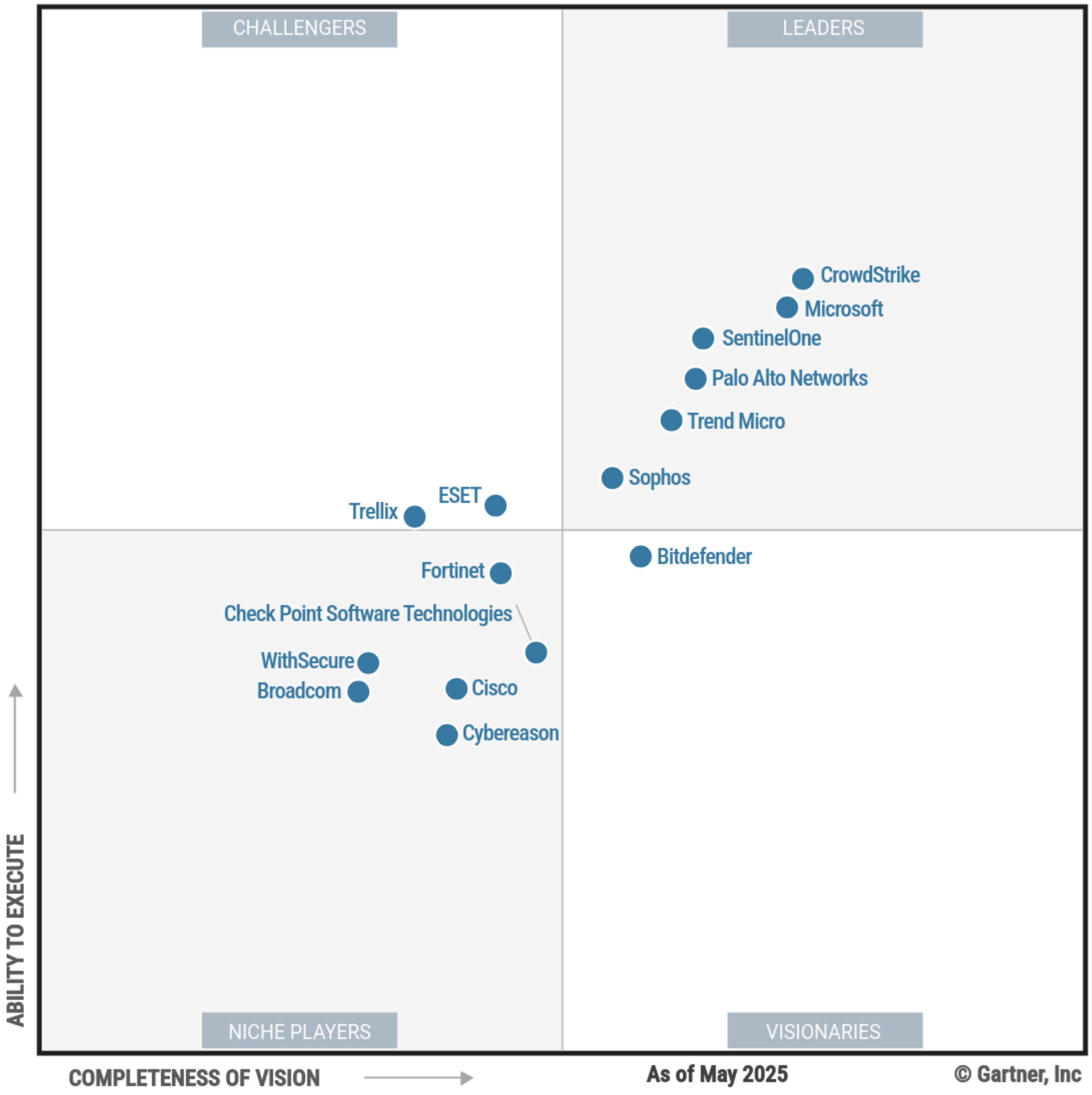
Common Features

- Integrated endpoint detection and response (EDR) functionality enabling real-time telemetry collection, detection customization, postincident investigation and response
- Assessment of endpoints for software and OS vulnerabilities and misconfigurations, as well as built-in or integrated patch management and virtual patching capabilities
- Capabilities for continuous assessment and optimization of EPP policies and settings against configuration best practices and emerging threats
- Workspace security platform integrations with email security, security service edge, identity protection, data security controls and endpoint management tools
- Integrations with native and third-party TDIR capable products enabling telemetry collection, correlation, investigation and remediation across multiple security controls
- Extended support for end-of-life, uncommon operating systems or legacy server workloads

- Partner- and vendor-delivered service wrappers, such as managed detection and response (MDR) and co-managed security monitoring services

Magic Quadrant

Figure 1: Magic Quadrant for Endpoint Protection Platforms



Gartner.

Vendor Strengths and Cautions

Bitdefender

Bitdefender is a Visionary in this Magic Quadrant. It's a vendor headquartered in Bucharest, Romania. Bitdefender GravityZone is the core endpoint protection platforms (EPPs) product. The vendor supports cloud-delivered, hybrid and on-premises (including air-gapped) management of EPP. In addition to EPP, Bitdefender offers workspace security controls, including email security and identity protection.

In the last year, Bitdefender added proactive hardening and attack surface reduction (PHASR). These capabilities aim to reduce endpoint attack surfaces through dynamic endpoint configuration, analyzing device and employee behavior, and correlating with external vulnerability and threat intelligence data to suggest prioritized posture changes, helping reduce exposure. The vendor also released Unified Security and Risk Analytics to prioritize and remediate hygiene findings across endpoint devices and identities. Bitdefender's 2025 roadmap calls for expansion of third-party integrations, enhanced log storage and capabilities to help visualize potential attack paths.

Bitdefender GravityZone is well-suited for small and midsize organizations looking for mature endpoint protection that balances ease of use with threat detection, investigations and response (TDIR) product functionality.

