



IDC MarketScape

IDC MarketScape: Worldwide Modern Endpoint Security for Enterprises 2026 Vendor Assessment

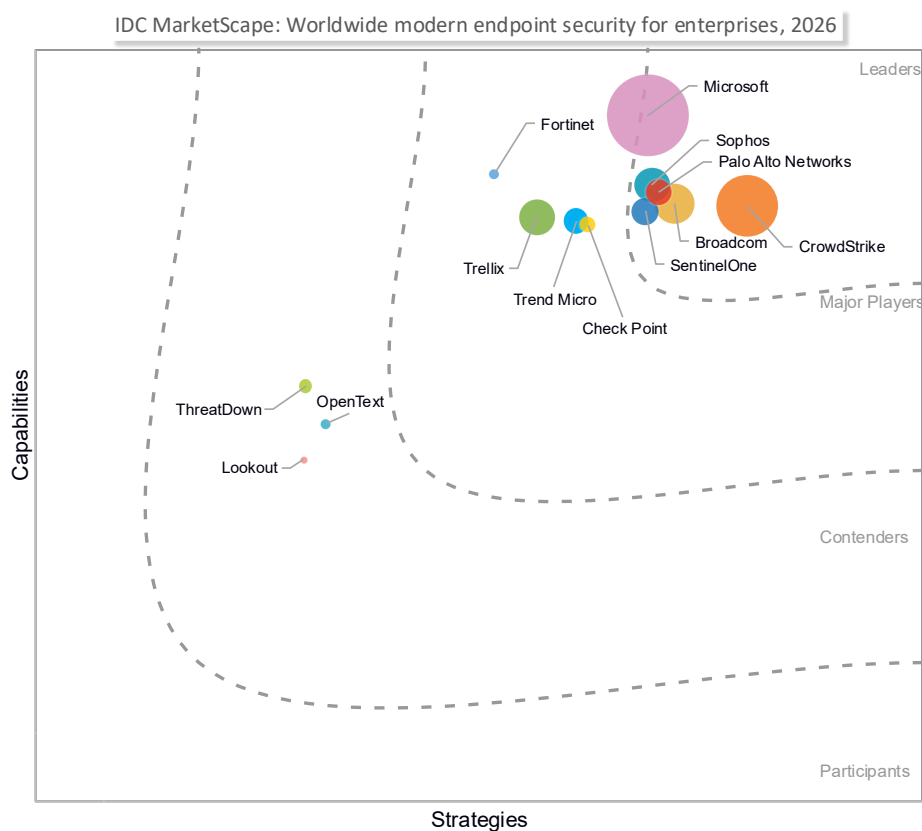
Mark Child

THIS EXCERPT FEATURES SOPHOS AS A LEADER

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape: Worldwide modern endpoint security for enterprises vendor assessment



Source: IDC, 2026

Please see the Appendix for detailed methodology, market definition, and scoring criteria.

ABOUT THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Worldwide Modern Endpoint Security for Enterprises 2026 Vendor Assessment (Doc # US54123526).

IDC OPINION

The legendary Italian defender Paolo Maldini once said, "If I have to make a tackle, then I've already made a mistake," meaning: read the game, know the opponent, anticipate what is coming even as a play develops, and be in the right place at the right time to stop an attack from unfolding. This 2026 IDC MarketScape found a comparable philosophy underpinning much of the development in the modern endpoint security (MES) space. The volume, velocity, and variety of attacks are such that security teams cannot hope to cope without automation, orchestration, and, increasingly, autonomous actions taken by their endpoint security platform. Even without a managed service wrapper, the solution must be able to take real-time actions, at scale, on behalf of defenders, blocking threats and bringing humans into the loop only when higher-level decisions are required.

AI is playing a significant part in this. All the vendors profiled for their enterprise offerings in this IDC MarketScape make extensive use of AI across their platforms, combining on-device static engines for real-time detection and prevention with cloud-based AI intelligence to expand contextual awareness and improve detection of emerging threats. Neither approach on its own provides sufficient protection against threats; combined, they complement each other.

