Magic Quadrant for Endpoint Protection

26 May 2026 - ID G00838669 - 41 min read

By Deepak Mishra, Evgeny Mirolyubov, and 1 more

Rapid AI adoption and emerging supplier sovereignty requirements are shaping buyer priorities for endpoint protection products. Buyers should factor in sovereignty objectives, as well as requirements for AI discovery and usage control on corporate endpoints, when selecting vendors.

Strategic Planning Assumptions

By 2028, 90% of endpoint protection vendors will offer AI discovery and usage control features.

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

By 2029, organizations that integrate endpoint security tools, management processes and operations teams will reduce incident response times by at least 40%.

Market Definition/Description

Gartner defines endpoint protection as security software that protects managed endpoints — including desktop PCs, laptop PCs, virtual desktops, mobile devices and, in some cases, servers — against known and unknown malicious attacks. Endpoint protection equips security teams with the tools necessary to investigate and remediate incidents that evade prevention controls. Endpoint protection products are delivered as

software agents deployed to endpoints and connected to centralized security analytics and management consoles.

Endpoint protection provides a defensive security control that protects end-user endpoints against known and unknown malware and fileless attacks using a combination of security techniques, such as static and behavioral analysis. It also uses attack surface reduction capabilities, such as device control, host firewall management and application control to limit exposure to threats. Organizations deploy endpoint protection as part of a defense-in-depth strategy to reduce the endpoint attack surface and minimize the risk of compromise. Its detection and response capabilities help uncover, investigate and remediate threats that evade prevention controls, often as part of broader threat detection, investigation and response (TDIR) products.

Mandatory Features

- Protect endpoints against malware through real-time scanning and anti-malware techniques.
- Reduce the endpoint attack surface with capabilities such as device control, host based firewall management, exploit protection or application control for various operating systems.
- Detects and blocks endpoint threats using behavioral analysis of endpoint, application and end-user activity.

Optional Features

- Integrate endpoint detection and response (EDR) capabilities that enable real-time telemetry collection, customizable detection, postincident investigation and response.
- Assess endpoints for software and operating system vulnerabilities and misconfigurations, and support built-in or integrated patch management and virtual patching for various operating systems.
- Provide integrated endpoint data loss prevention to identify and prevent sensitive data exfiltration through removable media, printing, Bluetooth and browser.
- Deliver continuous assessment and optimization of endpoint protection policies and settings against configuration best practices and emerging threats.

- Integrate with workspace security platforms, including email security, security service edge, identity protection, data security controls, endpoint management tools and secure enterprise browsers.
- Integrate with native and third-party TDIR products to enable telemetry collection, correlation, investigation and remediation across multiple security controls.
- Support extended protection for end-of-life, uncommon operating systems or legacy server workloads.
- Include an embedded cybersecurity AI assistant for alert summarization, content creation and response guidance.

Magic Quadrant

Figure 1: Magic Quadrant for Endpoint Protection

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 product. The vendor supports cloud-delivered, hybrid and on-premises (including air-gapped) management. Bitdefender GravityZone is well-suited for small and midsize organizations seeking mature endpoint protection that balances ease of use with robust TDIR functionality.

In the past year, Bitdefender's key product developments included:

- **Network vulnerability scanner:** Extends endpoint vulnerability assessment with network-based scanning to identify exposed services, open ports and common vulnerabilities and exposures (CVEs).
- **Compliance manager:** Supports continuous compliance monitoring, remediation, control mapping and reporting across standards such as NIST, CIS Controls, NIS2 and GDPR.

The vendor also launched new sovereign cloud partnerships with OVHcloud (France) and secunet (Germany), delivering GravityZone in EU-hosted environments. It also acquired Mesh Security (email security). Bitdefender's 2026 roadmap includes breach path prediction capabilities to improve exposure management, along with AI security to help organizations discover and control enterprise AI usage.

Strengths

- **Product strategy:** Bitdefender's ongoing investments are aligned with emerging buyer requirements in the endpoint protection market. These include investments in proactive hardening and attack surface reduction (PHASR), an intuitive and well-integrated product console, and a product roadmap aimed at helping organizations discover and control AI usage.
- **Geographic strategy:** The product console is available in multiple languages, and Bitdefender offers SaaS cloud hosting points of presence in Europe, North America and Asia/Pacific. Recent sovereign hosting options in France and Germany provide more deployment choices for European organizations.
- **Pricing:** Bitdefender's endpoint protection product pricing is competitive for the breadth and depth of capabilities it offers, relative to other vendors in this Magic Quadrant.

Cautions

- **Operations:** Bitdefender remains one of the smaller providers in this Magic Quadrant, with less-diversified operations, fewer resources and lower enterprise visibility compared to Leaders.
- **Sales strategy:** Based on Gartner client inquiries and Peer Insights feedback, Bitdefender is less frequently included on competitive endpoint protection provider shortlists than Leaders.

