XDR Is Now WCP. SMBs Get It Through MSPs.

Why Gartner retired a category, what replaced it, and what it means for the companies that never had a security team

EDAO Group · November 2026

The short version

For five years the cybersecurity industry sold "XDR" as the answer for organizations that could not run a security operations center. In 2026 Gartner stopped treating XDR as a market. In its place it defined the **Workspace Cybersecurity Platform (WCP)**: modular, preintegrated protection for the endpoints, identities, applications and data of digital workers.

That definition was written for enterprises with security teams. Small and midsize businesses have none. The only viable way for an SMB to get WCP-grade protection is through a managed service provider that can operate it. This paper explains what changed, why it matters more to SMBs than to anyone else, and what an SMB or an MSP should now ask of a security provider.

What Gartner changed

Three Gartner publications, in sequence, tell the story.

Date	Gartner publication	What it says
24 October 2025	*Embrace Workspace Security to Prepare for the End of XDR*	Security leaders no longer see stand-alone XDR as differentiating. Endpoint vendors keep adding controls and SIEM keeps getting more capable, so XDR evolves into a more integrated set of technologies
20 July 2026	*Market Overview for Workspace Cybersecurity Platforms* (Mirolyubov and Firstbrook)	Defines the WCP category. Per vendor summaries of the report, WCPs have replaced Gartner's coverage of the XDR market, and XDR became a feature within WCPs
5 June 2026	*Hype Cycle for Security Operations, 2026*	Plots XDR as moving toward obsolete before reaching the plateau, as large platform vendors absorb it as a feature layer

The reasoning is consistent across the three. XDR promised to correlate detections across endpoint, identity, email and cloud. Once every serious endpoint vendor shipped those controls natively, correlation stopped being a product and became a property of the platform. Gartner's answer was to stop grading the correlation engine and start grading the platform.

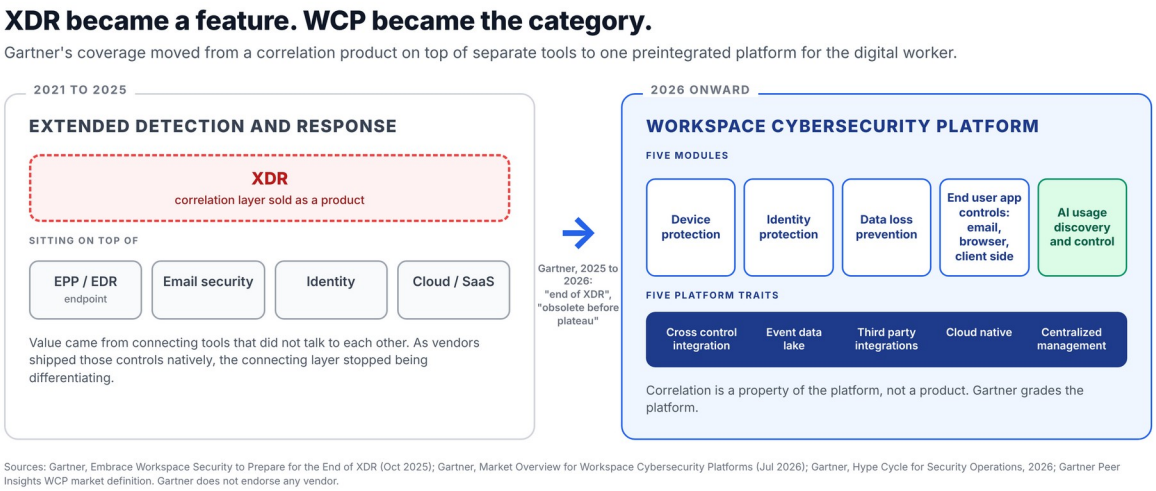

Figure 1. XDR became a feature of the platform; the Workspace Cybersecurity Platform became the category Gartner grades.

A note on precision: Gartner did not declare XDR dead. Forrester still publishes an XDR Wave, and the capability lives on inside every WCP. What Gartner retired is XDR as a separate thing to buy.

What a WCP is

Gartner's public definition lists five modules and five platform traits.

Modules: device protection; identity protection; data loss prevention; controls for end-user applications, meaning email, browser and client-side apps; and AI usage discovery and control.