The AI buck does not stop there. Most endpoint security vendors have been using neural networks for years to carry out extensive and deep telemetry analysis, delivering anomaly detection and pattern identification. Behavioral engines use machine learning (ML) to develop rich models of baseline states and behaviors and then track anomalous behavior, looking for signs of malicious activity such as lateral movement or memory exploits. These can help expose advanced threats or living-off-the-land activity that harnesses fileless attacks or emerging zero-day threats. In the advent of Mythos and other frontier AI models accelerating vulnerability discovery, these AI-augmented defenses become vastly more important. Predictive AI engines aim to further shift the needle and use complex analysis to project where or how emerging attacks could impact an organization and enable them to proactively harden their infrastructure.

All the aforementioned AI augmentation methods enhance the capabilities of endpoint security platforms; no single approach provides sufficiently broad, deep, rapid, and reliable coverage. A layered approach is paramount, and the research conducted for this IDC

MarketScape found that among enterprise-grade endpoint security platforms, such approaches have been broadly and effectively adopted.

AI is not the be-all and end-all of endpoint security evolution, however. As noted previously, frontier AI models are having a growing impact on enterprise security, and this is driving greater attention to software agent hardening, patch management, device vulnerability management (DVM), and more. How an endpoint security solution delivers those capabilities or integrates with other security solutions to deliver them is increasingly important for security and operational efficiency.

Two more significant dimensions are worth noting. First, mobile security and mobile threat defense (MTD) are increasingly significant as mobile devices have become operational infrastructure for so many users and business processes. This iteration of the MES IDC MarketScape includes a pure-play mobile endpoint security specialist worthy of serious consideration as a complementary deployment along with the core enterprise endpoint security platform. Second, taking that operational interface a step further, more organizations are looking at the browser as a key layer of their enterprise security stack. While some go as far as to deploy a standalone enterprise browser solution to secure this operational technology, how endpoint security solutions support various browser policy controls can also be an important consideration for security buyers, and this was also tracked in the IDC MarketScape.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

Vendors included in this evaluation met the following criteria:

- Offers a software product or products that deliver endpoint protection platform (EPP) capabilities, endpoint detection and response (EDR) capabilities, or combined EPP and EDR capabilities according to the description included in the Market Definition section (If the vendor offers products that are promoted as extended detection and response (XDR), they qualify if EDR capabilities are fully included in the XDR products.)
- Supports end-user devices that run the latest general availability (GA) version of Windows and macOS
- Had product sales in calendar year 2025 to the enterprise segment (2,500+ employees worldwide) of at least \$75 million

ADVICE FOR TECHNOLOGY BUYERS

Modern endpoint security vendors cannot stand still against a threat landscape that never does — and neither can the organizations buying from them. In the two years since IDC last assessed this market, your digital footprint, workforce model, regulatory obligations, and

cyber-risk tolerance have almost certainly shifted, and AI has begun to reshape both the attack surface and the defensive toolset. To assume that your incumbent MES product, or combination of products, remains the best fit is to forgo the opportunity either to make a positive change or to confirm that change is unnecessary. To guide your evaluation, IDC offers the following advice:

- **Fools rush in:** Do not let urgency substitute for diligence. Endpoint security decisions are often triggered by an incident, a renewal deadline, or a compelling discount, and each of those creates pressure to compress evaluation into a pricing exercise. Resist it. Price is the easiest variable to compare and the least predictive of outcome. Assess instead how the offering fits the environment you actually run: legacy operating systems (OSs), OT and IoT endpoints, virtual desktops, unmanaged and BYOD devices, and the identity, SIEM, cloud, and ITSM tools the platform must exchange signals with. Interrogate the functional road map, and ask which capabilities are shipping today, which are in beta, and which are aspirational. Examine the support and delivery model, including what the vendor performs directly versus what it delegates to channel partners in your regions. Then insist on testing — in your production environment, against your telemetry, with your own staff at the console. A vendor that resists a rigorous proof of value is telling you something worth hearing.
- **AI road map:** Press hard on the AI road map, not the AI feature list. Every vendor in this market now markets AI, so the question is no longer whether AI is present but whether it is applied where it changes outcomes. AI is simultaneously widening the attack surface — AI-assisted social engineering, faster exploit development, agents and copilots operating on the endpoint with delegated credentials — and accelerating the rate at which your own technology and business processes change. Ask how the vendor uses AI to compress detection and response time, to triage and contextualize alerts, and to lift the effective skill level of your analysts rather than simply generating more findings for them to read. Ask equally how it secures AI on the endpoint: visibility into local models, agent activity, and data leaving the device through AI tooling. Then ask the unglamorous questions. What data trains and grounds the models? Where does inference run? How are false positives governed, and what recourse do you have when automated action is wrong?
- **Support and relationships matter:** Treat support and vendor responsiveness as product capabilities. Across the customer interviews conducted for this study, one attribute that surfaced consistently among satisfied customers was responsiveness: vendors described as fast, flexible, and proactive, with escalation paths to human operators who already understood the environment. As one customer stated: By the time we knew about the incident, our vendor had already resolved it. That dynamic is more visible in smaller organizations that lean on the vendor as an extension of the team, but enterprises should not file it away as an SMB concern. Large environments

