SOLUTION BRIEF

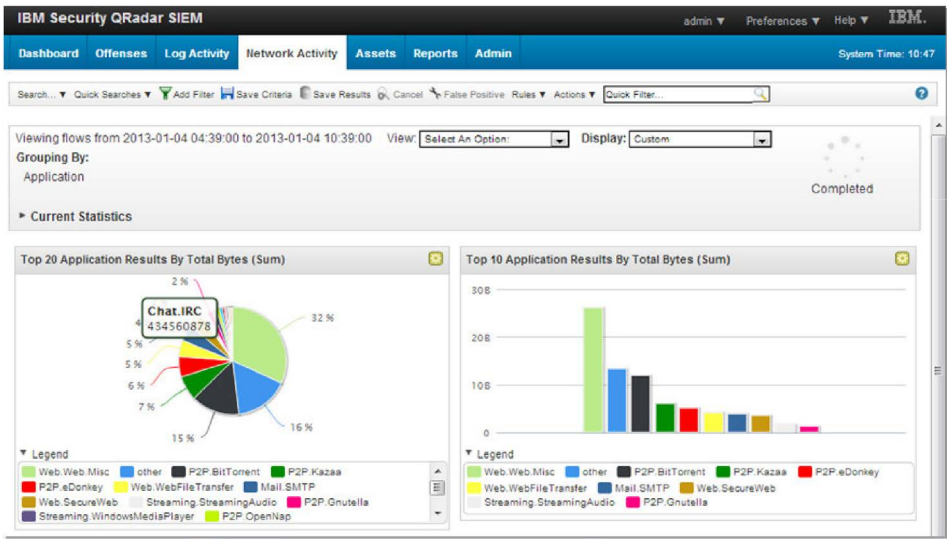
Fortinet and IBM Security QRadar Integrated Solution

IBM Security QRadar Security Intelligence Platform Integration with Fortinet FortiGate and FortiAnalyzer

Fortinet and IBM Security have partnered to integrate the IBM Security QRadar Security Intelligence Platform with Fortinet's FortiGate end-to-end next generation firewall platform. FortiGate log information can be forwarded by FortiAnalyzer to an upstream IBM Security QRadar deployment.

FortiGate

FortiGate firewalls can be deployed within a variety of different organizations including: MSSPs, datacenters, enterprise (NGFW) or small businesses (UTM). FortiGates support a comprehensive set of protection features such as anti-malware/AV, application control, data loss protection, email filtering, endpoint control, intrusion protection, vulnerability scanning and web filtering.



Risk	Application Name	Category	Technology	Bandwidth	Sessions
Botnet	Zeroaccess.Botnet	Botnet	Client-Server	17.57 KB	50
Evasive	WebEx	Collaboration	Browser-BasedClient-Server	41.16 MB	17.22 K
Evasive	Skype	P2P	Peer-to-Peer	5.78 MB	17.20 K
Evasive	Dropbox	File.Sharing	Browser-Based	8.12 GB	10.45 K
Evasive	Google.Docs	Collaboration	Browser-Based	1.17 MB	3.49 K
Evasive	Skype_Communication	P2P	Peer-to-Peer	592.29 KB	1.77 K
Evasive	Google.Desktop	General.Interest	Client-Server	1.36 GB	1.75 K
Evasive	EBay.Toolbar	General.Interest	Browser-Based	302.10 KB	908
Evasive	RDP	Remote.Access	Client-Server	382.62 MB	494
Evasive	SOCKS5	Proxy	Network-Protocol	163.26 KB	492
Evasive	Evernote	General.Interest	Browser-Based	163.71 KB	484
Evasive	Stumbleupon.Toolbar	General.Interest	Browser-Based	121.77 KB	357
Evasive	Yahoo.Toolbar	General.Interest	Browser-Based	114.54 KB	335
Evasive	Paypal	General.Interest	Browser-Based	111.93 KB	334
Evasive	Rss	Web.Others	Browser-Based	105.41 KB	314
Evasive	SOAP	Network.Service	Network-Protocol	100.60 KB	297
Evasive	Bitcomet.HTTP.Seed	P2P	Peer-to-Peer	77.66 KB	227
Evasive	Twitter	Social.Media	Browser-Based	72.35 KB	214
Evasive	Facebook.Chat	Social.Media	Browser-Based	60.52 KB	187
Evasive	Google.Earth	General.Interest	Client-Server	144.05 MB	180

Figure 1: FortiGate Application Visibility and Control.