Platform traits: cross-control integration; a data lake for events; third-party integrations; cloud-native architecture; centralized management.

Two things stand out. First, AI usage discovery and control is on the list. Gartner's 2026 Endpoint Protection Magic Quadrant expects 90% of endpoint vendors to add it by 2028, which means most do not have it today. Second, the traits are about operating the platform, not about any single control. Correlation, central management and openness are what separate a WCP from a bundle.

Why this matters most to SMBs

Gartner's 2026 Endpoint Protection Magic Quadrant projects that by 2029, 30% of midsize organizations will converge endpoint, data and identity security into a workspace security platform. Midsize organizations have IT staff who can do that convergence. SMBs do not.

The market is large and already being contested. Gartner's October 2026 note on the SMB managed security market sizes it at USD 14.9 billion and names regional MSPs and AI-enabled MDR providers as the contenders. Analysys Mason projects SMB cybersecurity spending at USD 109 billion in 2026, 60% of worldwide spend.

So the question for an SMB is not "which WCP should I buy." It is "which MSP can run a WCP for me, and what is actually inside it." The question for an MSP is "how do I deliver WCP-grade protection without building a SOC and without negotiating with six security vendors."

The MSP delivery problem

Delivering a WCP as a service is harder than buying one, for four reasons.

1. **One platform does not cover one SMB.** Enterprises buy the whole platform. MSPs sell it in pieces, because SMB budgets are built in pieces. The MSP needs to know, per customer, which modules are active and which are missing.
2. **Single-vendor correlation stops at the vendor's edge.** A WCP from one vendor correlates its own telemetry. The MSP also runs an RMM, often a vulnerability scanner, sometimes network monitoring, and now AI governance. None of those are in the vendor's console.
3. **Priorities have to cross customers.** A security team looks at one organization. An MSP looks at thirty. It needs one list of what to do first, across all of them.
4. **The MSP has no SOC.** Whatever the platform produces has to end in an action the MSP can take, not an alert the MSP has to interpret.

These are not criticisms of WCP vendors. They are the gap between a category defined for enterprises and the way SMBs actually buy security.

How EDAO approaches it

EDAO Control Hub is built to close that gap. Three design decisions define it.

Built on Gartner-listed WCP vendors, curated by EDAO. Control Hub's controls come from vendors Gartner already lists in the WCP market, integrated with the RMM and exposure tools an MSP needs around them. EDAO does not claim to be a WCP vendor. It selected, integrated and operationalized WCP vendors so that an MSP can deliver them to an SMB as one service, with one contract and one console.

A correlation and coverage layer above the platform. ACE, the Adaptive Correlation Engine, reads every module, scores each customer's coverage and posture, correlates signals across controls and vendors, and produces one prioritized action list per customer. Actions execute through the modules: patch, isolate, block, reboot. This is the trait Gartner's definition values most and the one single-vendor platforms cannot deliver across an MSP's whole stack.

Human-centric and AI-governed from the start. Gartner's Hype Cycle for Workspace Security names human-centric security as the organizing idea. In an SMB the individual is the unit of risk, so ACE links a person's signals across controls: a leaked credential, a missing MFA, a public file share, a risky device. AI-GS, launched in October 2026, adds AI usage discovery and control, the newest module on Gartner's list and the one most vendors do not yet ship.