Strengths

- **Market understanding:** Bitdefender's understanding of the EPP market helps it prioritize and release product enhancements, such as endpoint risk analytics and endpoint tagging that show demonstrable benefit to customers based on reviews.

- **Innovation:** Bitdefender's recent innovations, such as PHASR, are differentiated in the market and offer customers more dynamic endpoint security configuration options that align protection with specific device and worker behaviors.

- **Customer experience:** Customers generally rate the technical and account management support they receive from Bitdefender as responsive and helpful in addressing issues in a timely manner.

Cautions

- **Operations:** Bitdefender remains one of the smaller providers in this Magic Quadrant and as such, it has less-diversified operations and geographic presence compared to Leaders.

- **Market responsiveness and track record:** Bitdefender's share of the EPP market remains low compared to challengers and leaders in this Magic Quadrant.

- **Sales strategy:** Based on Gartner end-user client inquiries and Peer Insights customer feedback, Bitdefender is less frequently included on competitive EPP provider shortlists compared to other vendors represented in this Magic Quadrant.

Broadcom

Broadcom is a Niche Player in this Magic Quadrant. It's a vendor headquartered in Palo Alto, California, U.S. Broadcom offers two distinct EPP products: Symantec Endpoint Security (SES) Complete and Carbon Black Cloud. This vendor supports cloud-delivered (including GovCloud), hybrid and on-premises (including air-gapped) management of EPP. In addition to EPP, Broadcom offers workspace security controls, including secure access, email security, identity protection and data loss prevention.

In the last year, Broadcom released incremental enhancements to its EPP products. SES Complete improved tamper protection through stricter agent uninstall policies and added support for Microsoft Windows Server 2025. It also ported adaptive protection features to the on-premises Symantec EPP product version, helping mitigate the risk of living-off-the-land attacks in environments with restricted network connectivity. Carbon Black Cloud EPP added intrusion detection system alert exclusions to reduce alert noise as well as improved agent-based vulnerability prioritization. Additionally, Broadcom began migrating Carbon Black Cloud EPP from Amazon Web Services (AWS) to Google Cloud infrastructure and moving admin authentication to Broadcom's Authentication Hub.

Broadcom's EPP products are suited for large global enterprises and organizations already invested in the Broadcom product portfolio.

Broadcom declined requests for supplemental information or to review the draft contents of this document. Gartner's analysis is therefore based on other credible sources.

Strengths

- **Vertical strategy:** Broadcom continues to offer and deliver incremental improvements to its on-premises Symantec EPP offering, benefiting organizations requiring hybrid or on-premises (including air-gapped) management of EPP in architecturally constrained environments.

- **Geographic strategy:** Broadcom's SES Complete administration dashboard supports multiple European and Asian languages in addition to English, benefiting international operations teams.

- **Sales strategy:** Broadcom maintains direct sales relationships with strategic customers in the global large enterprise segment, enabling improved account management compared to that offered to smaller organizations.

Cautions

- **Product strategy:** Over the past year, Broadcom has introduced incremental enhancements and bug fixes to its EPP products, which are likely to have limited appeal to prospects beyond Broadcom's primary target audience.
- **Innovation:** Broadcom's R&D is historically focused on closing technical gaps in its products, such as Intrusion Detection System (IDS) alert exclusion functionality in Carbon Black Cloud EPP, to moderately improve usability for existing customers rather than delivering major innovations in the EPP market.
- **Sales execution:** Customers outside the vendor's target audience reported challenges engaging with Broadcom and obtaining product information; they also encountered inflated pricing during renewal cycles of the vendor's EPP products.

Check Point Software Technologies

Check Point Software Technologies is a Niche Player in this Magic Quadrant. It's a vendor headquartered in Tel Aviv, Israel. Check Point Harmony Endpoint is its core EPP product. This vendor supports cloud-delivered, hybrid and on-premises (including air-gapped) management of EPP. In addition to EPP, Check Point offers workspace security controls, including secure access, email security, identity protection and data loss prevention.

In the last year, Check Point added a new version of its EPP agent, which reduces the footprint on the endpoint. The vendor also enhanced its browser extension, deployed as part of the EPP product but requiring a licensing add-on, with AI usage controls, aiming to provide visibility, classification and enforcement for applications with embedded AI. Other releases were outside of EPP, such as automation and orchestration capabilities, aiming to improve usability for customers using the broader offering. Check Point's 2025 roadmap calls for new centralized endpoint quarantine management and a revamp of its management console.

Check Point Harmony Endpoint is best suited for organizations invested in Check Point's Harmony suite of workspace security products.

Strengths

- **Pricing:** Check Point's EPP product pricing is highly competitive for the breadth of prevention and protection features it offers relative to other vendors in this research.
- **Geographic strategy:** Check Point's administration dashboard offers support for multiple European languages along with English, Chinese and Japanese. The vendor also has at least one SaaS point of presence in most major geographies, catering to organizations with data residency requirements.
- **Vertical strategy:** Check Point maintains a balanced presence across its key industry verticals, such as banking and government. The vendor continues to enhance its on-premises product, narrowing the feature gap with its cloud-delivered offering. Notably, Check Point introduced agent software and security content caching for endpoints without direct internet connectivity.

Cautions

- **Product strategy:** Check Point's recent and planned enhancements do not adequately address enterprise buyer needs, such as the breadth of collected endpoint telemetry, role-based access control granularity, vulnerability prioritization and configuration optimization. The Harmony Endpoint agent remains more resource-intensive compared to other products in this Magic Quadrant.
- **Innovation:** In the last year, Check Point's R&D has been focused on addressing technical gaps in its EPP product, such as reducing agent footprint, and enhancing adjacent product capabilities, which are less likely to impact the broader enterprise EPP market.
- **Sales strategy:** Based on Gartner end-user client inquiries and Peer Insights customer feedback, Check Point is rarely included on competitive EPP provider shortlists compared to market leaders in this Magic Quadrant.

