Fortinet FortiGate App for Splunk

Threat Investigation Made Easy

The FortiGate App for Splunk combines the best security information and event management (SIEM) and threat prevention by aggregating, visualizing and analyzing hundreds of thousands of log events and data from FortiGate physical and virtual firewall appliances. The App dramatically improves the detection, response and recovery from advanced threats by providing broad security intelligence from data that is collected across the cloud.

Fortinet FortiGate App for Splunk

Every business has its specific demand and tolerance in terms of recovery and response time objectives to security events. The **Fortinet FortiGate App for Splunk** provides the Threat and UTM Dashboard, which offers presets and configuration to identify anomalous behavior.

FortiOS threat intelligence is built in the default App interface to quickly sort and de-duplicate threats. Instantaneous charting and pivoting on data analytics can pinpoint security breaches across multiple domains and geographic areas. Businesses can fulfill the fastest Response and Recovery Time Objectives with real-time information throughout Fortinet firewall infrastructure.

Benefits

- Visualizes logging data efficiently with integrated security analysis
- Makes data aggregation easier by interacting with pre-defined security metrics
- Improves protection from advanced threats with built-in Threat and UTM dashboards
- Extends datacenter security awareness with real time monitoring and trending

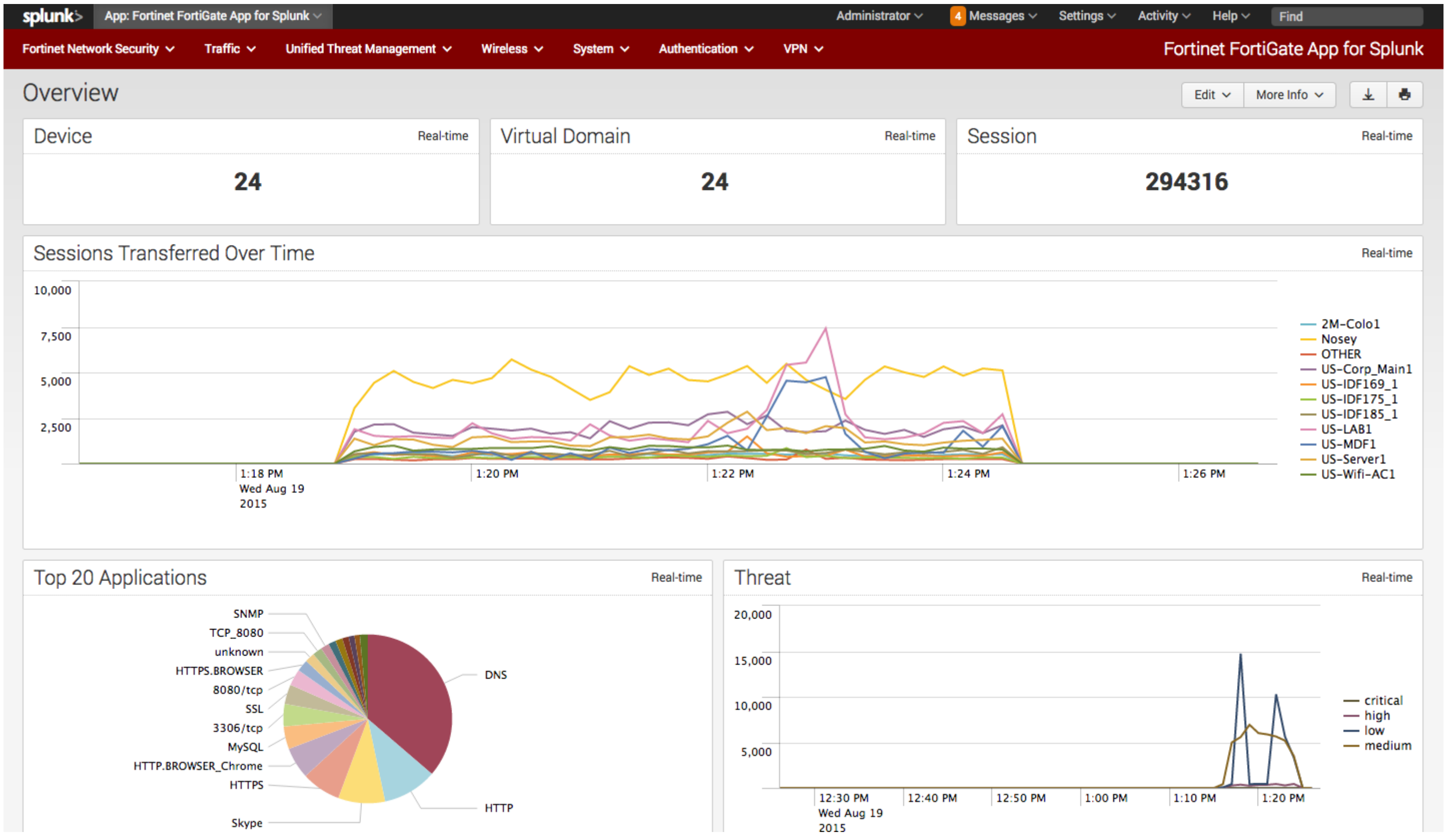
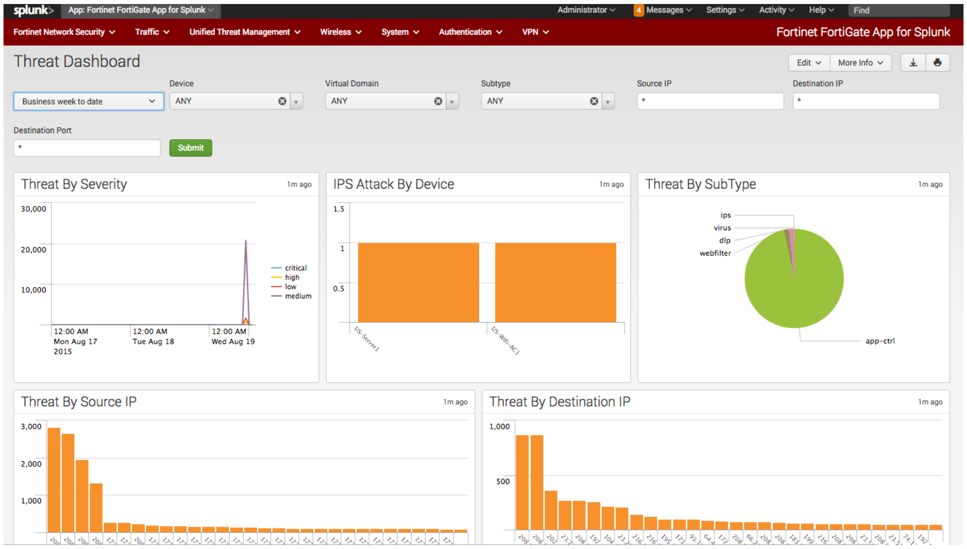


