07-12-2026

Fortinet

Fortinet is a global leader in broad, integrated, and automated cybersecurity solutions, best known for its FortiGate Next Generation Firewalls (NGFWs).

Before looking at documentation for specific data sources, review the Splunk Help information on general data ingestion for Splunk Enterprise, Splunk Cloud Platform or Splunk Observability Cloud.

Getting data in

Source	Add-ons and Apps	Guidance
FortiGate FortiGate Next Generation Firewalls provide comprehensive enterprise security, offering visibility and threat protection across various network edges. FortiGate datacenter threat visualizations in Splunk help you identify anomalous behavior and de-duplicate threat feed data to enable the fast creation and consolidation of analytics. In the Common Information Model, FortiGate data is typically mapped to the Firewall data model.	**Splunk platform** • Fortinet FortiGate Add-On for Splunk • Fortinet FortiGate App for Splunk • Fortinet FortiSOAR Add-on for Splunk	**Splunk Lantern Articles** • Monitoring for network traffic volume outliers • Reconstructing a website defacement • Monitoring ingress and egress traffic across Operational Technology perimeters • Monitoring common Operational Technology protocol ports