FortiAnalyzer

Instant visibility, situation awareness, real-time threat intelligence and actionable analytics for **Fortinet's Security Fabric**

Event Correlation & Advanced Threat Detection

Allows IT administrators to quickly identify and respond to network security threats across the network

Powerful NOC/SOC Dashboard

Customizable NOC/SOC dashboards provide management, monitoring and control over your network.

Scalable Performance & Flexible Deployments

Supports thousands of FortiGate and FortiClient™ agents, and dynamically scale storage based on retention requirements. Deploys as an individual unit or optimized for a specific operation.

Hardware:
400E, 1000E, 2000E, 3000F, 3500F, 3700F 3900E and FAZ-VM

FortiCare Worldwide
24/7 support
support.fortinet.com

FortiGuard Security
Services
www.fortiguard.com

DATA SHEET

FortiAnalyzer

FortiAnalyzer 400E, 1000E, 2000E, 3000F, 3500F, 3700F, 3900E and FAZ-VM

Enterprise networks are constantly evolving due to organization growth and regulatory or business requirements, which results in mountains of data from security appliances and no visibility into historic context for dynamic threats. With today's complex and rapidly changing threat landscape, these threats can remain undetected for an extremely long time.

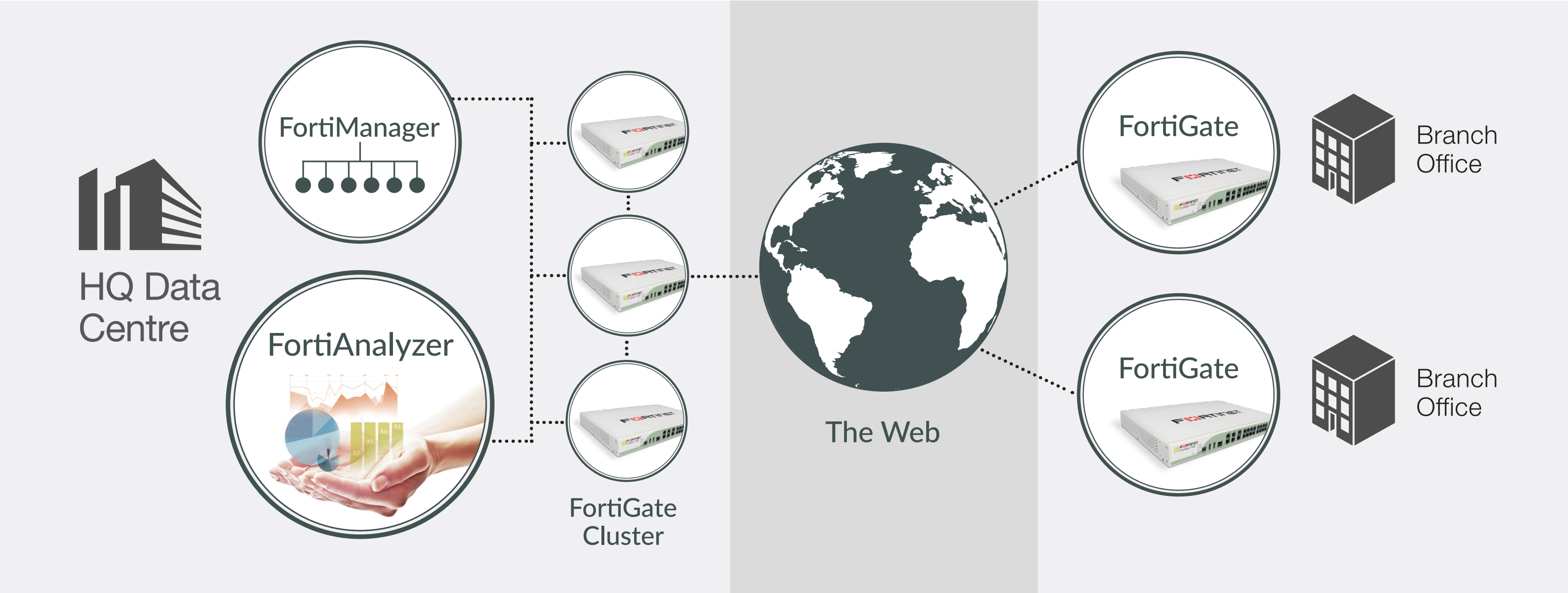
This is where Fortinet Security Fabric can provide unified, end-to-end protection by deploying Fortinet Enterprise Firewalls to battle the advanced persistent threats, and adding FortiAnalyzer to expand the Security Fabric for increased visibility and robust security alert information that is both actionable and automated.

