



CrowdStrike and Fortinet: Unifying AI-Native Endpoint Security and Next-Generation Firewall Protection

Converge best-in-class firewall and endpoint visibility and protection to elevate security operations and speed up defense

Challenges

Legacy firewall and endpoint solutions are struggling to keep pace with the growing complexity of modern cyber threats, advanced applications and increasingly intricate networks. Compounding this, the rise of hybrid work and remote access to distributed corporate systems has expanded the attack surface, creating gaps in protection across the organization. With limited capabilities from traditional tooling and dispersed network and endpoint access, security teams grapple with poor visibility across the environment and delayed detection and response, significantly heightening the risk of a successful attack.

Furthermore, with an average observed eCrime breakout time of **62 minutes in 2023**, adversaries are moving faster than ever and are targeting gaps in visibility across the growing attack surface. Security teams are forced to mitigate operational inefficiencies, eliminate disjointed products and unify siloed data to keep pace with today's threat actors.

Solution

Organizations require a multi-layer approach of best-in-class security tools for comprehensive protection of their infrastructure and data to quickly and effectively secure themselves from ever-evolving threats in the hybrid work era. The strategic partnership between Fortinet and CrowdStrike combines leading endpoint and network security platforms to offer joint customers unified and consolidated protection. This integration helps reduce risk through Zero Trust adaptive access, AI-powered threat protection and robust threat detection and response. By integrating platforms, your security team gains consolidated visibility and enhanced security control across network and endpoints, eliminating the need to switch between multiple interfaces. As a result, you can swiftly identify and respond to elusive threats traversing the environment, ensuring a robust and resilient security posture with defense in depth.

Key benefits

- **Industry-leading protection** from endpoint to network for robust and effective security that moves at the speed of the adversary
- **Advanced, AI-powered endpoint-to-firewall detection** to quickly and accurately find and prevent threats traversing the dispersed attack surface
- **Seamless integration and data sharing** for unified visibility, accelerating security operations, reducing friction and mitigating “swivel chair syndrome”

Technical solution

Industry-leading AI-powered threat protection across endpoint and firewall:

Layering best-in-class capabilities from Fortinet FortiGate next-generation firewall (NGFW) with CrowdStrike Falcon® Insight XDR endpoint security provides your team with enriched, contextual insight into network traffic, user activity and endpoint security posture. By leveraging high-fidelity security telemetry, threat intelligence and robust AI-powered security capabilities from both CrowdStrike and Fortinet, you can optimize network and endpoint security coverage, streamline operations and significantly enhance the detection and response to even the most elusive threats.

Adaptive, risk-based security for enhanced Zero Trust network access:

Leverage the CrowdStrike Falcon® Zero Trust Assessment (ZTA) score in FortiClient Universal ZTNA posture checks and FortiGate ZTNA access policies for adaptive, risk-based secure access. With these dynamic access policies for corporate applications based on the posture health of a device, you can ensure access to only healthy devices, minimizing lateral movement and insecure access, regardless of location.

Unified visibility and enhanced threat detection:

Get comprehensive visibility across the security landscape by centralizing and analyzing CrowdStrike endpoint security telemetry with Fortinet network security telemetry in CrowdStrike Falcon® Next-Gen SIEM. By seamlessly correlating data from both endpoints and networks alongside additional security insights, you can minimize data silos and visibility gaps for faster threat detection and prevention of malicious activities. With this unified logging, your team is empowered to quickly and accurately pinpoint threats, reduce false positives and streamline incident response processes.

Learn more in the
CrowdStrike Marketplace



About Fortinet

Fortinet is a driving force in the evolution of cybersecurity and the convergence of networking and security. Our mission is to secure people, devices and data everywhere, and today, we deliver cybersecurity everywhere you need it with the largest integrated portfolio of over 50 enterprise-grade products. Well over half a million customers trust Fortinet's solutions, which are among the most deployed, most patented and most validated in the industry.

Learn more at <https://www.fortinet.com> and the [Fortinet Blog](#).

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: <https://www.crowdstrike.com/>

Follow us: [Blog](#) | [X](#) | [LinkedIn](#) | [Facebook](#) | [Instagram](#)

Start a free trial today: <https://www.crowdstrike.com/free-trial-guide/>

