SOLUTION BRIEF

Fortinet and CrowdStrike Joint Solution

Delivering AI-Powered Protection, Adaptive Zero-Trust Access, and Accelerated Threat Detection and Response across Your Entire Digital Infrastructure

Executive Summary

Fortinet and CrowdStrike have partnered to offer an advanced layered protection, detection, and response solution from market leaders in endpoint and firewall to deliver best-in-class security and accelerated security operations. With the integration of the FortiGate Next-Generation Firewall (NGFW) with CrowdStrike Falcon Insight XDR endpoint protection, organizations can leverage AI-powered threat protection, adaptive zero-trust access, and unified visibility with accelerated threat detection and response across the digital infrastructure. By bringing together best-in-class endpoint and firewall protection, teams can address key security challenges in today's hybrid work environments, providing a unified approach to risk management and operational efficiency.

Expanding Attack Surface and Operational Inefficiencies

Hybrid work and the need for network and application access from any location have increased organizations' attack surface. Adversaries are exploiting this faster than before, leaving businesses with limited time to respond. Moreover, many security teams face operational inefficiencies due to limited skilled staff, disjointed products, and siloed data, which hinder effective security management.

Fortinet and CrowdStrike Solution: Best-in-Class Platform Integration

Fortinet and CrowdStrike have partnered to deliver an integrated security solution that simplifies zero-trust adoption. Combining Fortinet Secure Networking with CrowdStrike Endpoint Protection, the AI-powered platforms offers end-to-end protection, unified visibility, and adaptive, risk-based access. Designed to address staffing challenges and tool inefficiencies, Fortinet and CrowdStrike provide a seamless experience through a single console, enhancing threat detection, streamlining incident response, and strengthening overall security posture.

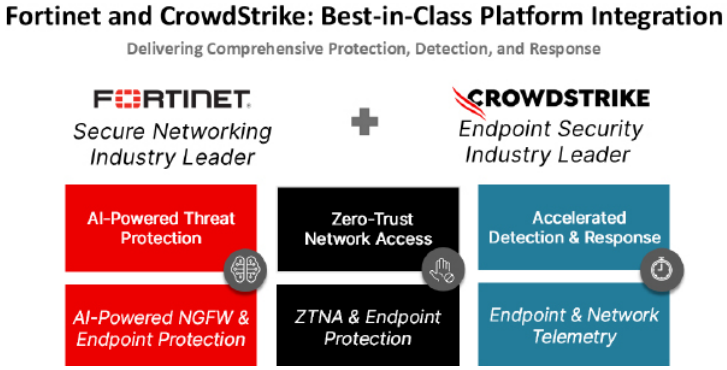
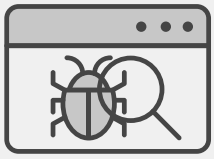


Figure 1: Fortinet and CrowdStrike: delivering an advanced end-to-end security platform



The threat landscape continues to evolve at a rapid pace,with new and sophisticated attacks emerging constantly. Organizations must stay ahead of the curve by investing in advanced security solutions that can detect and mitigate threats before they cause significant damage.[1]

FORTINET FABRIC-READY

Use Cases

#1: AI-Powered Threat Protection

Solution

Fortinet FortiGate NGFW, integrated with CrowdStrike Falcon Insight XDR endpoint protection, delivers comprehensive, AI-powered threat defense. FortiGate NGFW, combined with FortiGuard AI-Powered Security Services, ensures best-in-class network protection with high performance and minimal latency. Falcon Insight XDR provides top-tier and complete endpoint protection by continuously monitoring all endpoint activity and analyzing the data in real time to automatically identify threat activity. Together, they offer deep insights into network traffic, user behavior, and endpoint security posture. This unified approach enhances visibility and delivers robust protection across networks and endpoints.

Customer value

- Improved threat detection and response time

How it works

The FortiGate data connector sends firewall logs to the CrowdStrike Falcon platform, where the data is correlated and enriched with high-fidelity security data and threat intelligence within Falcon, unifying visibility for extended protection across networks and endpoints. The integration enables analysts to store, analyze, and visualize firewall logs alongside additional endpoint and security data in a single console, helping detect suspicious activity swiftly and enabling an effective layered security approach.

Figure 2: Falcon dashboard with analysis of FortiGate logs

#2: Adaptive, Risk-Based Zero-Trust Access

Solution

By combining Falcon Insight XDR endpoint protection with the FortiClient ZTNA agent and FortiGate ZTNA access policies, SOCs are enabled with adaptive, risk-based access controls. This minimizes lateral movement of malware and enhances secure access to corporate applications regardless of the user's location.

Customer value

- Strengthened security posture with dynamic, risk-based access, improved security for remote access, reduced risk of malware propagation

How it works

CrowdStrike Falcon offers real-time assessments of endpoint posture, including device health and user behavior. FortiGate enforces zero-trust access policies based on user and device identity, and device posture and enables granular application access control with best-in-class security inspection of ZTNA traffic. Together, the integration enables strong ZTNA and improves security posture.

#3: Unified Visibility with Accelerated Threat Detection and Response

Solution

Integrating CrowdStrike Falcon endpoint telemetry with Fortinet FortiGate network telemetry delivers unified visibility across the entire security landscape, accelerating threat detection and response. This integration, along with the broader best-in-class Fortinet and CrowdStrike Falcon platforms, enables automated, proactive threat detection and response.

Customer value

- Faster, more accurate threat detection with comprehensive visibility

How it works

FortiGate network telemetry and Falcon endpoint telemetry can be sent to a customer's security information and event management (SIEM) and security orchestration, automation, and response (SOAR) solutions to provide unified visibility so the security operations center (SOC) team can accelerate threat detection and trigger response workflows.

#4: Streamlining Detection and Response from Network to Endpoint

Solution

Through its integration with CrowdStrike Falcon Insight XDR and CrowdStrike Falcon Next-Gen SIEM, FortiNDR Cloud enables security teams to seamlessly move from detection to investigation and response - all within a few clicks.

Customer value

SOC teams can triage and investigate network events and then isolate affected endpoints directly from a single console - reducing complexity and accelerating response.

How it works

FortiNDR Cloud correlates CrowdStrike Counter Adversary Operations with network metadata to enhance investigation and response. These FortiNDR Cloud detections are then synchronized with the CrowdStrike Next-Gen SIEM console and integrated into FortiSOAR enabling automated playbooks and coordinated response actions to streamline response across the SOC.

Conclusion

The Fortinet and CrowdStrike layered solution provides industry-leading protection and integrated security for organizations looking to protect their digital environments against ever-evolving threats. By combining endpoint and network firewall security with AI-powered threat detection and zero-trust frameworks, this partnership empowers businesses to stay ahead of adversaries while streamlining security operations.

[1] Fortinet Global Threat Landscape Report 2023.

September 11, 2025 11:49 PM / 2865780-0-0-EN