FortiAnalyzer enables you to collect, analyze and correlate log data from your distributed network of Fortinet Enterprise Firewalls from one central location, and to view all your firewall traffic and generate reports from a single console. With a subscription to FortiGuard Indicator of Compromise (IOC) service, it can provide a prioritized list for compromised hosts, so you can quickly take action.

Key Features & Benefits

Centralized Search and Reports	Simple and intuitive Google-like search experience and reports on network traffic, threats, network activities and trends across the network.
Automated Indicators of Compromise (IOC)	Scans security logs using FortiGuard IOC Intelligence for APT detection.
Real-time and Historical Views into Network Activity	View a summary of applications, sources, destinations, websites, security threats, administrative modifications and system events.
Light-weight Event Management	Predefined security event definitions are easily customizable with automated alerts.
Seamless Integration with the Fortinet Security Fabric	Correlates with logs from FortiClient, FortiSandbox, FortiWeb and FortiMail for deeper visibility.

Deployment Diagram



Fortinet Security Fabric protects enterprises from IOT to Cloud. FortiAnalyzer collects and correlates network and security information from the fabric and presents them from a single management console: forti.net/sf

Feature Highlights

FortiView — Powerful Network Visibility

- Customizable interactive dashboard to rapidly pinpoint problems
- Intuitive summary views (Fig. 1) of network traffic, threats, applications and more
- Granular views of wireless users, rogue access points and endpoint vulnerabilities
- Visualization with graphical charts and maps
- Drill-down to follow the trail of an attacker, trace transactions and gain new insights

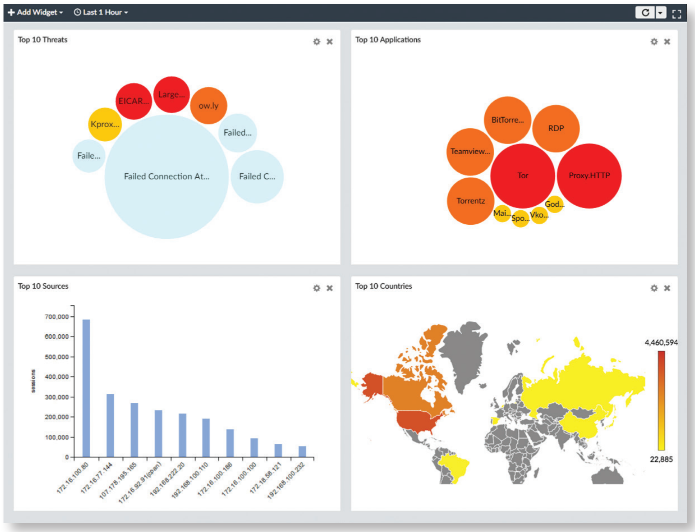


Figure 1

Indicators of Compromise — with FortiGuard Threat Intelligence

- Scans security logs to identify suspicious traffic patterns
- Automated breach defense system continuously monitors your network for signs of compromise
- Presents a prioritized list of possible compromised hosts for action
- Improves security posture and safeguards organizations through detection of advanced threats

Multi-tenancy with Flexible Quota Management

- Time-based archive/analytic log data policy per Administrative Domain (ADOM)
- Automated quota management based on the defined policy
- Trending graphs to guide policy configuration and usage monitoring

Report

- 28+ built-in templates with sample reports ready for use
- Run report on-demand or on a schedule with automated email notification and Calendar view
- Flexible report formats: HTML/CSV/XML/PDF
- Custom reports: 300+ built-in charts ready for custom reports

Log Fetch for Forensic Analysis

- Retrieve archived logs to perform analytics against historic data
- Flexible fetch options: fetch all or select logs of interest using filters
- Easy to configure: set up remote fetching between client and server in just a few clicks

Log Forwarding for Third-Party Integration

- Forward logs to a Syslog server, a CEF log server, a FortiSIEM or a FortiAnalyzer for long-term storage, forensics or regulatory compliance
- Flexible configuration: forward all logs or logs of interest using filters
- Control which log fields are sent to Syslog of CEF servers

Monitor and Alert

- Proactively monitors your network in real time to identify attacks
- 20+ built-in event definitions ready for use and highly customizable
- Automated alert notification for rapid response
- Drill-down to event details for fast investigation

Network Operation Center (NOC) and Security Operation Center (SOC)

- provides centralized monitoring and awareness of the threats, events and network activity. Use the predefined FAZ dashboards or customize your own. (Fig. 2)