Cisco

Cisco is a Niche Player in this Magic Quadrant. It's a vendor headquartered in San Jose, California, U.S. Cisco Secure Endpoint is the core EPP product. This vendor supports cloud-delivered, hybrid and on-premises (including air-gapped) management of EPP. In addition to EPP, Cisco offers workspace security controls, including secure access, email security and identity protection.

In the last year, Cisco added the Configuration Insights capability to provide continuous assessment of EPP configurations against Cisco's best practices and also expanded vulnerability assessment features to include not only endpoint OS but also applications. As a result of the Splunk acquisition, Cisco also updated its EPP integration with Splunk Enterprise core and Enterprise Security, improving event indexing and search. Other releases were outside of the core EPP, such as a MITRE ATT&CK coverage heat map in Cisco XDR. Cisco's 2025 roadmap calls for endpoint data loss prevention, integration of endpoint forensics capabilities and improved multitenancy to support deployments through managed services providers.

Cisco Secure Endpoint is best suited for organizations invested in Cisco's User and Breach Protection suite.

Strengths

- **Pricing:** Cisco's EPP product pricing is competitive compared to other vendors in this research, especially when purchased as part of one of its product suites.

- **Vertical strategy:** Cisco has a balanced presence across its key industry verticals, such as education and government. The vendor continues to enhance its on-premises product offering with recent enhancements such as remote agent uninstall, portable device control and additional OS support.

- **Operations:** Cisco is a large organization with geographically diverse operations and resources, which help support its customers in addressing security challenges that continue to extend beyond the EPP market.

Cautions

- **Product strategy:** Cisco's recent and planned enhancements do not adequately address enterprise buyer needs such as endpoint detection customization, breadth of collected endpoint telemetry, granular role-based access controls and API maturity. Cisco still has distinct administration consoles for several of its EPP product functions, which impacts the administration experience.

- **Market understanding:** Most buyers in the EPP market seek a single EPP product rather than the broad product suite positioned by Cisco. This mismatch with market needs makes Cisco's offering appealing to only a small subset of EPP buyers.

- **Sales strategy:** Based on Gartner end-user client inquiries and Peer Insights customer feedback, Cisco is rarely included on competitive EPP provider shortlists compared to market Leaders in this Magic Quadrant.

CrowdStrike

CrowdStrike is a Leader in this Magic Quadrant. It’s a vendor headquartered in Austin, Texas, U.S. CrowdStrike Falcon is the core EPP product. This vendor supports cloud-delivered (including GovCloud) management of EPP. In addition to EPP, CrowdStrike offers workspace security controls, including identity protection and data loss prevention.

In the last year, CrowdStrike released protection against ransomware attacks initiated from remote systems over Server Message Block (SMB) protocol, added granular security content update controls, and introduced Charlotte AI enhancements for augmenting incident triage and investigation. Other releases were outside of the core EPP, such as limited free third-party data ingestion. CrowdStrike’s 2025 EPP roadmap calls for Linux-host-based firewall management, device control enhancements for removable SD card media, agent-based network containment using fully qualified domain names (FQDNs), improved process exclusions management and support for Windows Subsystem for Linux.

CrowdStrike Falcon is well-suited for organizations looking for mature endpoint protection as part of a broader TDIR-capable product.

Strengths

- **Product:** CrowdStrike’s EDR functionality, cloud-based management, performance impact and TDIR product integration capabilities are well-regarded by customers for their efficacy and utility.

- **Product strategy:** CrowdStrike’s foundational developments in the EPP market, such as a lightweight endpoint agent with broad raw endpoint telemetry collection, enable it to continue to address emerging requirements of EPP buyers ahead of market competitors. Following the July 2024 Channel File 291 incident, CrowdStrike released granular content update controls for update scheduling, version control and group-based deployments, offered only by a few other vendors.

- **Market responsiveness and track record:** CrowdStrike holds a significant share of the EPP market and continues to demonstrate a leading rate of consideration by EPP buyers.

Cautions

- **Pricing:** Although CrowdStrike launched the Falcon Flex licensing model, customers report that its licensing is increasingly difficult to understand. Additionally, CrowdStrike remains one of the premium-priced offerings compared to other vendors in this research.

- **Geographic strategy:** CrowdStrike's dashboard language support is limited to English and Japanese. CrowdStrike also offers fewer geographic SaaS points of presence than other vendors in this Magic Quadrant.

- **Vertical strategy:** CrowdStrike's product offering is not suitable for organizations that require on-premises, air-gapped or hybrid management of EPP.

Cybereason

Cybereason is a Niche Player in this Magic Quadrant. It's a vendor headquartered in La Jolla, California, U.S. Cybereason Defense Platform is the core EPP product. This vendor supports cloud-delivered, hybrid and on-premises (including air-gapped) management of EPP. In addition to EPP, Cybereason offers workspace security controls such as identity protection.

In the past year, Cybereason introduced a new Application Control feature with allowlisting capabilities in its latest product version, aiming to enhance endpoint attack surface reduction. Cybereason also improved infostealer detection to help identify process activity associated with suspicious and unauthorized access to stored credentials and secrets on protected endpoints. Cybereason's 2025 roadmap calls for native vulnerability management and prioritization, endpoint data loss prevention, file integrity monitoring and detection customization capabilities in its TDIR product offering.

Cybereason Defense Platform is well-suited for organizations looking for solid endpoint protection in supported geographies.

Strengths

- **Pricing:** Cybereason's EPP product pricing is competitive for the breadth and maturity of behavioral endpoint monitoring and protection capabilities included.

- **Innovation:** Cybereason's recent releases, such as infostealer detection and Application Control, are likely to benefit the security of existing customers who successfully adopt them.

- **Product:** Cybereason's EDR functionality and hybrid management capabilities are well-regarded by customers for their effectiveness.

