DATA SHEET

FortiMonitor®

Unified event correlation and risk management for modern networks

FortiMonitor

Unified event correlation and risk management for modern networks

Network devices in modern enterprises must be proactively monitored on a constant basis in order to detect potential vulnerabilities and security anomalies. Nearly 85% of all breached organizations have evidence of vulnerabilities during post-mortem log analysis. The challenge for security administrators is to determine which of these vulnerabilities are most indicative of a future breach. Without advanced correlation combined with machine learning, this task becomes difficult and time consuming.

FortiMonitor utilizes big data analytics to provide a holistic view of your network security. Interoperating in conjunction with the Fortinet portfolio and/or third-party products, FortiMonitor gives you the visibility you need to identify future attack vectors within your network. It effectively gives you the ability to locate and prioritize vulnerabilities in your front-line security before attackers can exploit them.

Key Features & Benefits

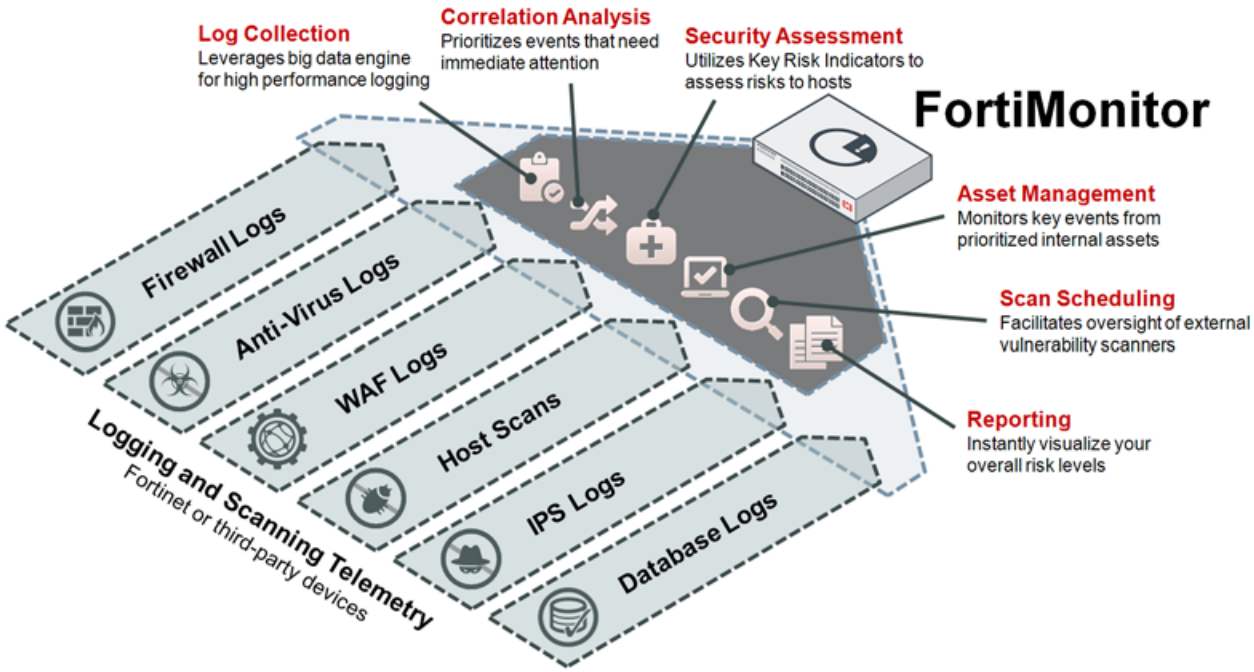
High performance host and security logging	Powerful, big data engine quickly identifies threats and areas of enterprise concern
Multiple vendor device support	Aggregate Fortinet or third-party logs without the need to invest in a homogenous network
Correlate vulnerable hosts with potentially malicious activity	Locate susceptible hosts based on current security exploit activity
Visualize threats at the speed of business	Large enterprises and service providers can visualize risks with a single, unified console

FortiMonitor utilizes big data analytics to provide a holistic view of your network security.

