SOLUTION BRIEF

Fortinet and CrowdStrike Security Solution

Unify security visibility by seamlessly connecting Fortinet FortiGate NGFW data with the CrowdStrike Falcon platform

Executive Summary

Accelerate operations and boost threat detection by seamlessly ingesting and unifying Fortinet firewall data with additional third-party data in the AI-native CrowdStrike Falcon® XDR platform.

Unify data across endpoint and firewall domains to enhance your team's detection of modern threats. Easily ingest Fortinet FortiGate Next-Generation Firewall (NGFW) data into the CrowdStrike Falcon® platform to gain comprehensive cross-domain visibility of threats throughout your attack surface. See Fortinet FortiGate NGFW's firewall event data directly within the Falcon console, alongside additional threat indicators from other domains, to minimize context-switching across multiple interfaces, allowing your team to improve detection, triage, and accuracy.

Joint Solution

CrowdStrike and Fortinet have partnered to deliver an industry-leading security solution to accelerate operations and boost threat detection.

Solution Components

CrowdStrike Falcon Next-Gen SIEM

CrowdStrike Falcon Next-Gen SIEM revolutionizes threat detection, investigation, and response by bringing together unmatched security depth and breadth in one unified platform to stop breaches. Falcon Next-Gen SIEM extends the industry's most dominant endpoint detection and response (EDR), threat intelligence and expert services to all data sources for complete visibility and protection.

Fortinet FortiGate Next-Generation Firewall

FortiGate NGFWs provide industry-leading threat protection and decryption at scale with a custom ASIC architecture. They also deliver Secure Networking with integrated features like SD-WAN, switching and wireless, and 5G. Converge your security and networking point solutions into a simple-to-use, centralized management console powered by a single operating system, FortiOS, and simplify IT management.

Solution Integration

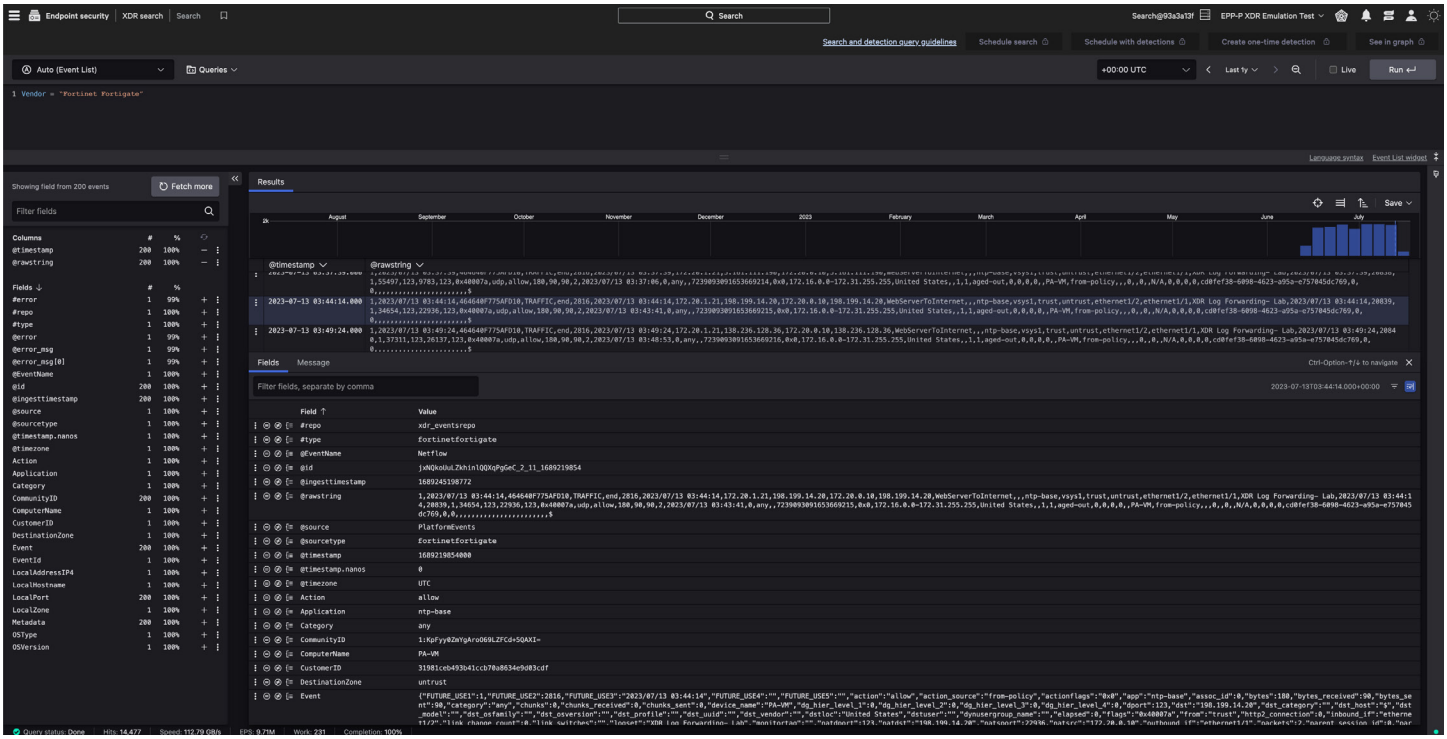
Create data connectors in the Falcon console to automate and manage ingestion from third-party data sources. You can seamlessly bring in firewall data from Fortinet FortiGate NGFW, alongside a range of CrowdStrike Marketplace data connectors for downstream analysis and processing in the Falcon platform to unlock insights and enhance your overall security posture. With this native Fortinet firewall data connector, you can easily collect data into the Falcon platform, so you can spend more time fighting threats and less time onboarding data.

Solution Components

- Fortinet FortiGate NGFW
- CrowdStrike Falcon® Next-Gen SIEM

Solution Benefits

- **Extended threat detection and alerting:** Get unified visibility across firewall and endpoint threat vectors with FortiGate threat indicators alongside indicators from other domains within the CrowdStrike Falcon R platform to swiftly detect threats in your environment
- **Unify investigation in a single console:** Minimize context-switching and accelerate threat detection to save your analysts valuable time through CrowdStrike's unified, threat-centric command console
- **Simplify data ingestion:** Streamline operations by easily ingesting Fortinet FortiGate data via the new Falcon Data Connectors user interface, providing rich insights across your attack surface and full visibility into your data ingestion pipeline
- **Unparalleled security protection:** Leverage the industry-leading threat protection provided by the Fortinet FortiGate NGFW



CrowdStrike Falcon and Fortinet FortiGate NGFW integration

Joint Use Case

AI-powered detections, extended to FortiGate NGFW data. Find the most sophisticated adversaries across firewalls and additional data sources with detections powered by the same advanced AI and behavior analysis as CrowdStrike's industry-leading EDR.

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.

FORTINET FABRIC-READY

FORTINET

www.fortinet.com

April 24, 2024 5:51 AM

2642807-0-0-EN