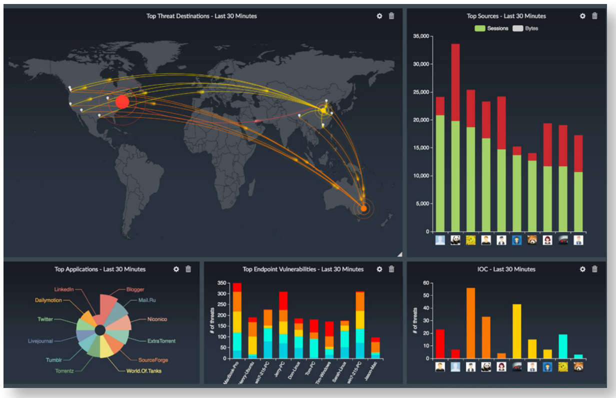


Figure 2.

Specifications	FORTIANALYZER 400E	FORTIANALYZER 1000E	FORTIANALYZER 2000E
CAPACITY AND PERFORMANCE			
GB/Day of Logs	200	600	1,000
Analytic Sustained Rate (logs/sec)[1]	6,000	18,000	30,000
Collector Sustained Rate (logs/sec)[1]	9,000	27,000	45,000
Devices/VDOMs/ADOMs (Maximum)	200	2,000	2,000
Max Number of Days Analytics[2]	30	30	30
OPTIONS SUPPORTED			
FortiGuard Indicator of Compromise (IOC)	✓	✓	✓
FortiManager Capabilities (up to 20 devices)	No	✓	✓
HARDWARE SPECIFICATIONS			
Form Factor	1 RU Rackmount	2 RU Rackmount	2 RU Rackmount
Total Interfaces	4x GE	2x GE	4x GE, 2x 10GE SFP+
Storage Capacity	12 TB (4x 3 TB)	24 TB (8x 3 TB)	36 TB (12x 3TB)
Usable Storage (After RAID)	6TB	18 TB	30 TB
Removable Hard Drives	✓	✓	✓
RAID Levels Supported	RAID 0/1/5/10	RAID 0/1/5/6/10/50/60	RAID 0/1/5/6/10/50/60
Default RAID Level	10	50	50
Redundant Hot Swap Power Supplies	No	✓	✓
DIMENSIONS			
Height x Width x Length (inches)	1.7 x 17.2 x 19.8	3.5 x 17.2 x 25.2	3.5 x 17.2 x 25.6
Height x Width x Length (cm)	4.3 x 43.7 x 50.3	8.9 x 43.7 x 68.4	8.9 x 43.7 x 64.8
Weight	31 lbs (14.1 kg)	52 lbs (23.6 kg)	58 lbs (26.3 kg)
ENVIRONMENT			
AC Power Supply	100–240V AC, 60–50 Hz	100–240V AC, 60–50 Hz	100–240V AC, 60–50 Hz
Power Consumption (Average)	93 W	192.5 W	293.8 W
Heat Dissipation	456 BTU/h	920 BTU/h	1840 BTU/h
Operating Temperature	41–95°F (5–35°C)	41–95°F (5–35°C)	50–95°F (10 – 35°C)
Storage Temperature	-40–140°F (-40–60°C)	-40–140°F (-40–60°C)	-40–158°F (-40–70°C)
Humidity	8– 90% non-condensing	8–90% non-condensing	8–90% non-condensing
Operating Altitude	Up to 9,842 ft (3,000 m)	Up to 7,400 ft (2,250 m)	Up to 7,400 ft (2,250 m)
COMPLIANCE			
Safety Certifications	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB

[1] Sustained Rate - maximum constant log message rate that the FAZ platform can maintain for minimum 48 hours without SQL database and system performance degradation.

[2] Max number of days increase with lower log rates.