Highlights

- Log collection with enterprise performance
- Correlation automatically determines priority threats
- Assess your network's Key Risk Indicators
- Manage host assets critical to your network
- Schedule regular vulnerability scans
- Visualize your holistic security with dashboards and reports

DEPLOYMENT



FEATURES

Asset Management

FortiMonitor allows administrators to monitor security events from defined internal assets. These assets can include individual hosts/devices, groups of hosts (including groupings by region), websites and network segments. Risks can then be determined from assets based on resultant vulnerability scans correlated with other security events. Assets can also be individually queried and rated for their resilience against varying attack types on an ad-hoc basis.

Log Collection and Normalization

When overseeing your enterprise security, the ability to collect and categorize logs from disparate devices is crucial. The relationships between devices are inherently difficult to normalize — parsers often need to be written to determine field mappings and security indicators are typically vendor specific. FortiMonitor is able to collect logs at speeds in excess of 120,000 logs per second from a myriad of vendor devices. Collected events are instantly normalized pursuant to the FortiMonitor knowledge base so fields can be further classified and correlated in a uniformed fashion.

Vulnerability Scanning

FortiMonitor can centrally manage and schedule a diverse set of third party vulnerability scanners. This will allow you to spend less time administrating individual vulnerability scanners and more time analyzing scan results. Results are also merged, allowing you to see vulnerability data using standard reference codes such as CVE and BugTraq. FortiMonitor supports eight industry leading scanning platforms out of the box.

Correlation Analysis

While individual security events can be indicative of potential vulnerabilities or malicious activity, it is often difficult to assign an importance to addressing them. By correlating events, you can immediately understand which assets need instant attention. For example, a vulnerability scan may uncover a potential SQL injection attack vector on a specific host. That same host may be the target of a set of external application attacks. Individually, these events may be flagged as low priority risks, but when combined they are indicative of an imminent breach.

FortiMonitor provides four types of correlation: cross correlation (target has the vulnerability that the attack exploits), inventory correlation (target has the OS/services that the attack exploits), asset correlation (based on the calculated asset value) and logical correlation (based on the number of attacks).

FEATURES

Security Assessment

By utilizing Key Risk Indicators (KRIs), FortiMonitor is able to assess security risks to a variety of targets including your entire network, regions, hosts groups, websites or individual devices. The more potential attack vectors assigned to a target, the higher the risk rating. Key Risk Indicators are based on a multitude of threat growth statistics (such as discovering malware or system/website attacks) combined with the detection of asset vulnerabilities (such as system or website vulnerabilities).

Reporting

In addition to drill-down style visibility, FortiMonitor supports several predefined reports which can be scheduled or run in ad-hoc fashion. Reports can also be customized with a detailed set of fields to choose from. Assess your current overall risk levels with KPI reporting or determine the security posture of specific assets at specific locations. FortiMonitor gives you the forewarning you need to ensure you're protected from any potential security incidents.

SPECIFICATIONS

	FORTIMONITOR 3000D
Hardware Specifications	
Hardware Form Factor	3 RU Rackmount
Total Interfaces	12x GE SFP+
Storage Capacity	48 TB (12 blades, 2x 2 TB each)
Removable Blades	12
Redundant Hot Swap Power Supplies	Yes
Environment	
AC Power Supply	100–240V AC, 50–60 Hz, 12 Amp Maximum
Power Consumption (Maximum)	1620 W
Heat Dissipation	5562 BTU/h
Operating Temperature	50–95°F (10–35°C)
Storage Temperature	-40–158°F (-40–70°C)
Humidity	8–90% non-condensing

	FORTIMONITOR 3000D
Compliance	
Safety Certifications	FCC Class A Part 15, UL/CB/cUL, C-Tick, VCCI, CE
Dimensions	
Height x Width x Length (inches)	5.21 x 17.5 x 29.5
Height x Width x Length (mm)	132 x 444.5 x 749.3
Weight	120 lbs (54.4 kg)

ORDER INFORMATION

Product	SKU	Description
FortiMonitor 3000D	FMR-3000D	Unified Risk Management System — 12 blades includes 12 IPMI Ports + 12x 10 GE SFP+

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
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480