Figure 1 **Fortinet FortiGate App for Splunk** Overview

The App can absorb a high volume of elevated logs in real time and expose insights to examine advanced threat intent, widespread backdoor viruses, and unexpected information flows in a single pane of glass, enabling quick visualization of everything that's happening in your datacenter and cloud.

The **Fortinet FortiGate App for Splunk** solution delivers advanced security reporting and analysis in the datacenter that benefits operational reporting, as well as providing simplified and configurable dashboard views across Fortinet firewall appliances, physical and virtual.

It enables security analysts, administrators, and architects to correlate application and user activities across all network and security infrastructures from a real-time and historical perspective.



Threat Dashboard

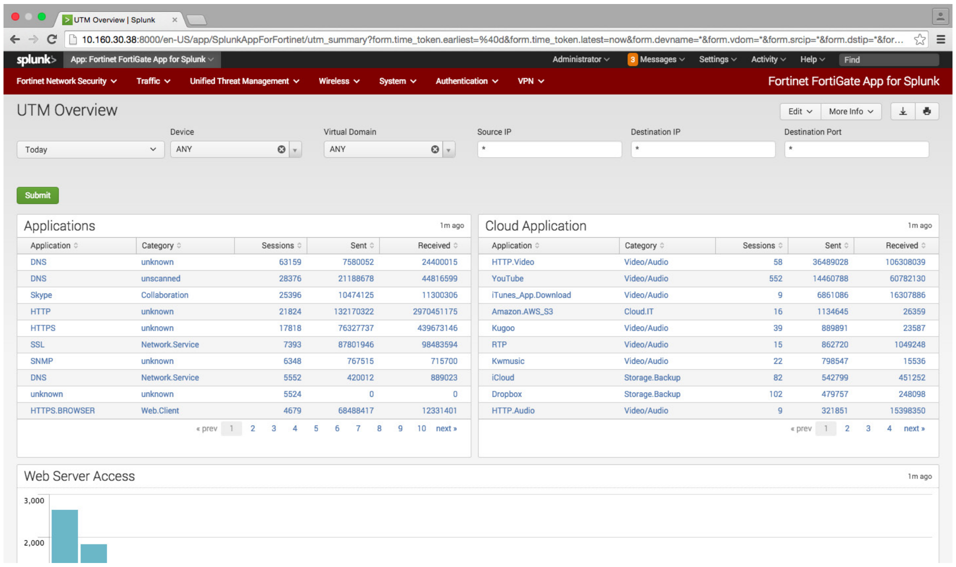
Device	Virtual Domain	Subtype	Source IP	Destination IP
Business week to date	ANY	ANY	ANY	*	*