- **Market responsiveness and track record:** Bitdefender's share of the endpoint protection market remains low compared to Challengers and Leaders 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 endpoint protection products: Symantec Endpoint Security (SES) Complete and Carbon Black Cloud. Broadcom supports cloud-delivered (including AWS GovCloud), hybrid and on-premises (including air-gapped) management. Its endpoint protection products are best-suited for large global enterprises and organizations already invested in the Broadcom portfolio.

In the past year, Broadcom's key product developments included:

- **Incidents summary view in SES Complete:** Provides a timeline summarizing each incident, including priority, severity, impacted entities and recommended remediation actions.
- **Unified Symantec Endpoint Security Agent:** Aims to reduce agent management overhead by unifying Broadcom's endpoint protection, web security and secure access agents.

The vendor also announced Symantec CBX (Carbon Black XDR), which integrates Symantec's prevention, protection, data security and secure web gateway capabilities with Carbon Black's detection and response technology. This aims to enhance visibility, threat detection and response across Broadcom's cybersecurity portfolio.

Broadcom did not disclose information regarding its 2026 roadmap.

Strengths

- **Vertical strategy:** Broadcom supports on-premises endpoint protection management capabilities, including deployment in the air-gapped environments required by highly regulated organizations.
- **Overall viability:** Broadcom is a large, well-funded vendor with a broad cybersecurity and infrastructure product portfolio. The company continues to make incremental enhancements and bug fixes to its endpoint protection products.

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

Cautions

- **Customer experience:** Broadcom primarily targets very large organizations, which limits its ability to effectively sell to, support and build trust with smaller organizations directly. Broadcom supports smaller and midsize organizations through its Catalyst partner program.
- **Innovation:** Broadcom focuses R&D on incremental enhancements and integration of endpoint protection products, with limited emphasis on addressing emerging risks such as shadow AI and enterprise AI adoption.
- **Market responsiveness and track record:** Broadcom's endpoint protection products primarily appeal to existing customers committed to its broader cybersecurity portfolio.

Check Point Software Technologies

Check Point Software Technologies is a Visionary in this Magic Quadrant. It's a vendor headquartered in Tel Aviv, Israel. Check Point Harmony Endpoint is its core endpoint protection product. This vendor supports cloud-delivered, hybrid and on-premises (including air-gapped) management. Check Point Harmony Endpoint is best-suited for organizations invested in Check Point's Harmony suite of workspace security products.

In the past year, Check Point's key product developments included:

- **Unified quarantine management:** Centralizes management of quarantined files and content across endpoint and email security products.
- **AI usage control:** Enhances discovery, risk scoring and control of employee AI usage, leveraging both an endpoint agent and a browser extension.

Check Point's 2026 roadmap includes risk-based, cross-product configuration assessment and remediation, as well as a more unified incident correlation and investigation experience across endpoint, email, browser, mobile and exposure management products.

In the past year, Check Point acquired Lakera, Cyata, Cyclops Security and Veriti to strengthen AI usage control, exposure management and automated security control assessment.

Strengths

- **Market understanding:** Check Point expands its endpoint and workspace security portfolio through acquisitions and organic development, increasing its relevance with target clients.
- **Geographic strategy:** The vendor supports at least one SaaS point of presence in most major geographic regions, including Europe, North America, Asia/Pacific and the Middle East, along with support for on-premises management.
- **Pricing:** Check Point's endpoint protection product pricing is competitive, given its breadth of prevention, protection and data security features compared to other vendors in this Magic Quadrant.

Cautions

- **Product:** Customers report that Harmony Endpoint can slow down protected endpoints due to high system resource consumption, primarily during scans.
- **Market responsiveness and track record:** Check Point's share of the endpoint protection market remains low compared to Challengers and Leaders.
- **Sales strategy:** Based on Gartner client inquiries and Peer Insights feedback, Check Point is rarely included on competitive endpoint protection provider shortlists compared to 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 endpoint protection product. This vendor only supports cloud-delivered (including AWS GovCloud) management. CrowdStrike Falcon is well-suited for organizations looking for mature endpoint protection as part of a broader TDIR-capable product.

In the past year, CrowdStrike's key product developments included:

- **Automated leads:** Detection enhancement that groups related events, indicators and detections into higher-fidelity leads to support security investigations.
- **Charlotte AI agents:** Automation features for executing threat investigations, scoping impact and documenting findings for security analysts.

CrowdStrike's 2026 roadmap includes features for protecting against abuse of legitimate applications, such as remote management tools and enhancements to secure AI assistants like Anthropic Claude, OpenAI Codex, Microsoft Copilot and others. CrowdStrike announced plans for new SaaS points of presence in Saudi Arabia, India and the United Arab Emirates, as well as a sovereign cloud partnership with Schwarz Group to deliver Falcon in an EU-hosted STACKIT environment in the future.