Specifications

	FORTIANALYZER 3000F	FORTIANALYZER 3500F	FORTIANALYZER 3700F	FORTIANALYZER 3900E
CAPACITY AND PERFORMANCE				
GB/Day of Logs	3,000	5,000	8,300	4,000
Analytic Sustained Rate (logs/sec)	42,000	63,000	100,000	72,000
Collector Sustained Rate (logs/sec)	60,000	90,000	150,000	108,000
Devices/VDOMs/ADOMs (Maximum)	4,000	10,000	10,000	10,000
Max Number of Days Analytics	21	30	60	5
OPTIONS SUPPORTED				
FortiGuard Indicator of Compromise (IOC)	✓	✓	✓	✓
FortiManager Capabilities (up to 20 devices)	✓	✓	✓	✓
HARDWARE SPECIFICATIONS				
Form Factor	3 RU Rackmount	4 RU Rackmount	4 RU Rackmount	2 RU Rackmount
Total Interfaces	4x GE, 2x GE SFP	2x GE, 2x GE SFP	2xSFP+, 2x1GE	2x GE, 2x 10GE SFP+
Storage Capacity	48 TB (16x 3 TB – 48 TB max)	72 TB (24x 3TB)	240 TB (60x4TB SAS HDDs)	15 TB SSD (15x 1 TB SSD)
Usable Storage (After RAID)	42 TB	63 TB	216TB	12 TB
Removable Hard Drives and Redundant Hot Swap Power Supplies	✓	✓	✓	✓
RAID Levels Supported	RAID 0/1/5/6/10/50/60	RAID 0/1/5/6/10/50/60	RAID 0/1/5/6/10/50/60	RAID 0/1/5/6/10/50/60
Default RAID Level	50	50	50	50
DIMENSIONS				
Height x Width x Length (inches)	5.2 x 17.2 x 25.5	6.9 x 19.0 x 27.2	7 x 17.2 x 30.2	3.5 x 17.2 x 26.9
Height x Width x Length (cm)	13.2 x 43.7 x 64.8	17.6 x 48.2 x 69.0	17.8 x 43.7 x 76.7	8.9 x 43.7 x 68.4
Weight	76 lbs (34.5 kg)	93.74 lbs (42.52Kg)	118 lbs (53.5Kg)	52 lbs (23.6 kg)
ENVIRONMENT				
AC Power Supply	100–240V AC, 50–60 Hz, 11.5 Amp Maximum	100–240V AC, 60–50 Hz	100-240V AV, 60-50 Hz	100–240V AC, 50–60 Hz, 11.5 Amp Maximum
Power Consumption (Average)	449 W for 12 HDD	465 W	850 W	470 W for 15 HDD
Heat Dissipation	1846.5 BTU/h	1,904 BTU/h	4858 BTU/h	1351 BTU/h
Operating Temperature	50–95°F (10–35°C)	32–104°F (0–40°C)	50–95°F (10–35°C)	50–95°F (10–35°C)
Storage Temperature	-40–158°F (-40–70°C)	-13–158°F (-25–70°C)	-40–158°F (-40–70°C)	-40–140°F (-40–60°C)
Humidity	8–90% non-condensing	10–90% non-condensing	8% to 90% (non-condensing)	5–95% non-condensing
Operating Altitude	Up to 7,400 ft (2,250 m)	Up to 7,400 ft (2,250 m)	Up to 7,000 ft (35°C ambient)	Up to 7,400 ft (2,250 m)
COMPLIANCE				
Safety Certifications	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB

	FAZ-VM-BASE	FAZ-VM-GB1	FAZ-VM-GB5	FAZ-VM-GB25	FAZ-VM-GB100	FAZ-VM-GB500	FAZ-VM-GB2000
CAPACITY AND PERFORMANCE							
GB/Day of Logs	1 incl.*	+1	+5	+25	+100	+500	+2,000
Storage Capacity	500 GB	+500 GB	+3 TB	+10 TB	+24 TB	+48 TB	+100 TB
Devices/ADOMs/VDOMs Supported (Maximum)	10,000	10,000	10,000	10,000	10,000	10,000	10,000
HYPERVISOR REQUIREMENTS							
Hypervisor Support	VMware ESX/ESXi 4.0/4.1/5.0/5.1/5.5/6.0, Microsoft Hyper-V 2008 R2/2012/2012 R2, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure						
Network Interface Support (Minimum / Maximum)	1 / 4						
vCPUs (Minimum / Maximum)	2/ Unlimited						
Memory Support (Minimum / Maximum)	4 GB / Unlimited						