generate difficult edge cases, complex migrations, and volumes of incidents where minutes of delay compound. Evaluate the relationship as deliberately as the technology: named technical contacts, documented response and escalation commitments, and coverage across your operating hours and geographies. In an increasingly regulated world with mandated incident reporting, these will be more and more important.

- **Telemetry, cost, and control:** Establish where your telemetry lives, what it costs, and who controls it. Endpoint data has become a high-value input to enterprise detection, feeding SIEM, XDR, identity analytics, and the AI-driven correlation increasingly sitting above all of them. That makes data questions strategic rather than administrative. Determine what the platform collects and what it discards, how long it is retained at full fidelity versus summarized, and the cost of retention beyond the default. Data and egress charges can be a source of unpleasant surprises long after signature. Confirm that you can export your own telemetry in a usable form, on your schedule, without a professional services engagement, and understand what happens to it if you leave. Establish where it is stored and processed, and whether that satisfies your sovereignty and regulatory obligations. Finally, be clear about the vendor's use of your data for model training and threat intelligence, what control you retain over it, and what you get in return.

VENDOR SUMMARY PROFILES

This section briefly explains IDC's key observations resulting in a vendor's position in the IDC MarketScape. While every vendor is evaluated against each of the criteria outlined in the Appendix, the description here provides a summary of each vendor's strengths and challenges.

Sophos

Sophos is positioned in the Leaders category of the 2026 IDC MarketScape for worldwide modern endpoint security for enterprises.

Sophos secures over 600,000 organizations globally, spanning large enterprises, SMBs, and diverse sectors, supported by 350+ third-party integrations and roughly 1,000 cybersecurity specialists and researchers across Sophos X-Ops, SophosLabs, Secureworks CTU, and Sophos Managed Risk. The company completed its acquisition of Secureworks and has integrated Taegis XDR technology into Sophos Fusion, expanding its open ecosystem; full technical integration of Taegis capabilities into Sophos XDR and MDR, along with a unified XDR/MDR user experience, is underway and will be completed in late 2026. Sophos Fusion is the unified management console for all endpoint, server, mobile, and cloud workloads, supporting Windows, Linux, macOS, and mobile devices, using the same agent and console whether managed by the customer or by Sophos MDR.

The Sophos Endpoint platform includes EPP, EDR, XDR, and ITDR offerings, as well as DLP, web protection/control, application/peripheral control, antiexploit, anti-ransomware, DNS protection, and ZTNA. Sophos AI Defense for AI tool governance is now in the vendor's Early Access Program (EAP).

Sophos Endpoint supports Windows, macOS, Linux, mobile (iOS/Android), and cloud/virtual workloads and can be deployed as SaaS, with on-premises and hybrid console options. It has a single agent for all modules and supports third-party telemetry and integrations.

Sophos emphasizes strong, up-front protection through preconfigured, best practice defaults that require no tuning, pointing to its handling of the May 2026 JDownloader supply chain attack, in which AI-generated malware with no known signature was blocked automatically at runtime through anti-exploitation and behavior-based detection. Independent testing supports this: Sophos Endpoint has been evaluated by SE Labs, AV-Test, AV-Comparatives, and MITRE ATT&CK Evaluations, including enterprise detection rounds covering groups such as DPRK, CL0P, LockBit, Scattered Spider, and Mustang Panda.

Agent hardening includes vulnerable driver protection, Event Integrity Protection against ETW tampering that safeguards the Windows event telemetry pipeline so attackers cannot blind the agent, optional Kernel Driver Monitoring for early warning on suspicious driver activity, Tamper Protection, Service Integrity Monitoring, Self-Repair, and Cloud Native Re-Install/Remote Install Repair. Sophos does not use Intel TDT; it assessed the potential value of TDT in 2024 but has not integrated it.