In the past year, CrowdStrike acquired SGNL (identity security), Seraphic Security (secure enterprise browser), Onum (telemetry pipelines) and Pangea (AI application security).

Strengths

- **Customer experience:** Customers rate account management, technical support and managed services as responsive and helpful, resulting in higher overall trust in CrowdStrike.
- **Product strategy:** CrowdStrike has rapidly broadened its offering by leveraging a strong market position and sustained investment in product expansion, all built on a single lightweight endpoint agent and administration console. This approach allows clients to address a wider range of existing and emerging challenges, including identity protection, exposure management, security operations, AI security and more.
- **Product:** CrowdStrike stands out for its lightweight performance impact, mature cloud-based management, deep EDR functionality and the growing maturity of its data security capabilities.

Cautions

- **Pricing:** CrowdStrike remains a premium-priced endpoint protection offering compared to other vendors in this Magic Quadrant.
- **Geographic strategy:** Despite recent announcements, customers and prospects still have limited choices for cloud-hosting points of presence outside Germany and the U.S.

- **Vertical strategy:** Falcon is not suitable for organizations requiring on-premises endpoint protection management, needing to protect air-gapped environments without proxy access, or pursuing full operational and technological sovereignty outside the U.S.

ESET

ESET is a Challenger in this Magic Quadrant. It's a vendor headquartered in Bratislava, Slovakia. ESET PROTECT is the core endpoint protection product. This vendor supports cloud-delivered, hybrid and on-premises (including air-gapped) management. ESET PROTECT is well-suited for small and midsize organizations seeking mature endpoint prevention and protection capabilities.

In the past year, ESET's key product developments included:

- **Enhanced incident graph:** Provides a visual attack timeline and entity relationships view to improve correlation and incident investigation.
- **Linux agent improvements:** Add patch management and network isolation capabilities to reduce the attack surface and improve threat response for Linux endpoints.

ESET's 2026 roadmap includes extended integrations with third-party hybrid mesh firewall providers, as well as response actions for integrated authentication infrastructure providers like on-premises Microsoft Active Directory and Microsoft Entra ID. These enhancements aim to improve identity threat detection and response.

Strengths

- **Customer experience:** Customers rate ESET's technical support as helpful and prompt. Combined with solid protection efficacy and ease of use for common administrative tasks, this results in a positive customer experience for ESET's target audience.
- **Overall viability:** Most of ESET's revenue comes from selling its endpoint protection product to SMB and MSE segments. Its long history and consistent performance underscore ESET's viability in this market.
- **Pricing:** ESET's endpoint protection product pricing is generally competitive compared to other vendors in this Magic Quadrant.

Cautions

- **Product strategy:** ESET focuses R&D on closing gaps, expanding third-party integrations and improving signal correlation. The product currently lacks data security and AI usage control features, which are increasingly demanded by buyers and offered by more vendors in this Magic Quadrant.
- **Market understanding:** In the past year, ESET has followed the market rather than led it, responding slowly to emerging end-user challenges like shadow and enterprise AI adoption.
- **Sales strategy:** Based on Gartner client inquiries and Peer Insights feedback, ESET is rarely included on competitive endpoint protection provider shortlists compared to Leaders in this Magic Quadrant.

Fortinet

Fortinet is a Niche Player in this Magic Quadrant. It's a vendor headquartered in Sunnyvale, California, U.S. FortiEndpoint is the core endpoint protection product. This vendor supports cloud-delivered, hybrid and on-premises (including air-gapped) management. FortiEndpoint is best-suited for organizations invested in the broader portfolio of Fortinet's workspace security products.

In the past year, Fortinet's key product developments included:

- **FortiDLP:** Adds data classification, detection and response features aimed at protecting against data loss to removable media, web applications and AI assistants.
- **Browser security:** Introduces a browser extension for browser-specific hardening, threat protection, data loss prevention and third-party extension management.

Fortinet's 2026 roadmap features tighter integration of FortiDLP into FortiEndpoint for unified protection and data loss prevention through a single endpoint agent and console. Planned enhancements include AI security for visibility and control over locally installed AI assistants, Model Context Protocol (MCP) servers, plug-ins and AI browsers.

In the past year, Fortinet acquired Suridata (SaaS security posture management).

Strengths

- **Vertical strategy:** Fortinet maintains a balanced presence across key industry verticals such as government and manufacturing. The company continues to enhance its on-

premises product, maintaining near-complete feature parity with its cloud-delivered offering.