Destination Port: *

Figure 2 **Fortinet FortiGate App for Splunk** Threat Dashboard

Security & Compliance

In the wake of high-profile data breaches, governments are looking to expand penalties for companies who are non-compliant, instead of just treating compliance mandates like PCI as a baseline for security. Security analytics are usually conducted manually and it becomes very time-consuming to drill into specific events, making the data mining process easily error-prone. Fortinet **FortiGate App for Splunk** is an enterprise-ready solution that effectively and efficiently inspects threats through up-leveled visualization. Less data loss means less revenue loss. This allows businesses to focus on critical investigations by responding more quickly to each data breach.



10.160.30.38:8000/en-US/app/SplunkAppForFortinet/utm_summary?form.time_token.earliest=%40d&form.time_token.latest=now&form.devname=*&form.vdom=*&form.srcip=*&form.dstip=*&for…

UTM Overview

	Device	Virtual Domain	Source IP	Destination IP	Destination Port
Today	ANY	ANY	*	*	*

Applications (1m ago)

Application	Category	Sessions	Sent	Received
DNS	unknown	63159	7580052	24400015
DNS	unscanned	28376	21188678	44816599
Skype	Collaboration	25396	10474125	11300306
HTTP	unknown	21824	132170322	2970451175
HTTPS	unknown	17818	76327737	439673146
SSL	Network.Service	7393	87801946	98483594
SNMP	unknown	6348	767515	715700
DNS	Network.Service	5552	420012	889023
unknown	unknown	5524	0	0
HTTPS.BROWSER	Web.Client	4679	68488417	12331401

Cloud Application (1m ago)