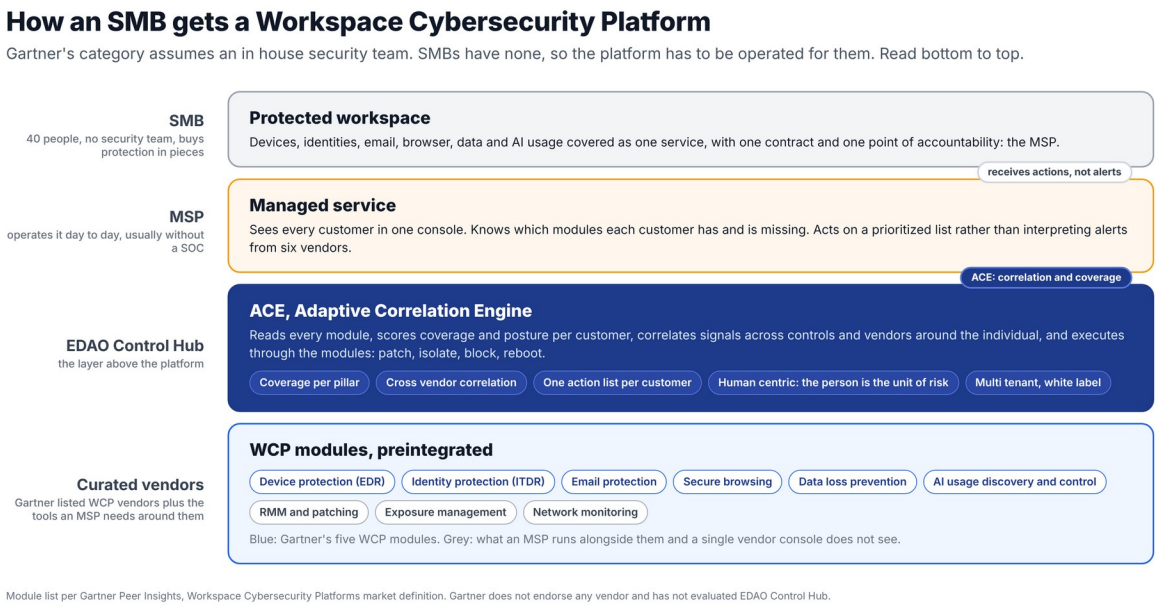

Figure 2. How an SMB gets a WCP: curated Gartner-listed vendors, ACE as the correlation and coverage layer, the MSP operating it, the SMB protected.

What to ask your provider

For an SMB evaluating an MSP, or an MSP evaluating a platform, five questions separate a WCP delivered as a service from a bundle with a new label.

1. Which of the five WCP modules are active for my organization today, and which are not? Can you show me the gap, not just the dashboard?
2. When two signals from different tools point at the same person, who connects them around that individual, and how fast? Human-centric security means the person is the unit of risk, not the alert.
3. What happens after a detection? Which actions are automated, and which wait for a human?
4. Do you see AI tools and agents in use in my environment, and can you set policy on them?
5. Who operates this day to day, and what do they need to know to do it well?

Closing

Categories change when the thing they described stops being special. XDR stopped being special because every platform learned to correlate. The new category, WCP, describes what enterprises now buy. SMBs will get the same protection, but only through MSPs equipped to run it. That is the work EDAO has chosen.

Sources

- Gartner, *Embrace Workspace Security to Prepare for the End of XDR*, 24 October 2025 — https://www.gartner.com/en/documents/7109530
- Gartner, *Market Overview for Workspace Cybersecurity Platforms*, Evgeny Mirolyubov and Peter Firstbrook, 20 July 2026, as summarized by Bitdefender — https://www.bitdefender.com/en-gb/blog/businessinsights/beyond-endpoint-workspace-security
- Gartner Peer Insights, Workspace Cybersecurity Platforms market definition — https://www.gartner.com/reviews/market/workspace-cybersecurity-platforms
- Gartner, *Hype Cycle for Security Operations, 2026*, as summarized by Dropzone AI — https://www.dropzone.ai/insights/blog/gartner-hype-cycle-security-operations-2026
- Gartner, *Hype Cycle for Workspace Security, 2026*, Franz Hinner, 2 June 2026 (abstract) — https://www.gartner.com/en/documents/7947473
- Gartner, *CSPs Must Scale Using Governed AI to Win the $14.9 Billion SMB Managed Security Market*, 28 October 2026 (abstract) — https://www.gartner.com/en/documents/8566173
- Gartner, *Magic Quadrant for Endpoint Protection Platforms, 2026*, forecasts as summarized by WithSecure — https://www.withsecure.com/en/resources-hub/blog/gartner-magic-quadrant-for-endpoint-protection/
- Analysys Mason, SMB cybersecurity spending to reach USD 109 billion in 2026 — https://www.analysysmason.com/research/content/articles/smb-cyber-spending-rsmb1-ren04/

Gartner, Hype Cycle and Magic Quadrant are trademarks of Gartner, Inc. and/or its affiliates. Gartner does not endorse any vendor, product or service depicted in its research publications and has not evaluated EDAO Group or Control Hub.