- **Pricing:** Fortinet's endpoint protection pricing is competitive compared to other vendors in this Magic Quadrant.
- **Overall viability:** Fortinet is a large, well-funded vendor with consistent revenue growth and strong market presence across multiple business lines. Fortinet continues to invest in workspace security technologies, including FortiEndpoint, as evidenced by recent agent unification initiatives aimed at enhancing integrated data protection capabilities.

Cautions

- **Product strategy:** Delays in release of prevention features, like host firewall management for non-Windows systems, hinder Fortinet's product strategy. Full value is realized only within the broader Fortinet ecosystem; stand-alone deployments may face functional limitations for administration and security operations.
- Sales strategy: Based on client inquiries and Peer Insights feedback, Fortinet is rarely included on competitive endpoint protection provider shortlists compared to Leaders in this Magic Quadrant.
- Market responsiveness and track record: Fortinet's share of the endpoint protection market remains significantly lower than that of Leaders or Challengers in this Magic Quadrant.

Microsoft

Microsoft is a Leader in this Magic Quadrant. It's a vendor headquartered in Redmond, Washington, U.S. Microsoft Defender for Endpoint is the core endpoint protection product. This vendor only supports cloud-delivered (including AWS GovCloud) management. Defender for Endpoint is well-suited for organizations looking for mature endpoint protection integrated within a broader workspace security offering, as well as for those invested in the Microsoft security product portfolio.

In the past year, Microsoft's key product developments included:

- **Predictive shielding:** Introduces just-in-time endpoint hardening, aimed at stopping the propagation of detected in-progress attacks like ransomware.

- **Defender deployment tool:** A new tool for Windows and Linux to improve agent onboarding for both modern and legacy operating systems, specifically for customers without Microsoft Intune.

The company also launched Microsoft Defender for Endpoint on the Microsoft Azure cloud in the United Arab Emirates and an additional U.S. government cloud.

The 2026 roadmap includes a new AI agent for malware analysis to improve malware reverse engineering, as well as AI security features for visibility and control over locally installed AI assistants, MCP servers, plug-ins and AI browsers as part of Microsoft Agent 365.

Strengths

- **Product:** Defender for Endpoint stands out for its mature cloud-based management, advanced EDR capabilities, a tight integration with Microsoft's Defender Suite and increasing maturity of data security features.
- **Product strategy:** Microsoft continues to advance its endpoint protection product with enhancements like predictive shielding, demonstrating ongoing commitment to addressing emerging customer requirements.
- **Market responsiveness and track record:** Microsoft holds a significant share of the endpoint protection market and is frequently considered by buyers, especially through the Microsoft 365 E5 bundle.

Cautions

- **Sales execution:** Customers report that Microsoft's licensing model is complex and difficult to understand. Microsoft Defender for Servers is not included in popular packages like Microsoft 365 E3 or E5.
- **Customer experience:** Customers indicate that ease of product use and technical support resolution are variable.
- **Vertical strategy**: Defender for Endpoint does not support on-premises management and is not suitable for organizations pursuing full operational or technological sovereignty outside the U.S.

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 endpoint protection product. This vendor only supports cloud-delivered (including AWS GovCloud) management. Cortex XDR is well-suited for organizations looking for mature and highly customizable endpoint protection as part of a broader TDIR-capable product.

In the past year, Palo Alto Networks' key product developments included:

- **Cortex XDR Endpoint DLP:** Adds data classification, detection and response to protect against data loss to removable media, web applications and AI assistants.
- **Dynamic driver protection:** Enhances visibility into user-to-kernel interactions to detect malicious intent and kernel driver abuse without relying on signatures.

The company also launched new cloud-hosting points of presence in South Africa, Brazil and India.

Palo Alto Networks' 2026 roadmap includes enhanced application control and allowlisting, AI security features for visibility and control over locally installed AI assistants, MCP servers, plug-ins, and AI browsers following its acquisition of Koi Security. Other planned enhancements include AI-assisted configuration management and threat investigation.

In addition to its acquisition of Koi Security (AI security for endpoints), in the past year Palo Alto Networks has also acquired CyberArk (privileged access management), Protect AI (AI application security) and Chronosphere (observability solution).

Strengths

- **Product:** Cortex XDR is valued by customers for effective prevention, protection and EDR features, as well as flexible customization and automation.
- **Product strategy:** Palo Alto Networks invests in mature EDR, prevention and protection feature parity across major operating systems, mature cloud-based management, expanding endpoint DLP capabilities and a strong roadmap for AI security.
- **Innovation:** Recent developments, such as behavioral protection for kernel drivers, enhanced use of control context in exposure prioritization, and built-in AI agents for security operations, demonstrate commitment to addressing emerging end-user requirements.