Cautions

- **Product strategy:** Cybereason's product lacks features such as native endpoint vulnerability assessment, which most other EPPs already offer. Additionally, Gartner notes an ongoing effort to consolidate administration dashboards across old and new EPP product versions as well as adjacent TDIR-capable products.
- **Operations:** In the past year, Cybereason has undergone multiple organizational structure and leadership changes, indicating that the organization remains in flux.
- **Sales strategy:** Based on Gartner end-user client inquiries and Peer Insights customer feedback, Cybereason is rarely included on competitive EPP provider shortlists.

ESET

ESET is a Challenger in this Magic Quadrant. It's a vendor headquartered in Bratislava, Slovakia. ESET PROTECT is the core EPP product. This vendor supports cloud-delivered, hybrid and on-premises (including air-gapped) management of EPP. In addition to EPP, ESET offers workspace security controls such as email security.

In the last year, ESET released a proprietary ransomware rollback feature that helps restore systems to their preattack state, aiming to reduce operational impact from threats. ESET launched AI PC integration with Intel, helping to reduce endpoint CPU load and speed up endpoint scanning. The vendor has also expanded vulnerability assessment and patch management across Windows, macOS and Linux. ESET's 2025 roadmap calls for expanded support for third-party integrations, enhanced multitenancy and new offerings in adjacent market categories, such as identity and workload protection.

ESET PROTECT is well-suited for small and midsize organizations seeking mature endpoint prevention and protection capabilities.

Strengths

- **Customer experience:** Customers rate the technical and account management support they receive from ESET as responsive and helpful in addressing issues in a timely manner.
- **Operations:** Most ESET resources are dedicated to supporting EPP research and development and most of ESET's revenue comes from selling its EPP product.
- **Geographic strategy:** ESET's dashboard and documentation support multiple European and Asian languages in addition to English, making it attractive to customers worldwide.

Cautions

- **Product strategy:** ESET's recent enhancements do not adequately address certain enterprise buyer needs, such as breadth of collected endpoint telemetry (especially on Linux OS), the range of prebuilt third-party integrations and mature vulnerability prioritization. Additionally, ESET's product requires installation of multiple endpoint applications to access its full range of EPP capabilities.

- **Market responsiveness and track record:** In the last year, ESET's market share growth has been slower compared to the overall market growth rate.

- **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 Leaders in this research.

Fortinet

Fortinet is a Niche Player in this Magic Quadrant. It's a vendor headquartered in Sunnyvale, California, U.S. FortiEDR is the core EPP product. This vendor supports cloud-delivered, hybrid and on-premises (excluding air-gapped) management of EPP. In addition to EPP, Fortinet offers workspace security controls, including secure access, email security and data loss prevention.

In the last year, Fortinet released the new FortiEndpoint agent, which integrates the installers for the FortiEDR and FortiClient components, aiming to reduce agent deployment and maintenance efforts. The vendor has also introduced a new file reclassification engine to reduce false positives in FortiEDR. Fortinet's 2025 roadmap calls for support for FortiEDR deployments in air-gapped environments, device control for macOS, ARM (Acorn RISC Machine) support for Windows and Linux, and the transition of the FortiEDR Linux agent to an eBPF-based architecture. At the end of 2024, Fortinet acquired and started the integration process of Perception Point, a provider of email, collaboration and web browser security technologies, expanding workspace security controls offered by Fortinet.

FortiEDR is best suited for organizations invested in the broader portfolio of Fortinet's workspace security products.

Strengths

- **Geographic strategy:** Fortinet has multiple SaaS points of presence in most major geographies, catering to organizations with data residency and regulatory requirements.

The vendor continues to enhance its administration dashboard by adding new language support options, including Spanish, Portuguese and German.

- **Vertical strategy:** Fortinet maintains a balanced presence across its key industry verticals, such as government and manufacturing. The vendor continues to enhance its on-premises product, maintaining feature parity with its cloud-delivered FortiEDR product offering.

- **Overall viability:** Fortinet is a large, well-funded vendor with a strong presence in the market across various lines of business and consistent revenue growth. Fortinet made public statements about its intention to continue to invest in technology for security operations, including FortiEDR.

Cautions

- **Product strategy:** Fortinet's past and planned enhancements do not adequately address certain enterprise buyer needs, such as granular role-based access controls, built-in controls for scheduling endpoint updates, intuitive detection customization UX or a fully streamlined security analyst workflow.

- **Innovation:** In the last year, there were limited notable innovative EPP capabilities released by Fortinet compared to the market. R&D was focused on integration (Perception Point acquisition) and unification of endpoint protection and secure access agents.

- **Market responsiveness and track record:** Fortinet's share of the EPP market remains low compared to Challengers and Leaders in this Magic Quadrant.

Microsoft

Microsoft is a Leader in this Magic Quadrant. It's a vendor headquartered in Redmond, Washington, U.S. Defender for Endpoint is the core EPP product. This vendor supports cloud-delivered (including GovCloud) management of EPP. In addition to EPP, Microsoft offers workspace security controls, including secure access, email security, identity protection and data loss prevention.

In the last year, Microsoft expanded its Linux distribution support, introduced ARM64-based Linux support, reduced resource requirements for Linux, added new attack surface reduction rules and integrated its endpoint and identity protection agents, aiming to reduce maintenance efforts on domain controllers. Microsoft also added agent-based network containment of compromised unmanaged devices (in preview) as part of its automatic attack disruption capability. Other releases were outside of the core EPP, such as Security Exposure Management, helping evolve Microsoft’s Secure Score. Microsoft’s 2025 roadmap calls for simplified EPP product onboarding across different OS through a new package manager and new capabilities for a more dynamic configuration of endpoint attack surface reduction rules, aiming to reduce exposure and speed up response during attacks.

Defender for Endpoint is well-suited for organizations looking for mature endpoint protection that is integrated as part of a broader workspace security offering as well as for those invested in the Microsoft security product portfolio.