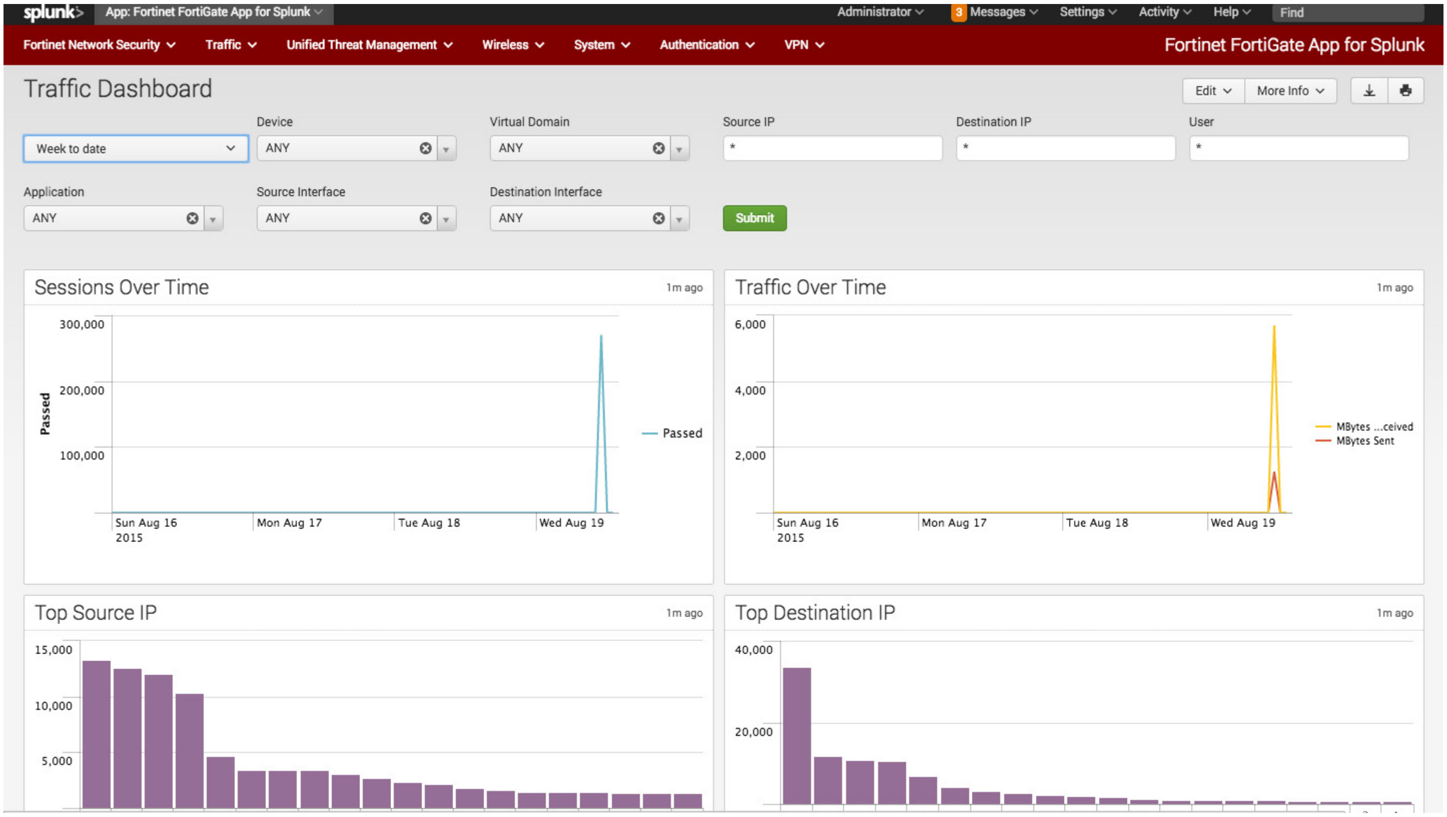
Application	Category	Sessions	Sent	Received
HTTP.Video	Video/Audio	58	36489028	106308039
YouTube	Video/Audio	552	14460788	60782130
iTunes_App.Download	Video/Audio	9	6861086	16307886
Amazon.AWS_S3	Cloud.IT	16	1134645	26359
Kugoo	Video/Audio	39	889891	23587
RTP	Video/Audio	15	862720	1049248
Kwmusic	Video/Audio	22	798547	15536
iCloud	Storage.Backup	82	542799	451252
Dropbox	Storage.Backup	102	479757	248098
HTTP.Audio	Video/Audio	9	321851	15398350

Figure 3: Built-In UTM Overview

Seamless Integration with FortiGate Firewalls

The FortiGate App also verifies current and historical logs and administrative events including firewall, anti-virus, IPS and application control. All features are supported with Fortinet VDOM enabled, in both NAT and Transparent mode. Most common traffic protocols are supported and included over IPv4 such as:

TCP: telnet, http, ftp
UDP: syslog, tftp
ICMP: ping



Traffic Dashboard

Week to date

Device: ANY

Virtual Domain: ANY

Source IP: *

Destination IP: *

User: *

Application: ANY

Source Interface: ANY

Destination Interface: ANY

Figure 4: Traffic Analysis in **Fortinet FortiGate App for Splunk** Presets

Compatibility List

Fortinet versions

- FortiGate appliances with FortiOS v5.0/v5.2/v5.4
- FortiGate-VM on VMware ESXi 6 with FortiOS v5.0/v5.2/v5.4