Cautions

- **Vertical strategy:** Despite offering Broker VM, Cortex XDR does not support on-premises management and is not suitable for organizations that need to protect air-gapped environments without proxy access, or for those pursuing full operational and technological sovereignty outside the U.S.
- **Pricing:** Cortex XDR remains a premium-priced offering; customers often report increasing licensing costs at renewal.
- **Market responsiveness and track record:** The company's share of the endpoint protection 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 Endpoint is the core endpoint protection product. This vendor supports cloud-delivered (including AWS GovCloud), hybrid and on-premises (including air-gapped) management. SentinelOne Singularity is well-suited for organizations looking for mature endpoint protection, as well as threat detection, investigation and response functionality that promotes ease of use.

In the past year, SentinelOne's key product developments included:

- **Lateral movement mitigation:** Enhances blocking of the source IP of devices initiating lateral movement, aimed at reducing mean time to respond.
- **DNS collection:** Extension of collected DNS telemetry to improve endpoint-level detection of DNS tunneling, C2 communication, lateral movement and other threats.

The company launched a new cloud-hosting point of presence in Saudi Arabia and announced a new cloud hosting partnership with Google to deliver SentinelOne's product on Google Cloud Platform.

SentinelOne's 2026 roadmap includes expanded endpoint visibility into network telemetry for improved detection of lateral movement and command and control communications, as well as new endpoint DLP capabilities for protecting against data loss to removable media and web applications.

In the past year, SentinelOne acquired Prompt Security (AI usage control) and Observo AI (telemetry pipelines).

Strengths

- **Product strategy:** SentinelOne's product strategy and security roadmap align with emerging customer needs by enhancing detection and response capabilities, expanding network telemetry visibility and maintaining strong feature parity across supported operating systems. The platform offers robust TDIR integrations with third-party products and plans to add endpoint DLP capabilities, as well as integrate Prompt Security for AI usage control.
- **Market understanding:** The company demonstrates strong understanding of endpoint protection market direction, especially with acquisitions such as that of Prompt Security.
- **Market responsiveness and track record:** SentinelOne's share of the endpoint protection market is larger than most other vendors included in this Magic Quadrant.

Cautions

- **Geographic strategy:** Market penetration outside North America and Europe remains limited, compared to the more geographically diversified competitors.
- **Sales strategy:** According to Gartner client inquiries and Peer Insights feedback, SentinelOne is included on buyers' shortlists less frequently than in previous years.
- **Innovation:** SentinelOne's recent innovations, such as advanced DNS collection and lateral movement mitigation, are less likely to shape the broader endpoint protection market.

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 endpoint protection product. This vendor only supports cloud-delivered management. Sophos Endpoint is well-suited for organizations looking for endpoint protection that is integrated within a broader workspace security offering.

In the past year, Sophos' key product developments included:

- **Sophos Protected Browser:** Introduces a hardened, Chromium-based browser with integrated browser-specific threat protection, secure access and data loss prevention.
- **Sophos AI Assistant:** Adds a built-in AI assistant for alert triage, incident prioritization, threat hunting and analyst guidance.

The company launched Sophos Workspace Protection to secure remote and hybrid workers, and introduced a new cloud hosting point of presence in the United Arab Emirates.

The 2026 roadmap includes a new SIEM offering (from its 2025 Secureworks acquisition) with capabilities for third-party telemetry ingestion, long-term retention, custom data parsing and compliance reporting. It also features a new continuous controls monitoring offering (from its 2026 Arco Cyber acquisition) to assess effectiveness of controls, map them to risk and compliance frameworks, and support executive decision making.

Strengths

- **Operations:** Sophos has strengthened operational execution through increased team size in quality assurance, expanded customer reach and improved global presence, supported by the Secureworks acquisition.
- **Overall viability:** Consistent revenue growth, attribution of most revenue to endpoint protection product sales, and long-established market presence indicate continued commitment to endpoint protection offerings.
- **Pricing:** Sophos's endpoint protection product pricing is generally competitive compared to other vendors in this Magic Quadrant. Its per-user licensing model is attractive to organizations where employees have multiple devices.

Cautions

- **Vertical strategy:** Sophos does not offer on-premises management capabilities, making its product unsuitable for organizations requiring data sovereignty outside of its supported points of presence.
- Sales strategy: Based on client inquiries and Peer Insights feedback, Sophos is rarely included on competitive enterprise endpoint protection provider shortlists compared to other Leaders in this Magic Quadrant.

- **Innovation:** Recent R&D focused on improving endpoint agent performance and adding AI assistance for alerts summarization, addressing existing product gaps rather than delivering innovation.

Trellix

Trellix is a Niche Player in this Magic Quadrant. It's a vendor headquartered in Frisco, Texas, U.S. Trellix Endpoint Security Solutions is the core endpoint protection product. The vendor supports cloud-delivered (including AWS GovCloud), hybrid and on-premises (including air-gapped) management. Trellix Endpoint Security Suite is well-suited for organizations requiring comprehensive on-premises endpoint protection with granular customization options.