Sophos Fusion provides a unified dashboard for all modules, with health scores, policy status, and misconfiguration detection through the Account Health Check, which offers one-click remediation and lets customers compare scores against similarly sized peers over time. Alerts and cases are prioritized, with AI-generated summaries and recommended actions. Live response terminal, forensic log collection, and isolation are available, and policy management is granular, with default best practice settings enabled out of the box.

Web protection and control block malicious and inappropriate sites and downloads using deep learning URL security models, backed by category-based Web Control policies and Sophos threat intelligence; DNS protection adds another layer. Sophos Email Security applies deep learning natural language processing to catch phishing and impersonation attempts, complemented by download reputation checks, Man-in-the-Browser protection, and automatic endpoint isolation through Synchronized Security.

CryptoGuard monitors files for malicious encryption, blocks local and remote ransomware, and automatically rolls back affected files to their pre-encryption state without relying on Volume Shadow Copy, which ransomware can itself compromise; Master Boot Record protection is included. The approach is technique based rather than signature based.

Sophos Mobile Threat Defense is natively developed and can be deployed through Sophos Fusion or a third-party MDM, including Microsoft Intune, Jamf, Citrix, Google Endpoint Management, Ivanti, and Omnisia Workspace ONE. It protects against network-based threats such as reconnaissance and man-in-the-middle attacks; flags unhealthy device conditions such as jailbreaking, missing encryption, and outdated OS or app versions; detects abnormal or malicious application behavior; defends against phishing; enforces application allow/denylists; flags data privacy risks in third-party apps; and generates regulatory-specific alerts and direct user warnings.

A device exposure dashboard highlights out-of-date devices and OS versions to prioritize remediation, but this is not a full patching solution. Patch management covers operating system patches only for Windows, macOS, and Linux. OS patch deployment is not automated from the platform; it is achieved through the Live Response functionality available with EDR, XDR, and MDR licenses, and it does not require devices to be on-net or rely on a CDN architecture.

AI is infused throughout the platform: case summaries drawn from MDR frontline analyst workflows, natural language threat hunting that produces executable queries without complex syntax, process lineage visualization, script de-obfuscation, and reputation enrichment. A proprietary scoring algorithm draws on more than 50 factors, including CISA's known exploited vulnerability data, to reprioritize risk; Sophos cites a case where a CVSS 6.2 vulnerability was elevated to a 10 based on unusual port combinations and network anomalies. Sophos Intelix brings X-Ops threat intelligence into Microsoft 365 and Security Copilot through natural language chat at no additional charge to Copilot users. AI models are refined using data from MDR operations and threat intelligence across SophosLabs, Secureworks CTU, and Intelix, and Secure AI, still on the road map, will add AI tool discovery and governance.

Strengths

- Strong up-front protection across web, exploit, and ransomware vectors, validated across multiple independent testing programs, which reduces analyst workload and alert volume
- Unified, open platform with deep third-party integration, native ITDR, and automation spanning SOAR, playbooks, and an AI assistant
- Democratized, out-of-the-box security for organizations of all sizes, backed by global reach, embedded threat intelligence, and expanding Secureworks-powered XDR/MDR capability

Challenges

- Patch management is limited to OS-level patching for Windows, macOS, and Linux; third-party application patching is not offered natively, and deployment is not automated from the platform.
- Mobile threat defense and agent hardening are natively built and detailed, but Sophos has chosen not to adopt Intel TDT.
- Full integration of Secureworks/Taegis technology into Sophos XDR and MDR is still underway and will be completed in late 2026.

Consider Sophos when

- SMBs to large enterprises are seeking out-of-the-box, protection-first endpoint security with minimal tuning.
- Organizations need a unified, open platform with strong third-party integration, native identity threat detection, and automation.
- Customers with limited security staff or no dedicated CISO function are seeking democratized, AI-augmented security and reporting.

APPENDIX

Reading an IDC MarketScape graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here and now. Under this category, IDC analysts will look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis or strategies axis indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the market share of each individual vendor within the specific market segment being assessed.

IDC MarketScape methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the

range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information and end-user experiences in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behavior and capability.

Market definition

Modern endpoint security products protect personal computing devices (e.g., workstations/PCs and laptops) and mobile devices (e.g., smartphones and tablets) from cyberattacks through the detection of malicious code and behaviors present or operating within the devices and then facilitate a response (e.g., block, remove, or isolate).