Strengths

- **Product:** Microsoft’s EDR functionality, protection, cloud-based management and workspace security integration capabilities are generally well-regarded by customers for their effectiveness and maturity.
- **Product strategy:** Microsoft’s planned enhancements, such as autonomous attack surface reduction, build on a long history of consistent investment in its EPP product capabilities, such as rules for endpoint attack surface reduction. Microsoft’s integration with its broader ecosystem is notable.
- **Market responsiveness and track record:** Microsoft holds a significant share of the EPP market and continues to demonstrate a leading rate of consideration by EPP buyers.

Cautions

- **Sales execution:** Customers using Microsoft licensing bundles often report product underutilization and diminished discounts at renewal time, which can be challenging in the current macroeconomic environment.
- **Customer experience:** Customers report that initial deployment, configuration optimization and relatively slow pace of support issue resolution may degrade the overall customer experience.
- **Innovation:** In the last year, Microsoft’s R&D appears to have been focused on bolstering adjacent products, such as Security Exposure Management, which is less likely to impact the broader EPP market.

Palo Alto Networks

Palo Alto Networks is a Leader in this Magic Quadrant. It’s a vendor headquartered in Santa Clara, California, U.S. Cortex XDR is the core EPP product. This vendor supports cloud-delivered (including GovCloud) management of EPP. In addition to EPP, Palo Alto Networks offers workspace security controls, including secure access and identity protection.

In the last year, Palo Alto Networks increased endpoint-exception-handling granularity, enhanced malware detection across major OSs — including macOS and Linux — and improved Windows antitampering, aiming to strengthen protection against endpoint security bypasses. The vendor also updated its security modules for shellcode and kernel protection, and expanded its file type coverage on Windows to include ASP and ASPX types. Other releases were outside of the core EPP, focusing on improvements to the overall investigation-and-response workflow in its broader TDIR-capable product. Palo Alto Networks’ 2025 roadmap calls for enhancements to EDR functionality, support for additional Windows architectures, improved vulnerability prioritization and remediation and a new email security product, bolstering workspace security.

Cortex XDR is well-suited for organizations looking for mature and highly customizable endpoint protection as part of a broader TDIR-capable product.

Strengths

- **Product:** Cortex XDR’s capabilities, such as EDR functionality, protection, cloud-based management and TDIR product integration are generally well-regarded by customers for their efficacy and maturity.

- **Product strategy:** Palo Alto Networks consistently demonstrates improvements in its EPP product functionality and protection efficacy across major operating systems. The vendor’s planned enhancements align with emerging requirements of EPP buyers.

- **Overall viability:** Palo Alto Networks is a large, well-funded vendor with strong global presence and faster-than-average revenue growth in the EPP market. Palo Alto Networks publicly stated its intentions to continue to invest in its Cortex product portfolio.

Cautions

- **Pricing:** Although Palo Alto Networks offers a competitive displacement program, the vendor’s offering remains a premium-priced product with some customers expressing concern over cost at renewal time.

- **Vertical strategy:** Palo Alto Networks' product offering is not suitable for organizations that require on-premises or air-gapped management of EPP.
- **Market responsiveness and track record:** The vendor's share of the EPP market remains significantly lower than that of other Leaders in this Magic Quadrant.

SentinelOne

SentinelOne is a Leader in this Magic Quadrant. It's a vendor headquartered in Mountain View, California, U.S. SentinelOne Singularity is the core EPP product. This vendor supports cloud-delivered (including GovCloud), hybrid and on-premises (including air-gapped) management of EPP. In addition to EPP, SentinelOne offers workspace security controls such as identity protection.

In the last year, SentinelOne improved detection of infostealers, malicious macros and lateral movement techniques in its EPP. It also released a new community verdict feature as part of Purple AI that helps users understand the opinions of other organizations on similar alerts, supporting analyst decision making. Other releases were outside of the core EPP, such as automation and orchestration capabilities introduced following SentinelOne's acquisition of Stride Security. In 2025, SentinelOne's roadmap calls for improved exclusion management hygiene and optimization of EPP agent resource requirements among other enhancements.

SentinelOne Singularity is well-suited for organizations looking for mature, endpoint protection balancing ease of use and configuration granularity depth.

Strengths

- **Product:** SentinelOne's EDR functionality, cloud-based management, ease of use and hybrid management capabilities are generally well-regarded by customers for their efficacy and maturity.
- **Product strategy:** SentinelOne's developments in the EPP market resulted in differentiated and intuitive console UX, balancing high configuration granularity with capability depth and ease of use. Recent and planned releases reaffirm its continued investment in maintaining EPP product efficacy while gradually expanding its portfolio.
- **Market responsiveness and track record:** SentinelOne's share of the EPP market is larger than that of most other vendors included in this Magic Quadrant.

Cautions

- **Geographic strategy:** SentinelOne’s administration dashboard supports only English and Japanese. Most of SentinelOne’s customers are based in the U.S., resulting in lower market penetration in international markets compared to other Leaders in this Magic Quadrant.
- **Innovation:** In the last year, SentinelOne’s R&D appears to be focused on bolstering adjacent product capabilities, such as automation and orchestration, which are less likely to impact the broader EPP market.
- **Pricing:** SentinelOne’s offering remains a premium-priced product in the EPP market, which may put a strain on organizations in the current macroeconomic environment.

Sophos

Sophos is a Leader in this Magic Quadrant. It’s a vendor headquartered in Abingdon, England, U.K. Sophos Endpoint powered by Intercept X is the core EPP product. This vendor supports cloud-delivered management of EPP. In addition to EPP, Sophos offers workspace security controls, including secure access, email security and identity protection.

In the last year, Sophos released protection against attacks from rogue or unmanaged devices through agent-based network containment. The vendor also completed the initial integration of Sophos Endpoint powered by Intercept X with Taegis XDR (through its Secureworks acquisition), enhancing customers’ ability to correlate Sophos endpoint alerts with third-party controls. In 2025, Sophos completed its acquisition of Secureworks, a provider of TDIR technologies and managed detection and response (MDR) services, and is pursuing further convergence of Sophos Central with Taegis XDR. This aims to offer customers a more unified experience, built-in identity protection and improved third-party integration. Sophos’ 2025 roadmap also calls for agent antitampering enhancements as well as integration of endpoint protection and secure access capabilities.