In the past year, Trellix's key product developments included:

- **Ransomware detection:** Combines behavioral rules with bait files for deception to improve ransomware detection efficacy and mitigation.
- **Enhanced forensic data collection in a single agent:** Adds actions for collecting command shell history, PowerShell history, memory acquisition, and file and directory records to support investigations.

The company's 2026 roadmap includes further integration of on-premises product components, such as common UX design, alert management, search and the management plane. The goal is to improve the overall usability of the Trellix portfolio. Planned enhancements also focus on accelerating organizationwide ransomware response earlier in the attack chain.

Strengths

- **Geographic strategy:** Trellix offers multiple SaaS points of presence in key markets, including North America, Europe, Australia, Singapore and India, and provides multilingual support to global customers.
- **Vertical strategy:** The company supports and invests in improving its on-premises management offering, including deployments in air-gapped environments required by highly regulated organizations.
- **Pricing:** Trellix's endpoint protection pricing is generally competitive compared to other vendors in this Magic Quadrant.

Cautions

- **Product strategy:** Trellix focuses on closing product gaps through feature parity, improved detection and customizable alerting, remote shell, and configurable data retention for its on-premises offering. The product still lacks AI discovery and usage control features increasingly sought by buyers and offered by more vendors in this Magic Quadrant.
- **Market responsiveness and record**: Based on Gartner's assessment of market share, seat count estimates and client inquiries, Trellix's share of the endpoint protection market has declined relative to leading providers in this Magic Quadrant.
- Sales strategy: Based on client inquiries and Peer Insights feedback, Trellix is rarely included on competitive endpoint protection provider shortlists compared to Leaders in this Magic Quadrant.

TrendAI

TrendAI is a Leader in this Magic Quadrant. It's a vendor headquartered in Tokyo, Japan. TrendAI Vision One Endpoint Security is the core endpoint protection product. This vendor supports cloud-delivered, hybrid and on-premises (including air-gapped) management. TrendAI Vision One is well-suited for organizations looking for mature endpoint protection integrated as part of a broader workspace security offering.

In the past year, TrendAI's key product developments included:

- **Recommended exclusions:** Enhanced exclusion management capabilities, featuring recommendations based on endpoint context, aimed at reducing operational overhead.
- **Enhanced data security**: Adds a data security sensor that classifies and tracks movement of sensitive data across TrendAI's protected environment.

The vendor also launched new cloud-hosting points of presence in Canada, the U.K. and South Africa.

TrendAI's 2026 roadmap includes vulnerability assessment enhancements designed to provide early access to unpublished endpoint vulnerability information and threat intelligence from TrendAI. Additionally, the roadmap features enhanced correlation of telemetry, security events, context and intent to improve threat detection fidelity.

Strengths

- **Product strategy:** TrendAI continues to invest in its endpoint protection product and supports a broad range of operating systems, including legacy versions. Recent enhancements, such as data security, attack path mapping and adaptive protection, align with emerging buyer requirements. The roadmap focuses on reducing attack surface through hardening rules, browser-based prompt injection protection and AI usage discovery, further strengthening its position in the endpoint protection market.
- **Product:** TrendAI's strong prevention capabilities, cloud-based, hybrid and on-premises management, broad range of OS support, and workspace security are well-regarded by customers.
- **Pricing:** TrendAI's endpoint protection product pricing is generally competitive compared to other vendors in this Magic Quadrant.

Cautions

- **Sales strategy:** Recent customer feedback indicates that TrendAI's credit-based licensing model is hard to interpret, noting limited transparency around how credits are distributed across the vendor's broader product portfolio.
- **Overall viability:** In recent years, TrendAI's revenue growth in the endpoint protection market has been slower than that of other Leaders in this Magic Quadrant.
- **Customer experience**: Recent customer feedback and third-party testing results indicate that high alert volumes and resource-intensive scanning can degrade end-user experience. Some customers also reported support quality issues in the analysis period.

WithSecure

WithSecure is a Niche Player in this Magic Quadrant. It's a vendor headquartered in Helsinki, Finland. WithSecure Elements XDR is the core endpoint protection product. This vendor supports cloud-delivered, hybrid and on-premises management. WithSecure Elements XDR is well-suited for small and midsize organizations, especially those headquartered in Europe.

In the past year, WithSecure's key product developments included:

- **Attack path visualization:** New threat simulation capabilities to help visualize potential attack paths, aimed at improving the prioritization of suggested remediation actions.
- **Integration enhancements:** An expanded library of prebuilt endpoint- and identity-related integrations and APIs, aimed at enabling integration with third-party security orchestration tools.

