POINT OF VIEW

The Need for Unified Endpoint Security

Avoid Endpoint Agent Sprawl

Executive Summary

As organizations continue to support and expand remote and hybrid work environments, securing endpoints has become more complex. Devices, including workstations, mobile devices, and servers, that were once tightly governed by centralized policies now operate across distributed locations, accessing enterprise data from unmanaged networks. In this context, endpoint security is no longer just about malware prevention; it's about reducing operational complexity, closing visibility gaps, and accelerating response to increasingly sophisticated threats.

Fragmented endpoint protection technology stacks composed of multiple standalone tools for threat prevention, detection, and response are proving ineffective. Organizations must move beyond endpoint agent sprawl and disjointed operations toward unified endpoint security that consolidates visibility, simplifies management, and enables faster threat containment.

According to Gartner, "By 2029, 50% of organizations will evaluate endpoint protection platforms as part of a comprehensive workspace security strategy, up from approximately 20% in 2024."[1]

The Challenges of Endpoint Agent Sprawl

Endpoint protection strategies have historically relied on layering discrete tools to meet emerging threats. As a result, many endpoints today run three to five agents simultaneously. Using multiple endpoint tools can lead to degraded system performance, increased resource consumption, software conflicts, and complex patching schedules. Fragmentation also impacts the security operations center (SOC), creating blind spots in telemetry, increasing alert fatigue, and making it harder to triage and correlate threats.

To further reduce complexity, organizations are increasingly seeking to consolidate secure connectivity functions, such as ZTNA, VPN, and SASE, into the same lightweight agent used for endpoint security. This unified approach eliminates overlapping agents, reduces performance overhead, and ensures consistent policy enforcement across both access and protection layers.

The Security Risks of Fragmented Endpoint Protection

Security teams face mounting pressure to reduce risk while maintaining business agility. However, a fragmented endpoint stack often results in inconsistent policy enforcement and detection gaps, especially when adversaries use tactics such as credential abuse, lateral movement, or living-off-the-land techniques.

According to the *Verizon Data Breach Investigations Report*, 60% of breaches involve the human element, with stolen credentials and phishing as top initial access vectors.[2] Isolated detection systems are rarely able to correlate such activity with endpoint telemetry in real time, allowing attacks to escalate unchecked.

Gartner forecasts that "By 2029, 30% of midsize organizations will have converged their workspace, data security and identity security capabilities into a workspace security platform, enabling holistic protection and centralized policy management."[3]

In 2025, ESG found that organizations using a unified operational approach reduced average time spent on incident response by 86% to 99%, freeing teams to focus on proactive defense and strategic initiatives.[4]

The Case for Unified Endpoint Security

To mitigate risk and improve security, organizations are adopting a consolidated approach to endpoint protection that combines prevention, detection, and response into a single, integrated workflow. Key benefits of this model include:

- High-fidelity detection and response across the attack life cycle, from initial access to lateral movement
- Improved visibility through centralized telemetry and unified threat intelligence across users, devices, and networks
- Faster containment and remediation (ESG reported a 99% reduction in time to investigate and remediate threats, going from 18 hours to less than 5 minutes)[5]
- Operational efficiency gains so small teams can deliver outcomes equivalent to those of large, mature SOCs
- Reduced risk exposure, with 97% to 99% fewer hours exposed to threats compared to baseline operating models[6]

A consolidated endpoint approach helps eliminate redundant tools, minimizes performance overhead, and facilitates automation and playbook-driven response.

From Silos to Security Outcomes

Security teams are under pressure to accomplish more with fewer resources. They are confronting an expanding attack surface, rising alert volumes, and growing compliance mandates. A unified endpoint protection model enables teams to detect and stop advanced threats faster, reduce operational load, and focus their limited resources on higher-value activities. According to a 2025 ESG study, organizations adopting this approach improved team productivity by up to 99%, avoided up to $1.9 million in annual operational costs, and reduced incident containment times from hours to seconds.[7] More importantly, they strengthened resilience, identifying threats earlier, minimizing damage, and reducing reliance on large, specialized teams.

The path forward is clear. Organizations must move from fragmented point solutions to integrated, outcome-driven endpoint protection. Those organizations that adopt this strategy will be best positioned to manage hybrid work securely, efficiently, and at scale.

[1] Gartner, Securing Hybrid Work: Adopting the Right Workspace Security Strategy, By Evgeny Mirolyubov, Peter Firstbrook, Chris Silva, May 2024.

[2] Verizon, 2025 Data Breach Investigations Report, April 2025.

[3] Gartner, 2025 Strategic Roadmap for Workspace Security, By Peter Firstbrook, Evgeny Mirolyubov, Franz Hinner, April 2025.

[4] Aviv Kaufmann, Economic Validation: The Quantified Benefits of Fortinet Security Operations Solutions, ESG, January 2025.

[5] Ibid.

[6] Ibid.

[7] Ibid.

Copyright © 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's SVP Legal and above, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

July 10, 2025 6:22 PM / MKTG-1648-0-0-EN