Sophos Endpoint powered by Intercept X is well-suited for organizations looking for endpoint protection that is integrated as part of a broader workspace security offering.

Strengths

- **Sales strategy:** Sophos offers user-based licensing, enhancing the competitiveness of its EPP product pricing for organizations where each employee uses multiple devices that require protection.

- **Operations:** Sophos' acquisition of Secureworks increases available resources, helping expand operations, sales reach and expertise in adjacent market segments. This acquisition is expected to help close gaps in TDIR functionality and product customization, potentially improving appeal to larger enterprises.

- **Overall viability:** Sophos demonstrates consistent revenue growth and a long history in the EPP market, indicating a likelihood to continue to invest in its EPP.

Cautions

- **Innovation:** In the last year, Sophos' R&D appears to be focused on addressing gaps in Sophos Endpoint powered by Intercept X endpoint telemetry collection. Additionally, Sophos is focused on integrating its EPP with Taegis XDR, resulting in fewer EPP-specific innovations during the analysis period.

- **Customer experience:** Customers report that high system resource consumption during full system scanning and inefficient security workflows in Sophos Central may degrade the overall user and customer experience.

- **Vertical strategy:** Sophos' product offering is not suitable for organizations that require on-premises or air-gapped management of EPP.

Trellix

Trellix is a Challenger in this Magic Quadrant. It's a vendor headquartered in Plano, Texas, U.S. Trellix Endpoint Security Suite is the core EPP product. This vendor supports cloud-delivered (including GovCloud), hybrid and on-premises (including air-gapped) management of EPP. In addition to EPP, Trellix offers workspace security controls, including email security and data loss prevention.

In the last year, Trellix continued to work on simplifying agent installation, reducing maintenance overhead and integrating EDR and forensics features. Other capabilities released were outside of the core EPP, such as a new vendor-delivered service wrapper and attack-path-discovery capabilities to help security teams understand the exploitability of various organizational assets. Trellix's 2025 roadmap calls for improvements to in-memory and code injection attack detection, and further consolidation of various endpoint security features in a single agent to reduce system footprint and maintenance overhead, among other enhancements.

Trellix Endpoint Security Suite is well-suited for organizations requiring a comprehensive set of endpoint protection capabilities with granular customization options.

Strengths

- **Geographic strategy:** The Trellix administration dashboard and documentation support multiple European and Asian languages in addition to English, making it attractive to customers worldwide.

- **Vertical strategy:** Trellix maintains a balanced presence across its key industry verticals, such as government and manufacturing. The vendor's offering is attractive to organizations requiring hybrid or on-premises (including air-gapped) management of EPP.

- **Market responsiveness and track record:** Trellix's share of the EPP market remains significantly higher than that of Niche Players and Visionaries.

Cautions

- **Product strategy:** Trellix's recent enhancements do not adequately address gaps in its product UX, which remains highly fragmented with numerous role-specific dashboards loosely integrated via single sign-on. Customers report that the current UX can impact the ease of administration and necessitate longer training.

- **Innovation:** In recent years, Trellix's R&D has been mostly focused on product integration efforts, aiming to rationalize agents and administration dashboards.

- **Operations:** In the past year, Trellix has undergone multiple executive leadership and product management role changes, indicating the organization is in transition.

Trend Micro

Trend Micro is a Leader in this Magic Quadrant. It's a vendor headquartered in Tokyo, Japan. Trend Vision One Endpoint Security is the core EPP product. This vendor supports cloud-delivered, hybrid and on-premises (including air-gapped) management of EPP. In addition to EPP, Trend Micro offers workspace security controls, including secure access, email security and identity protection.

In the last year, Trend Micro released adaptive threat detection and behavioral protection capabilities that adjust based on employee, system and threat context, aiming to help optimize protection. It also released granular controls for security content updates, helping to manage operational risk originating from updates. Trend Micro added deepfake detection capabilities as part of its EPP. Other releases outside of the core EPP included capabilities to help visualize potential attack paths. Trend Micro's 2025 roadmap calls for features that aim to reduce risk by enabling safe adoption of generative AI, integration of AI PCs as well as enhancements to data loss prevention and agent maintenance and hygiene.

Trend Vision One Endpoint Security is well-suited for organizations looking for mature endpoint protection integrated as part of a broader workspace security offering.

Strengths

- **Product:** Trend Micro's prevention, cloud-based management, hybrid management, OS support and workspace security capabilities are generally well-regarded by customers. Notably, Trend Micro's virtual patching helps shield vulnerabilities in applications that can't be easily patched.

- **Product strategy:** Trend Micro's developments in the EPP market resulted in a differentiated, well-integrated set of endpoint protection capabilities, such as adaptive protection settings. Recently released and planned enhancements reaffirm its continued commitment to advancing its product against emerging customer requirements.

- **Innovation:** Trend Micro's recent innovations, such as deepfake detection, adaptive threat detection and behavioral protection, and granular content update controls, offer customers early access to improved endpoint security and operations.

Cautions

- **Customer experience:** Indications from customers and third-party efficacy tests are that high-alert volume and resource consumption during scanning impact the overall user and customer experience.

- **Sales strategy:** Customers report that Trend Micro's credit-based licensing can be difficult to understand, citing lack of clarity regarding how credits are allocated within the vendor's broader portfolio.

- **Overall viability:** In the last year, Trend Micro's revenue growth in the EPP market has been slower than that of other Leaders in this Magic Quadrant.

WithSecure

WithSecure is a Niche Player in this Magic Quadrant. It's a vendor headquartered in Helsinki, Finland. WithSecure Elements XDR is the core EPP product. This vendor supports cloud-delivered, hybrid and on-premises (including air-gapped) management of EPP. In addition to EPP, WithSecure offers workspace security controls, including email security and identity protection.