WithSecure's 2026 roadmap includes AI-augmented threat investigation capabilities aimed at reducing operational overhead through automation, summarization of key findings and recommended response actions. It also features enhancements to software inventory and patch management capabilities, aiming to include SaaS application inventory, usage and cybersecurity assessment.

Strengths

- **Market understanding:** WithSecure's understanding of the endpoint protection market's dynamics and competitors helps the company concentrate its efforts on helping organizations in Europe meet their regulatory, product and service needs.
- **Vertical strategy:** WithSecure announced plans to make its offering available on the AWS European Sovereign Cloud (ESC) in Germany. This move aligns with its target audience and is attractive to organizations in Europe pursuing data and operational sovereignty objectives.
- **Pricing:** WithSecure's endpoint protection product pricing is competitive compared to other vendors in this Magic Quadrant.

Cautions

- **Product Strategy:** WithSecure's latest updates, including threat simulation to visualize possible attack paths and enhanced APIs, primarily address product deficiencies rather than drive innovation, making them unlikely to significantly influence the broader enterprise endpoint protection landscape.
- **Market responsiveness and track record:** WithSecure's share of the endpoint protection market remains lower than that of Leaders or Challengers in this Magic Quadrant.
- **Operations:** WithSecure remains a comparatively small company with less-diversified operations and geographic presence than Leaders in this Magic Quadrant, particularly

following its recent divestment of the cybersecurity consulting business and resulting reduction in headcount.

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

- Cisco
- Cybereason

Inclusion Criteria

Gartner did not define any exclusion criteria for this research.

To qualify for inclusion in this Magic Quadrant, providers had to meet the definition of the endpoint protection market and satisfy all inclusion criteria using their core endpoint protection product as of the start of Gartner’s research and survey process (on 9 February 2026). 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 and attack surface reduction controls, as well as operating system and endpoint application vulnerability assessment.
- The solution embeds 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 endpoint protection vendors maintain.
- 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 (MDR) or co-managed security monitoring.
- A vendor must sell endpoint protection 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 or MRG Effitas) for security efficacy within the 24 months before 9 February 2026.
- A vendor must have over 10 million endpoints protected and actively under management in production using its endpoint protection as of 9 February 2026, 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. Marketing execution is not a rated criterion, as it is not relevant to buyers in this market.

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 (May 2026)

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. Marketing strategy and business model are not rated criteria, as they are not relevant to buyers in this 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 (May 2026)

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 mature 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 endpoint protection 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 endpoint protection for better defense-in-depth.

Context

Organizations primarily use endpoint protection 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 endpoint protection with broader workspace security platforms and TDIR-capable products (such as integrated security operations center solutions and SIEM offerings) to reduce operational complexity and help optimize cybersecurity technology stacks.

Gartner Magic Quadrant vendor surveys reveal that over 60% of enterprise endpoints are protected by cloud-delivered endpoint protection products that include modern behavioral protection capabilities. The mature endpoint protection market, evolving threats and the need for more effective security operations have started to shift buyer interest to other market categories. An estimated 25% of organizations purchase adjacent TDIR-capable products (such as ISOC and SIEM) from their endpoint protection provider to achieve better efficiency and optimize cost, compared to manually integrating otherwise disjointed controls.

All vendors in this research offer cybersecurity AI assistant capabilities as part of their endpoint protection 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 endpoint protection 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 is a mature market in which buyers increasingly select providers based on vendor trust and the vendor's ability to deliver on broader cybersecurity outcomes (see **Leverage Gartner's Vendor Trust Index in Your Next Cybersecurity Purchase**). Gartner estimates the endpoint protection market at approximately $18 billion in 2025, growing at approximately 14% per year (see **Market Share: Enterprise Software,**

Worldwide, 2025). Notably, Microsoft and CrowdStrike hold an estimated 40% of the endpoint protection market share. Gartner forecasts that the market will expand at a compound annual rate of approximately 11% through 2028, reaching a size of $26 billion based on constant currency (see **Forecast: Information Security, Worldwide, 2024-2030, 1Q26**).

Cybersecurity Rationalization

In 2026, most cybersecurity leaders aim to rationalize strategic cybersecurity vendors and simplify their cybersecurity tool stack to reduce complexity and optimize costs. This trend enables established endpoint protection providers to incrementally expand their product footprint during contract renewals, often displacing or augmenting adjacent products and services in markets such as exposure assessment platforms, security information and event management, identity threat detection and response, MDR and others. However, this also increases pressure on vendors that are narrowly focused on endpoint protection or are not seen as potentially strategic providers by buyers. Recent market acquisition and merger activity illustrates this trend, as providers seek to expand their capabilities and service offerings to meet evolving cybersecurity needs. There were 400 reported mergers of cybersecurity companies in 2025, and the top 10 cybersecurity enterprise software security vendors continue to grow their revenue (see **Optimize Strategic Cybersecurity Vendors with Gartner's 4-Pillar Evaluation Framework**).