With increasing commonality, modern endpoint security products combine detection and response mechanisms differentiated based on elapsed time and human involvement. Endpoint protection platforms (EPPs) reach detection verdicts and initiate mitigating responses in real time and autonomously (i.e., without human involvement). Endpoint detection and response (EDR) is the second stage of detection and mitigating response for cyberattacks that have evaded EPP detection. With EDR, the time to reach detection verdicts and initiate responses can span minutes to days. How fast the cyberattack unfolds, its sequence of steps, and its sophistication and uniqueness are factors that affect the elapsed time in detection and response. Automation and predefined workflows assist in reducing the elapsed time. Security analysts (humans) are typically involved, at a minimum, to validate detections and/or authorize responses.

For many modern endpoint security vendors, EDR products have evolved into extended detection and response (XDR) products that, at a base level, ingest and correlate detection-supporting telemetry from endpoints and other sources (e.g., firewalls/UTMs, authentication servers, email gateways, secure web gateways, and network taps) and prepare and apply mitigating responses at endpoints and other security control points.

Modern endpoint security suites may also accomplish more than detect malicious code and behaviors and initiate mitigating responses. They may include capabilities that thwart threats during the initial stages of an attack and reduce the endpoint's attack surface area and exploitability. Initial-stage attack prevention and surface area reduction capabilities vary by vendor and include, but are not limited to, DNS and URL filtering; hardening of device, OS, and application controls; file sandboxing, sanitization, and file integrity monitoring; browser isolation and browser policy controls; application allowlisting; antiphishing; DLP and data-at-rest encryption; device vulnerability and patch management; policy configuration of host-based firewall and intrusion detection functionality; and endpoint-hosted deception.

Related research

- *Market Forecast: European Endpoint Security Forecast, 2026–2030* (IDC #EUR153620326, August 2026)
- *IDC Survey: Modern Endpoint Security — Western European Markets, 2026* (IDC #EUR254663026, July 2026)
- *Worldwide Corporate Endpoint Protection Software Market Share, 2025* (IDC #US53713926, June 2026)
- *Securing the Agentic Enterprise: Part 1 — Updating IDC's Cybersecurity Capabilities Assessment Framework for the AI Age* (IDC #EUR154585226, June 2026)
- *Securing the Agentic Enterprise: Part 2 — Assessing the Impact of Agents on Key Security Domains* (IDC #EUR154585326, June 2026)
- *IDC Survey: IDC's Worldwide Modern Endpoint Security Survey, April 2026* (IDC #EUR254526826, May 2026)
- *IDC MarketScape: Worldwide Extended Detection and Response Software 2025 Vendor Assessment* (IDC #US52997325, September 2025)

Synopsis

This IDC study represents a vendor assessment of modern endpoint security offerings for enterprises in 2026, through the IDC MarketScape model.

"The defining shift in this iteration of the IDC MarketScape is that prevention has moved from aspiration to architecture. Attack volume, velocity, and variety now exceed what any security team can meet by hand, so enterprise endpoint platforms are increasingly expected to act autonomously and in real time, blocking threats at scale and bringing analysts in only for higher-order decisions. AI is doing much of that work, but no single method is sufficient; the strength lies in layering complementary engines," says Mark Child, associate research director, security and trust at IDC. "Buyers should press on exactly that point. Ask not whether a vendor has AI, but where it is applied, what it decides without you, and how its road map answers frontier models that are accelerating vulnerability discovery. Then insist on testing in your own environment before committing, because a platform acting on your behalf at machine speed has to earn that trust on your estate, not the vendor's."

ABOUT IDC

International Data Corporation (IDC) is the premier global market intelligence, data, and events provider for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight help IT professionals, business executives, and the investment community make fact-based technology decisions and achieve their key business objectives.

Global headquarters

One Beacon Street
Suite 33100
Boston, MA 02108
USA
508.872.8200
X: @IDC
blogs.idc.com
www.idc.com

Copyright and trademark notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, and web conference and conference event proceedings. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit idc.com/about/offices. Please contact IDC at customerservice@idc.com for information on additional copies, web rights, or applying the price of this document toward the purchase of an IDC service.

Copyright 2026 IDC. Reproduction is forbidden unless authorized. All rights reserved.