Splunk versions

Version 6.x

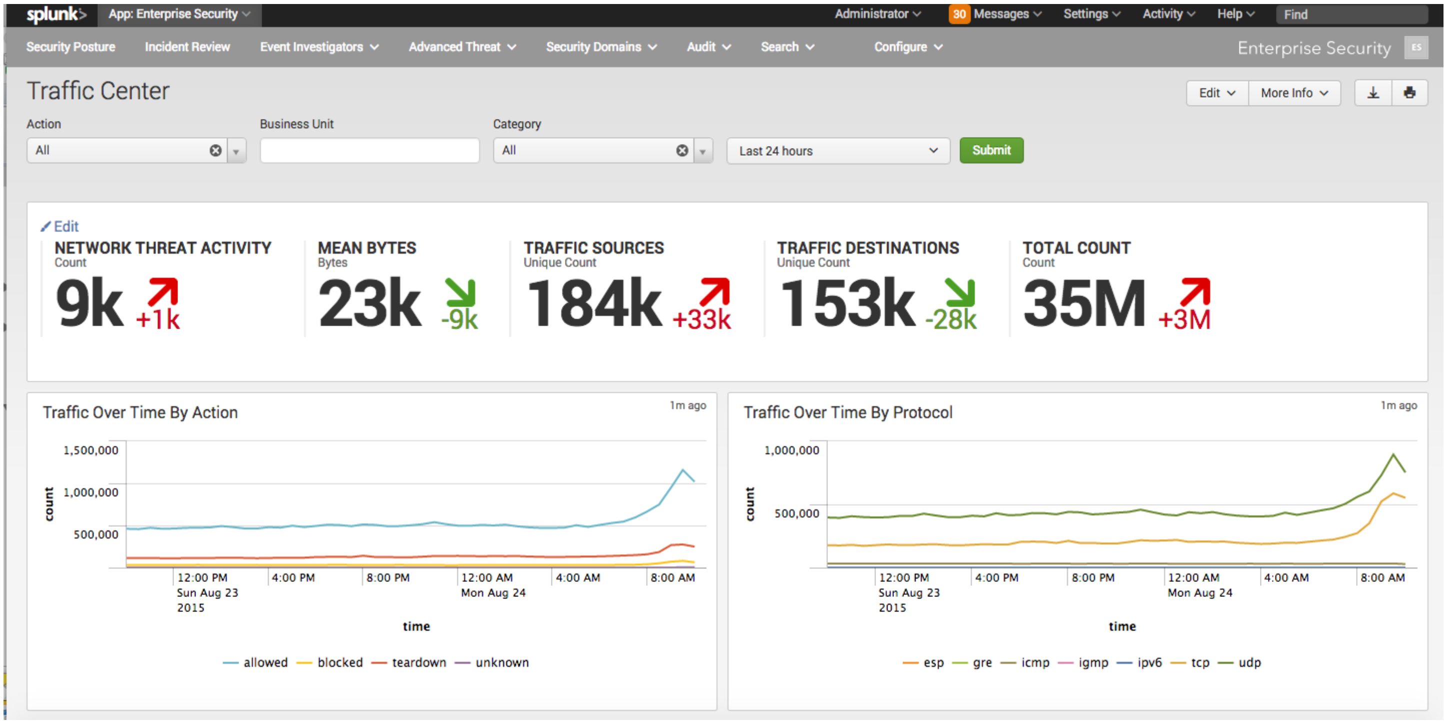
- Linux Enterprise version
- Windows Server 2008, 2008 R2, 2012 and 2012 R2, Windows 7, and 8 and 8.1

Fortinet FortiGate Add-On for Splunk

In addition to the direct **Fortinet FortiGate App for Splunk** listed in Splunkbase https://splunkbase.splunk.com/app/2800/, Fortinet has also developed the **Fortinet FortiGate Add-On for Splunk**, the technical add-on (TA) can be added into solutions such as Splunk App for Enterprise Security.

The FortiGate add-on enables Splunk Enterprise and Enterprise Security to ingest or map security and traffic data collected from FortiGate physical and virtual appliances across domains. Key features include:

- Streamlining authentication and access from FortiGate, such as administrator login, user login, and VPN termination authentication into Splunk Enterprise Security Access Center
- Mapping FortiGate malware reporting into Splunk Enterprise Security Endpoint Malware Center
- Ingesting traffic logs, IPS logs, system configuration logs and Web filtering data, etc.



