SOLUTION BRIEF

Get Advanced Threat Protection and Secure Connectivity with FortiEndpoint

Executive Summary

Given today's complex threat landscape, ensuring secure connectivity and robust threat protection is paramount for every organization. The Fortinet FortiEndpoint unified client converges endpoint protection platform (EPP) technology with zero-trust network access (ZTNA), endpoint detection and response (EDR), and extended detection and response (XDR) solutions, providing secure remote access, advanced web filtering, vulnerability management, and real-time threat detection and response. Using its XDR capabilities, FortiEndpoint correlates alerts across various security layers, offering a comprehensive threat view and enabling effective responses. By integrating FortiEndpoint with the Fortinet Security Fabric and third-party solutions, organizations can protect networks and endpoints, reduce threat detection and remediation times, and simplify security management.

Organizations using Fortinet security operations solutions saw up to 99% improvement in security team productivity.[2]

The Need for Endpoint Security

Many organizations struggle with fragmented security solutions that do not integrate secure access with EDR capabilities. This disjointed approach leaves security gaps and makes it difficult to ensure that only the right users and devices can access critical applications, especially in remote and hybrid work environments. Managing multiple, disparate security tools across various endpoints also often leads to operational inefficiency and inconsistent security policies. Organizations need advanced endpoint protection to secure connectivity and protect against cyberthreats, but they also need to reduce complexity by integrating solutions into a unified endpoint agent.

The FortiEndpoint unified client combines EPP with ZTNA, EDR, and XDR providing a comprehensive approach to endpoint security. ZTNA restricts access to authenticated users and devices to secure remote work while minimizing the attack surface. EDR continuously monitors endpoints for threats, and XDR expands this capability by correlating alerts from multiple security layers to provide a complete view of the IT environment.

Fortinet takes a holistic approach to endpoint security with real-time threat detection and automated responses that reduce the mean time to detect (MTTD) and mean time to remediate (MTTR) from more than 21 days to less than an hour.[1] By minimizing manual intervention, organizations can maintain robust security and protect their networks and endpoints from advanced cyberthreats.

The Benefits of ZTNA for Securing Access

FortiEndpoint helps IT teams secure access through Universal ZTNA. It safeguards remote access by granting only authenticated users and verified devices access to critical applications using a proxy, which prevents direct application exposure and minimizes the attack surface. By integrating with the Fortinet Security Fabric, ZTNA provides continuous verification, advanced threat intelligence, and real-time monitoring. The comprehensive approach reduces complexity, improves compliance, and enhances protection against threats, creating a more resilient and secure IT infrastructure.

EDR Behavior-Based Controls

EDR capabilities are critical in modern cybersecurity strategies, playing a vital role in defending against advanced cyberthreats. The artificial intelligence of FortiEndpoint resides at the kernel level of the system, continuously monitoring endpoints and detecting and responding to malicious behaviors in real time. This design ensures the agent is very lightweight, grants superior visibility into system processes, makes it evasion-resistant, and allows the development team to support a broad range of operating systems. Furthermore, its constant vigilance ensures that threats are identified and neutralized promptly before they can cause significant damage.

By leveraging behavior-based anti-malware technology, FortiEndpoint can detect sophisticated threats that traditional signature-based methods might miss, providing a robust line of defense at the endpoint level that security teams need. This proactive approach to threat detection helps organizations maintain a strong security posture and protect sensitive data and critical systems. The forensic capabilities enable organizations to summon memory snapshots and record rule violations and MITRE tagging to quickly understand why and how something may be a threat.

The Fortinet Security Fabric can reduce risk by up to 99% through faster identification and remediation of threats.[3]

XDR Capabilities and Security Fabric Integration

The FortiEndpoint XDR capabilities extend traditional EDR by correlating alerts from network, email, endpoint, server, and cloud security layers. Leveraging the Fortinet Security Fabric threat intelligence, FortiEndpoint provides a comprehensive view and response to threats. This integration enhances the overall effectiveness of security operations by delivering an end-to-end comprehensive view of the threat landscape.

By aggregating data, the onboard machine learning (ML) capabilities identify attack patterns and anomalies, enhancing threat visibility. The automated response capabilities further strengthen this defense, reducing the need for manual intervention and allowing security teams to focus on more strategic tasks. Using these capabilities, organizations can significantly reduce MTTD especially for low-fidelity alerts and MTTR through automated correlation and analysis of security events. Its multi-lake design allows FortiEndpoint to integrate with various data lakes, including Fortinet and third-party solutions, to reduce ownership costs.

Integration with Other Solutions

FortiEndpoint seamlessly integrates with other Fortinet products and third-party solutions to create a unified security infrastructure. The integration with FortiGate Next-Generation Firewalls (NGFWs) allows real-time threat intelligence sharing and dynamic security policy enforcement. For example, if an endpoint attack is detected, the originating IP address is blocked on all integrated firewalls, preventing attack spread.

The FortiEndpoint integration with FortiNAC network access control enables security policies to be based on endpoint compliance and network context. For example, endpoints with suspicious activity can be automatically moved to a remediation VLAN, isolating them while addressing the threat. Because of this integration, organizations can contain potential threats and ensure only secure devices access critical resources.

The FortiEndpoint integration with FortiSandbox, FortiAnalyzer, FortiSIEM, FortiSOAR, and third-party solutions enhances threat analysis, centralized logging, reporting, threat correlation, and incident response. For example, FortiSandbox inspects suspicious files for proactive protection, while FortiAnalyzer provides high-level insights into activities across the ecosystem. This extensive integration enables comprehensive threat detection, real-time threat intelligence sharing, and coordinated responses, improving security operations efficiency. Organizations can leverage existing security investments while building a robust cybersecurity infrastructure.

Augmented by Services

FortiEndpoint is strengthened by best practice service (BPS) and managed detection and response (MDR). BPS ensures smooth deployments tailored to each organization's needs. The add-on MDR service provides 24×7 threat monitoring, analysis, and mitigation by security experts. These services enhance security operations, reduce strain on internal teams, and provide a robust defense against cyberthreats.

A Comprehensive Approach to Endpoint Security

Integrating ZTNA, EDR, and XDR is crucial for organizations to protect their networks and endpoints. FortiEndpoint provides strong protection and seamless remote access and enhances overall security. Continuous monitoring, behavior-based detection, and automated responses improve security operations efficiency and reduce MTTD and MTTR. The extensive integration with Fortinet and third-party solutions creates a unified security infrastructure with real-time threat intelligence sharing and dynamic policy enforcement. By adopting integrated Fortinet solutions such as FortiEndpoint, IT teams can achieve a robust and scalable cybersecurity framework to protect their critical assets and maintain business continuity.

[1] Economic Validation: The Quantified Benefits of Fortinet Security Operations Solutions, Enterprise Strategy Group, July 2023.

[2] Ibid.

[3] Ibid.

Copyright © 2024 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.

September 16, 2024 11:33 PM / 2817607-0-0-EN