In the last year, WithSecure released additional response capabilities for macOS and Linux, such as file retrieval and process enumeration, upgraded custom detections allowing for more granular definition and blocking of indicators of compromise and added support for ChromeOS. Other releases were outside the core EPP, such as capabilities to help visualize potential attack paths as well as response actions for Entra ID to help mitigate identity threats by terminating active user sessions, resetting account credentials and restricting compromised user account access. WithSecure's 2025 roadmap calls for reporting exposure findings with incidents, additional third-party integrations and the deployment of its EPP on AWS European Sovereign Cloud, helping organizations in the EU address data sovereignty and compliance requirements.

WithSecure Elements XDR is well-suited for small and midsize organizations, especially those headquartered in Europe.

Strengths

- **Market understanding:** WithSecure's understanding of the EPP market's dynamics and competitors helps it concentrate its efforts on helping organizations in Europe meet their regulatory, product and service needs.
- **Geographic strategy:** WithSecure's administration dashboard and documentation support multiple European and Asian languages in addition to English, making it attractive to customers worldwide.
- **Overall viability:** WithSecure has a long history in the EPP market and most of its revenue comes from selling EPP software.

Cautions

- **Product strategy:** WithSecure's recent product enhancements, such as advanced response actions for non-Windows OSs and detection customization, appear to be focused on closing the gaps in its product and are less likely to impact the broader enterprise EPP market.
- **Operations:** WithSecure remains a comparatively small company with less-diversified operations and geographic presence compared to Leaders in this research.

- **Market responsiveness and track record:** WithSecure’s share of the EPP market remains lower than that of Leaders or Challengers 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

- No vendors were dropped from this Magic Quadrant.

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 are the specific attributes a provider must have to be included in this Magic Quadrant. 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 inclusion criteria using their core EPP product as of the start of Gartner’s research and survey process (on 31 March 2025). Products and capabilities had to be generally available to be considered for the evaluation. Requirements included:

- The solution supports at least Windows, macOS and Linux operating systems.

- The solution combines prevention, protection, detection and response functionality in a single agent.

- The solution enforces protection using a combination of endpoint security techniques, attack surface reduction controls and assessment capabilities.
- The solution embeds endpoint detection and response (EDR) functionality, including real-time (or near real-time) automated endpoint telemetry collection as well as detection customization, postincident investigation and response capabilities.
- The solution provides a severity rating, a process tree and a mapping of events and alerts to MITRE ATT&CK 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 integrates with native or third-party TDIR-capable products, enabling telemetry collection, correlation, investigation and response across multiple security controls.
- 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 orMRG Effitas) for security efficacy within 24 months before 31 March 2025.
- A vendor must have over 7.5 million endpoints protected and actively under management in production using its EPP as of 31 March 2025, excluding seats sold via OEM agreements. More than 500,000 seats 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.

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.

Ability to Execute Evaluation Criteria

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	High

Source: Gartner (July 2025)

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.

Completeness of Vision Evaluation Criteria

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	Medium

Source: Gartner (July 2025)

Quadrant Descriptions

Leaders

Leaders consistently demonstrate progress across all criteria related to Ability to Execute and Completeness of Vision. They offer mature endpoint telemetry support, integrated EDR functionality and proven cloud-based management. Leaders provide bidirectional workspace security integrations, holistic exposure assessment and TDIR capabilities, enabling buyers to optimize their security stacks. Leaders hold significant mind and market share. However, being a Leader does not make them a default choice for every buyer. Customers should not assume they must purchase only from a Leader. Leaders may be less agile in responding when Visionaries challenge the status quo in the market.

Challengers

Challengers offer mature endpoint protection products that effectively meet the needs of EPP buyers. They also have strong market visibility, resulting in better Ability to Execute compared to Niche Players. However, Challengers are often late in addressing emerging needs, lack in-depth product integration and may have accumulated technical debt, affecting usability. They may also lack alignment with the market's direction, impacting their Completeness of Vision compared to Leaders. Challengers are practical choices, especially for customers with established strategic relationships with them.

Visionaries

Visionaries deliver new and emerging capabilities ahead of their market competitors, providing buyers with early access to enhanced security and administration. For example, Visionaries may offer features such as dynamic endpoint and security policy configuration based on employee, device and threat context; bidirectional integrations with native and third-party workspace security controls and broader TDIR capabilities. While Visionaries can influence the direction of technological development in the market, they may not yet demonstrate a consistent track record of execution and often lack market share. Customers choose Visionaries for early access to innovative features.

Niche Players

Niche Players offer solid products but rarely lead the market in introducing new and emerging capabilities or in acquiring and maintaining significant market share. Some vendors are Niche Players because they focus on a specific geographic region or market segment. Others are Niche Players because they excel in a particular use case, industry or technical capability set. Niche Players can be a good choice for existing customers, those in the vendor's target market segment, change-averse organizations in supported regions or organizations looking to augment their existing EPP for better defense in depth.

Context

Organizations primarily use EPPs to secure end-user endpoints like laptops, workstations, virtual desktops, mobile devices and, in some cases, servers by reducing the endpoint attack surface and providing real-time protection, detection and response capabilities. Vendors increasingly integrate EPPs with broader workspace security platforms and TDIR-capable products to reduce operational complexity and help optimize cybersecurity technology stacks.

Gartner Magic Quadrant vendor surveys reveal that over 60 percent of enterprise endpoints are protected by cloud-delivered EPPs that include modern behavioral protection capabilities. The mature EPP market, evolving threats and the need for more effective security operations have started to shift buyer interest to other market categories. An estimated 20 percent of organizations purchase adjacent TDIR-capable products from their EPP provider to achieve better efficiency and optimize cost compared to manually integrating otherwise disjointed controls.

All vendors in this research offer generative AI or AI assistant capabilities as part of their EPP products. Despite market hype, current practical applications of these technologies remain in their infancy. Today, AI assistants are most useful for triaging and interpreting preexisting findings, especially for less experienced analysts or those unfamiliar with specific security tools. Most EPP providers pursuing a platform strategy still need to integrate their AI assistants with third-party products to meaningfully accelerate automation of tasks across heterogeneous security stacks.