IBM Security QRadar Security Intelligence Platform Provides

- Integrated log, threat, compliance management
- Asset profiling and flow analytics
- Offense management and workflow

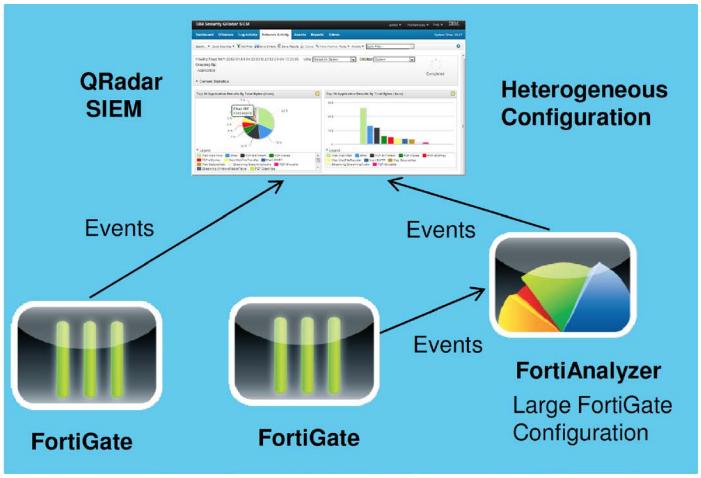
QRadar SIEM allows single pane troubleshooting of issues to create a Security Operations Center (SOC). Its powerful rules engine correlates data, detects anomalies and generates a manageable list of the highest priority risks requiring forensic investigation and remediation. QRadar SIEM derives value by working with best of breed products.

FORTINET Fabric-Ready

Premier Business Partner IBM
Ready For Security Intelligence

FortiAnalyzer

FortiAnalyzer provides event logging, security reporting and analysis functions for several key Fortinet products, including FortiGates. Security logs can be filtered and drilled-down to specific instances or security violations; alerts can also trigger for predefined criteria. IBM Security QRadar SIEM and the Fortinet products can be configured in several ways.



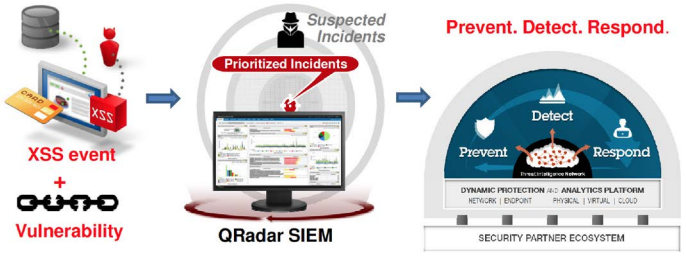
Indirect Logging to IBM Security QRadar Via FortiAnalyzer

In this scenario, FortiGates are configured to send event logs to a FortiAnalyzer. On the FortiAnalyzer, an IT administrator can view logs, run reports and correlate log information. While this is ideal for FortiGate-centric security deployments, large enterprises with heterogeneous environments may look for a full SIEM such as QRadar. In this case, the FortiAnalyzer can be configured to forward Syslog events to an upstream QRadar deployment.

Here are some real world examples of the value combining these products brings to customers.

1. Prevent Data Loss

- The SOC analyst responsible for the credit card gateways and servers at an international retailer receives an email alert from QRadar due to cross-site scripting activity. This alert is sent when QRadar detects several cross-site scripting events from a Fortinet FortiGate on 2 servers that are vulnerable. The analyst patches the vulnerable hosts and prevents personally identifiable information (PII) data from being sent to the attacker.



2. Virus detected and remediated

- A university with several campuses is running QRadar and FortiAnalyzer. FortiAnalyzer sends QRadar 4 virus blocked events, followed by a “virus detected” event. QRadar generates an offense when the FortiAnalyzer virus detected event is correlated with several virus events reported by endpoint solutions on critical assets. The university security analyst sees all of the endpoints that need to be cleaned and prioritizes them based on the asset weight, which reflects the business importance.

3. DoS attack stopped

- The network administrators at a national bank go on alert when they see a DoS attack offense on their QRadar dashboard. Based on the offense, the administrator sees the FortiGate DoS event and the flows and network traffic that triggered the offense. She reacts immediately to write a rule for her FortiGate IPS that will block such traffic, and stops the attack.

These examples show how QRadar can leverage the value of best of breed products customers have already invested in throughout their infrastructure and enable them to reach their compliance and security goals.

Integrating FortiGate and FortiAnalyzer with QRadar enables data centers, enterprises and small to medium size businesses to improve their security posture and protect their organization from malware and viruses, application vulnerabilities, data loss, spam, and other threats.

FORTINET

www.fortinet.com

June 8, 2019 5:17 AM

D:\Fortinet\Solution Brief\TEAL SB\Fortinet QRadar IBM\FA - SB - Fortinet QRadar IBM

59887-B-0-EN