Emerging Sovereignty Requirements

Heightened geopolitical instability is driving stronger technological sovereignty requirements, with increasing regulatory pressure and expectations for enforcement. Buyers in industries and geographies susceptible to geopatriation are revisiting their data, operational and technological sovereignty objectives, which prompts them to evaluate regional data hosting, on-premises management options, multitenant strategies for operations across multiple jurisdictions, and generally reducing reliance on foreign cybersecurity providers. In response, several endpoint protection providers have recently expanded and announced plans to further expand their cloud-hosting SaaS points of presence to new regional clouds, particularly in Middle Eastern and Asia/Pacific countries, following prior efforts to expand coverage within the European Union. (See **Europe Context: Magic Quadrant for Endpoint Protection.**)

AI Impacts on Endpoint Protection

Impact of Shadow AI, AI Browsing, Enterprise AI Adoption

The rapid adoption of various forms of AI by organizations is outpacing the speed of cybersecurity control planning, deployment and fine tuning, and has already resulted in heightened threat of data loss to AI services on corporate endpoints and beyond. Employees and developers increasingly use AI assistants and agents outside formal controls, increasing the attack surface and the risk of data leakage, credential exposure, and unmanaged data flows beyond the visibility of traditional endpoint and other detection approaches. The real issue is that the loss of sensitive data to AI services can be irreversible and untraceable, and organizations may never recover lost data (see **Discover and Manage 3 AI Blind Spots: Embedded AI, Shadow AI and AI Browsing**).

In response to these risks, most endpoint protection vendors are introducing AI discovery and usage control capabilities, either through organic development or acquisitions. Key use cases that are starting to emerge include:

- **Employee shadow AI:** Discovery, risk scoring and control of unsanctioned AI usage by employees, including AI browsing agents (OpenAI ChatGPT, Anthropic Claude), AI browsers (Perplexity Comet, OpenAI ChatGPT Atlas), and computer use agents (Anthropic Claude Cowork, Microsoft Copilot Cowork, Meta Manus, OpenClaw) on corporate-managed devices without approval. Employee shadow AI usage can lead to sensitive data exposure, regulatory noncompliance, and loss of intellectual property data to AI services.

- **Developer shadow AI:** Discovery, risk scoring and control of unsanctioned AI usage by developers, including the use of AI coding assistants (Claude Code, GitHub Copilot, Cursor), local LLMs, MCP servers, and external AI APIs without approval. Developer or citizen developer use of shadow AI can lead to leakage of source code and embedded secrets (API keys, credentials), as well as licensing or IP violations introduced by AI-generated code.

Impact of Cybersecurity AI Assistants on Endpoint Protection Management

Vendors are increasingly investing in generative and agentic AI to improve product usability, but adoption by security teams remains limited. This is especially true considering that most midsize organizations do not have mature security operations or exposure management processes, which vendors often aim to optimize or automate with

AI assistants. As a result, cybersecurity leaders, especially in less-mature cybersecurity organizations, continue to prioritize MDR services over AI assistants for outcome delivery.

According to Gartner survey data, only a minority of organizations currently use these capabilities for threat detection, incident response or policy administration. [1] Today's generative AI features primarily focus on administrative assistance, such as incident summarization and documentation discovery, while agentic AI roadmaps target automation of repetitive tasks like alert triage, automated investigation, query or custom playbook creation, malware analysis, response planning and others. Realizing meaningful value from these capabilities requires deep product and workflow integration, which remains challenging. Buyers evaluating AI assistant features must focus on measuring hard operational efficiency gains and improvements in existing metrics before investment.

Product Evolution

In 2026, most endpoint protection vendors show limited innovation or enhancements to core endpoint protection capabilities. Instead, they are prioritizing the addition of adjacent product capabilities that aim to address emerging buyer requirements, such as AI discovery and usage control, integrated endpoint and enterprise data loss prevention, browser security, application abuse prevention, exposure assessment, proactive and just-in-time endpoint hardening. They are also enhancing agentic AI features that aim to augment security operations teams through automation. While these new capabilities are necessary for addressing emerging threats, it also means that old gaps remain unaddressed for longer, leading to significant differentiation in products across several key capabilities, which, among others, include:

- Near-real-time endpoint telemetry collected for behavioral analysis and protection
- Resource consumption and performance impact by endpoint agents
- Depth of customization for various administrative functions and detection logic
- Supported controls for non-Windows and legacy operating systems

Cybersecurity leaders selecting endpoint protection products should use **Critical Capabilities for Endpoint Protection** to assess functionality against specific organizational use cases or build custom use cases that suit their needs.

⊕ Evidence

⊕ Evaluation Criteria Definitions