

SOLUTION BRIEF

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 deduplicate 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.

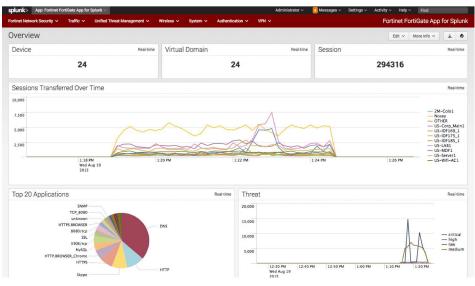


Figure 1: Fortinet FortiGate app for Splunk overview.

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



1

The App can absorb a high volume of elevated logs in real time and provide 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

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.

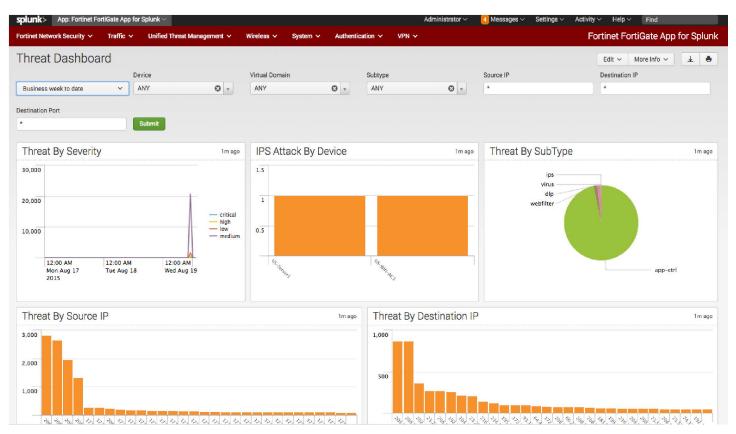


Figure 2: Fortinet FortiGate app for Splunk threat dashboard.

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.

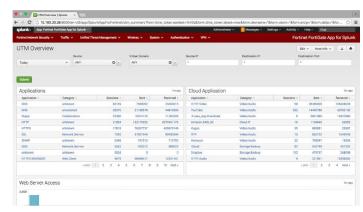


Figure 3: Built-in UTM Overview.



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, ftpUDP: syslog, tftp

ICMP: ping



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.

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.



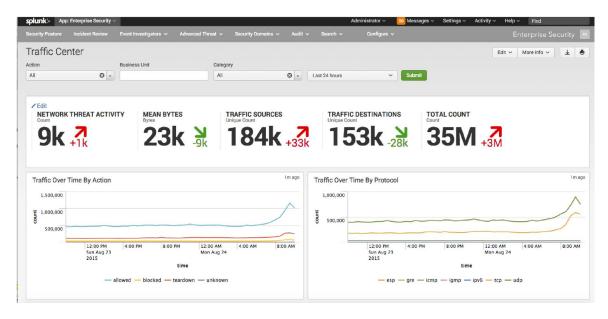
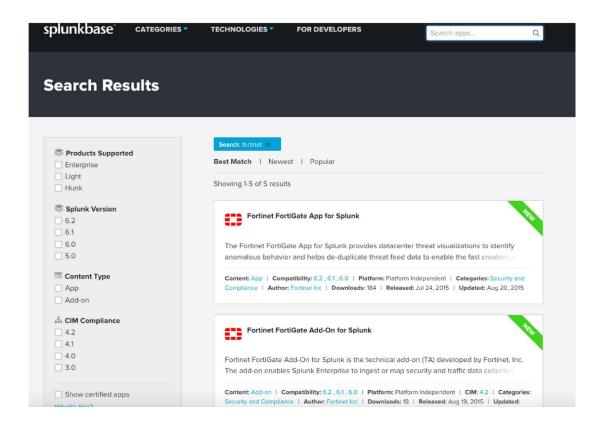


Figure 5: Fortinet FortiGate Add-On for Splunk Overview.





www.fortinet.com

Copyright © 2019 Fortinet, Inc. All rights reserved. Forticate*, FortiCare* and FortiGuard*, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Coursel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.