Market Overview

Endpoint protection platforms is a mature market. Gartner estimates the EPP market at $15.7 billion in 2024, growing at 16.3 percent per year (see **Market Share: Security Software, Worldwide, 2024**). Notably, Microsoft and CrowdStrike hold an estimated 40 percent of the EPP market share. Gartner forecasts that the market will expand at a compound annual rate of approximately 14 percent through 2027, reaching a size of $23.4 billion based on constant currency (see **Forecast: Information Security, Worldwide, 2023-2029, 1Q25 Update**).

In 2025, EPP buyers prioritize vendor trust, customer experience and the vendor’s ability to deliver on security outcomes as crucial factors when selecting providers. Buyers assess both technical and nontechnical aspects, including product quality, protection efficacy, overall reliability, commercial behaviors, third-party risk and the vendor’s track record of handling operational and security incidents among others.

Product Evolution

In 2025, most vendors exhibit limited innovation in their EPP products, opting instead to concentrate their research and development on adjacent products, integrations and advancements in generative and agentic AI, promising improvements for security operations teams.

Concurrently, industry reports indicate that attacks on security products and bypasses of endpoint protection tools are increasingly common. [1] Most EPP vendors are reactive in how they address these challenges, requiring content updates or configuration changes, placing the responsibility on the operators of these tools and leaving organizations exposed for longer. To mitigate these challenges, EPP buyers should invest in continuous security control optimization, efficacy validation testing and control resilience initiatives, as well as demand these from incumbent vendors.

Most vendors are also expanding agent-based vulnerability and exposure assessment and prioritization. These capabilities are often inadequate to support comprehensive threat exposure management programs due to the lack of context about assets, threats and environment. For example, most vendors struggle to demonstrate how their EPP product helps mitigate or protect against exploitation of vulnerabilities and exposures that it discovers. As a result, EPP buyers should use built-in vulnerability assessment features as context for incident investigation and response but not as a replacement for a comprehensive exposure management solution.

The outage caused by the CrowdStrike content update on 19 July 2024 brought renewed focus on content update controls, which remain rudimentary in most products. [2] Unlike with agent software updates, most products still offer no support for content update scheduling, version control or group-based deployment.

Product Differentiation

All products in this research include endpoint real-time scanning, anti-malware, attack surface reduction and behavioral analysis capabilities.

The primary differences among EPP products are:

- Near-real-time endpoint telemetry collected and used for behavioral analysis
- Customization for admin functions and detection logic
- Feature support for non-Windows and legacy OS

- Resource consumption and performance impact
- Built-in vulnerability assessment and prioritization
- Hybrid and on-premises deployment support
- Language support and points of presence and data residence across geographies
- API maturity and integration with TDIR products and workspace security controls

Prospective buyers should use Critical Capabilities for Endpoint Protection Platforms to assess products against specific organizational use cases or build custom use cases that suit their needs.

Generative and Agentic AI

Vendors continue to enhance product usability through investment in generative and agentic AI, yet adoption by security teams remains limited. Based on data from the 2025 Gartner Cybersecurity Innovations in AI Risk Mgmt and Use Survey, only 14% of respondents currently use such capabilities for threat detection and incident response, and only 9% for security policy administration. [3]

Some vendors in the EPP market offer these capabilities with no additional cost in their product’s base license. Current generative AI capabilities, based on LLM integration, provide administrative assistance such as incident summarization, documentation discovery, text-to-code and code-to-text translation. Agentic AI roadmaps point toward more task-oriented solutions that can replace repetitive jobs like alert triage or credential reset tasks.

Realizing the benefits of generative AI and agentic AI add-ons requires intrinsic product and workflow integration that will be difficult for organizations with heterogeneous security stacks. Prospective buyers should assess how generative and agentic AI affect the overall ease of use and analyst experience.

Integration

Vendors continue to integrate EPP products with other workspace security controls and TDIR-capable products. Workspace security is founded upon integrated, modular capabilities required for protecting the modern knowledge worker’s devices, identity, applications and data. Vendors in the EPP market also expand their TDIR product coverage beyond the endpoint to other workspace security controls, such as identity, email, network and data.

To manage cost and complexity, midsize organizations with limited resources should evaluate EPP products within a workspace security strategy. Such organizations should aim for a minimal effective workspace security stack, which is highly integrated rather than using a disjointed best-of-breed product approach.

Market Drivers

Buyers often face one or more of the following market trends that affect their selection of EPP providers:

- **Cybersecurity technology optimization:** Security leaders depend on optimization of their technology stacks to reduce inefficiencies, manage complexity and optimize cost. Organizations need to strike the right balance between consolidation of commodity capabilities and purchase of separate, differentiated products to address niche requirements. Vendors increasingly offer EPP products as part of a broader security platform strategy, necessitating organizations to reassess incumbent EPP providers and capabilities during major contract renewals (see **Simplify Cybersecurity with a Platform Consolidation Framework**).

- **Evolving threat environment:** The continued stream of attacks targeting modern hybrid work environments, combined with limited resources, underscores the need to integrate various workspace security controls as well as TDIR capabilities to improve operational effectiveness. To reduce exposure to emerging threats and realize the full potential of investments in EPP, organizations also need to continuously optimize endpoint and workspace security control configurations (see **2025 Strategic Roadmap for Workspace Security** and **Reduce Threat Exposure with Security Controls Optimization**).

- **Security operations effectiveness:** Resource-constrained organizations often seek partner- and vendor-delivered service wrappers, choosing from outcome-driven MDR or co-managed security monitoring service options. Organizations expect their providers to perform investigation, containment and exposure reduction, regularly allowing providers to perform remote responses to disrupt or contain threats. Many of these response actions are centered around EPPs but expand to a broader set of TDIR-capable controls (see **Market Guide for Managed Detection and Response**).

⊕ Evidence

⊕ Evaluation Criteria Definitions