* Unlimited GB/Day when deployed in collector mode

Order Information

PRODUCT	SKU	DESCRIPTION
FortiAnalyzer 400E	FAZ-400E	Centralized log and analysis appliance — 4x GE RJ45, 12 TB storage, up to 200 GB/day of logs.
FortiAnalyzer 1000E	FAZ-1000E	Centralized log and analysis appliance — 2x GE RJ45, 24 TB storage, dual power supplies, up to 650 GB/day of logs.
FortiAnalyzer 2000E	FAZ-2000E	Centralized log and analysis appliance — 4x GE RJ45, 2x SFP+, 36 TB storage, dual power supplies, up to 1,000 GB/day of logs.
FortiAnalyzer 3000F	FAZ-3000F	Centralized log and analysis appliance — 4x GE RJ45, 2x SFP+, 48 TB storage, dual power supplies, up to 3,000 GB/day of logs.
FortiAnalyzer 3500F	FAZ-3500F	Centralized log and analysis appliance — 2x GE RJ45, 2x GE SFP slots, 72 TB storage, dual power supplies, up to 5,000 GB/day of logs.
FortiAnalyzer 3700F	FAZ-3700F	Centralized log and analysis appliance — 2x SFP+, 2x1GE slots, 240 TB storage, dual power supplies, up to 8,300 GB/day of logs.
FortiAnalyzer 3900E	FAZ-3900E	Centralized log and analysis appliance — 2x GE RJ45, 2x SFP+ slots, flash-based 15 TB SSD storage, dual power supplies, up to 4,000 GB/day of logs.
FortiAnalyzer VM	FAZ-VM-BASE	Base license for stackable FortiAnalyzer VM; 1 GB/day of logs and 500 GB storage capacity. Unlimited GB/day when used in collector mode only. Designed for VMware vSphere, Xen, KVM and Hyper-V platforms.
	FAZ-VM-GB1	Upgrade license for adding 1 GB/day of logs and 500 GB storage capacity.
	FAZ-VM-GB5	Upgrade license for adding 5 GB/day of logs and 3 TB storage capacity.
	FAZ-VM-GB25	Upgrade license for adding 25 GB/day of logs and 10 TB storage capacity.
	FAZ-VM-GB100	Upgrade license for adding 100 GB/day of logs and 24 TB storage capacity.
	FAZ-VM-GB500	Upgrade license for adding 500 GB/day of logs and 48 TB storage capacity.
	FAZ-VM-GB2000	Upgrade license for adding 2 TB/Day of Logs and 100 TB storage capacity.
FortiAnalyzer VM for AWS	FAZ-VM-BASE-AWS	Base license for stackable FortiAnalyzer VM; 1 GB/day of logs and 500 GB storage capacity. Unlimited GB/day when used in collector mode only. Designed for Amazon Web Services (AWS) platform.
	FAZ-VM-GB1-AWS	Upgrade license for adding 1 GB/day of logs and 500 GB storage capacity.
	FAZ-VM-GB5-AWS	Upgrade license for adding 5 GB/day of logs and 3 TB storage capacity.
	FAZ-VM-GB25-AWS	Upgrade license for adding 25 GB/day of logs and 10 TB storage capacity.
	FAZ-VM-GB100-AWS	Upgrade license for adding 100 GB/day of logs and 24 TB storage capacity.
	FAZ-VM-GB500-AWS	Upgrade license for adding 500 GB/day of logs and 48 TB storage capacity.
	FAZ-VM-GB2000-AWS	Upgrade license for adding 2 TB/day of logs and 100 TB storage capacity.
	FortiAnalyzer AWS On-Demand	https://aws.amazon.com/marketplace/pp/B01N5K7210/ref=portal_asin_url
FortiAnalyzer VM for Azure	FAZ-VM-BASE-AZ	Base license for stackable FortiAnalyzer VM; 1 GB/day of logs and 500 GB storage capacity. Unlimited GB/day when used in collector mode only. Designed for Azure platform.
	FAZ-VM-GB1-AZ	Upgrade license for adding 1 GB/day of logs and 500 GB storage capacity.
	FAZ-VM-GB5-AZ	Upgrade license for adding 5 GB/day of logs and 3 TB storage capacity.
	FAZ-VM-GB25-AZ	Upgrade license for adding 25 GB/day of logs and 10 TB storage capacity.
	FAZ-VM-GB100-AZ	Upgrade license for adding 100 GB/day of logs and 24 TB storage capacity.
	FAZ-VM-GB500-AZ	Upgrade license for adding 500 GB/day of logs and 48 TB storage capacity.
	FAZ-VM-GB2000-AZ	Upgrade license for adding 2 TB/day of logs and 100 TB storage capacity.
FortiAnalyzer Add-on Management Capabilities	FAZ-MGMT20	License to add FortiManager capabilities for up to 20 devices (1000 series and above — hardware only).
FortiGuard Indicator of Compromise (IOC) Subscription	FC-10-[Model code]-149-02-DD	1 Year Subscription license for the FortiGuard Indicator of Compromise (IOC).

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

EMEA SALES OFFICE
905 rue Albert Einstein
Valbonne 06560
Alpes-Maritimes, France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6395.2788

LATIN AMERICA SALES OFFICE
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
United States
Tel: +1.954.368.9990

Copyright© 2017 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, 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 Counsel, 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. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. 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.