Traffic Center

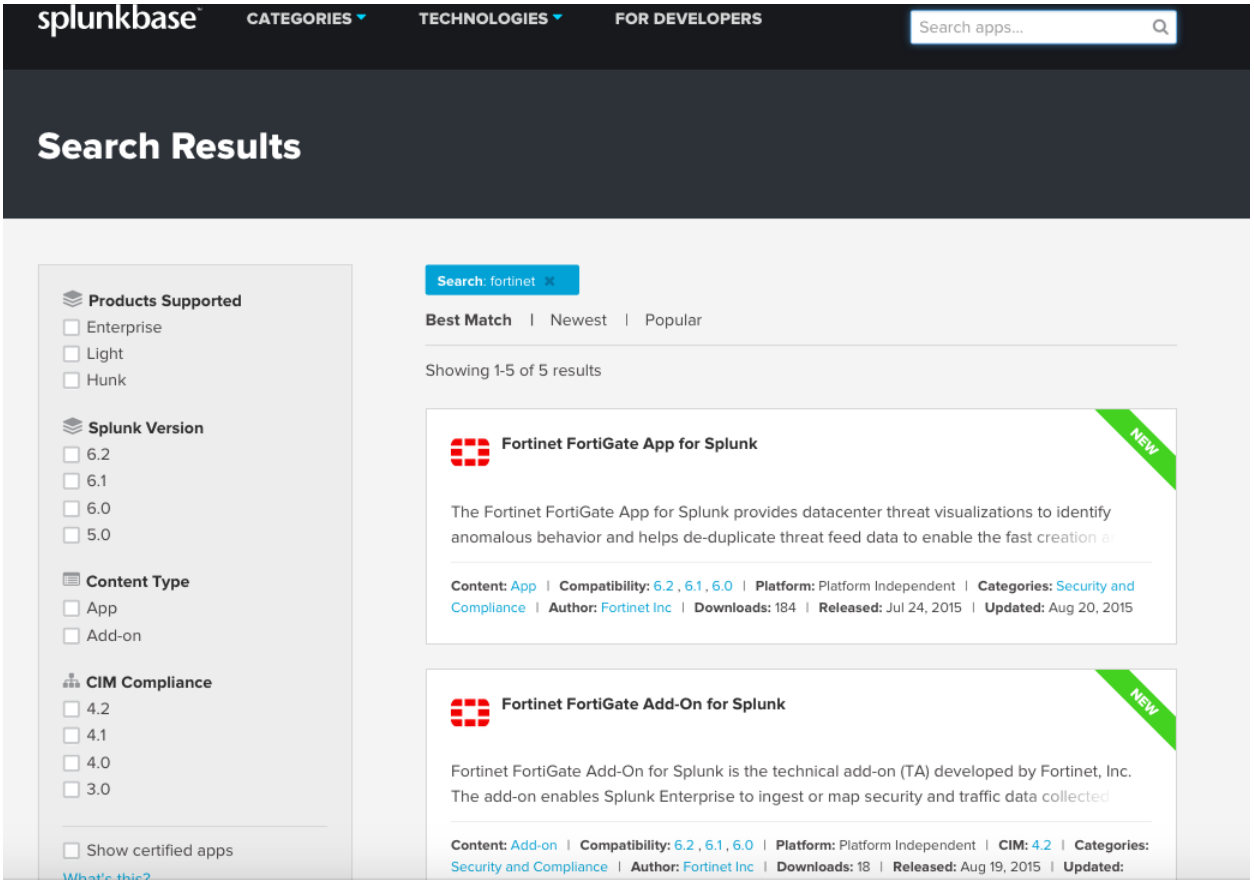
Action: All

Business Unit:

Category: All

Last 24 hours

Figure 5: **Fortinet FortiGate Add-On for Splunk Overview**



Search Results

Products Supported
□ Enterprise
□ Light
□ Hunk

Splunk Version
□ 6.2
□ 6.1
□ 6.0
□ 5.0

Content Type
□ App
□ Add-on

CIM Compliance
□ 4.2
□ 4.1
□ 4.0
□ 3.0

□ Show certified apps
What's this?

Search: fortinet ✕

Best Match | Newest | Popular

Showing 1-5 of 5 results

Fortinet FortiGate App for Splunk NEW

The Fortinet FortiGate App for Splunk provides datacenter threat visualizations to identify anomalous behavior and helps de-duplicate threat feed data to enable the fast creation a

Content: App | **Compatibility:** 6.2 , 6.1 , 6.0 | **Platform:** Platform Independent | **Categories:** Security and Compliance | **Author:** Fortinet Inc | **Downloads:** 184 | **Released:** Jul 24, 2015 | **Updated:** Aug 20, 2015

Fortinet FortiGate Add-On for Splunk NEW

Fortinet FortiGate Add-On for Splunk is the technical add-on (TA) developed by Fortinet, Inc. The add-on enables Splunk Enterprise to ingest or map security and traffic data collected

Content: Add-on | **Compatibility:** 6.2 , 6.1 , 6.0 | **Platform:** Platform Independent | **CIM:** 4.2 | **Categories:** Security and Compliance | **Author:** Fortinet Inc | **Downloads:** 18 | **Released:** Aug 19, 2015 | **Updated:**

Fortinet FortiGate Add-On for Splunk provides common information model (CIM) knowledge, advanced “saved search”, indexers and macros to use with Splunk App for Enterprise Security.

FORTINET®

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE
Paseo de la Reforma 412 piso 16
Col. Juarez
C.P. 06600
México D.F.
Tel: 011-52-(55) 5524-8428

Sep 18, 2015