DATA SHEET

FortiAnalyzer™

Centralized logging, analytics and reporting

FortiAnalyzer

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

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

Instant Visibility, Fast Incident Response

This is where Fortinet Security Fabric comes into the picture for unified, end-to-end protection — deploying Fortinet Enterprise Firewalls to battle the advanced persistent threats, and adding FortiAnalyzer to expand the Security Fabric for increased visibility, 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 etc for deeper visibility.

FORTINET SECURITY FABRIC

Fortinet Security Fabric protects enterprise from IOT to Cloud. FortiAnalyzer collects and correlates network and security information from the fabric and present them from a single management console.

forti.net/sf

FortiCare Worldwide 24x7 Support
support.fortinet.com

FortiGuard Security Services
www.fortiguard.com

HIGHLIGHTS

FortiView — Powerful Network Visibility

- Customizable interactive dashboard to rapidly pinpoint and resolve problems
- Intuitive summary views of network traffic, threats, applications and many more
- Granular views of wireless users, rouge access points and endpoint vulnerabilities
- Visualization with graphical bubble charts, and a geographical Threat Map
- Drill-down to follow the trail of an attacker, trace transactions, and gain new insights

FortiGuard Indicators of Compromise — Automated Correlation Engine

- Scans FortiGate security logs to identify suspicious traffic patterns
- Automated breach defense system that continuously monitors your network for attacks
- Presents a prioritized list of hosts which are compromised and required further action
- IOC improves security posture and helps safeguard organizations through accurate detection of advanced threats

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 for custom reports, and an intuitive chart builder helps to easily build custom graphs and charts from log view search results

Monitor and Alert

- Proactively monitors your network in real time to identify issues, problems, and 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

Multi-tenancy with Flexible Quota Management

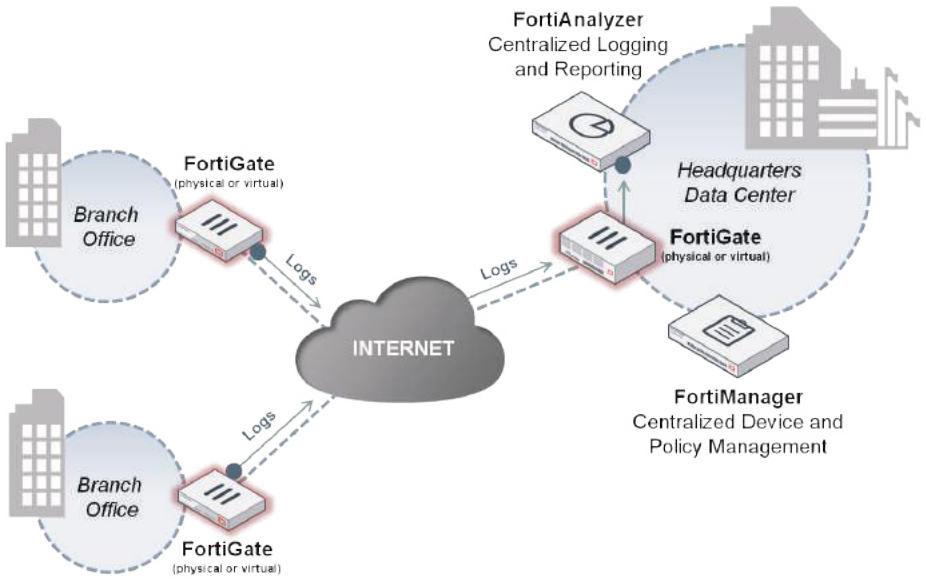
- Time-based archive/analytic log data policy per Administrative Domain (ADOM)
- Automated quota management based on the defined policy
- Trending graphs to guide the policy configuration and usage monitoring

Log Fetch for Forensic Analysis

- Retrieve archived logs to perform analytics against historic data for forensic analysis
- Flexible fetch options: fetch all or selected logs for the specified time period
- 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 systems such as a Syslog server, a CEF log server or a FortiAnalyzer for purposes of long-term storage, forensics or regulatory compliance
- Flexible configuration: forward all logs, or configure to only forward logs of interest using filters
- Control which log fields are sent to Syslog of CEF servers



SPECIFICATIONS

	FORTIANALYZER 400E	FORTIANALYZER 1000E	FORTIANALYZER 2000E
Capacity and Performance			
GB/Day of Logs	75	300	500
Analytic Sustained Rate (logs/sec)	500	4,000	7,500
Collector Sustained Rate (logs/sec)	725	6,000	11,250
Devices/VDOMs/ADOMs (Maximum)	200	2,000	2,000
Options Supported			
FortiGuard Indicator of Compromise (IOC)	Yes	Yes	Yes
FortiManager Capabilities (up to 20 devices)	No	Yes	Yes
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)
Removable Hard Drives	Yes	Yes	Yes
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	Yes	Yes
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	390 W
Heat Dissipation	456 BTU/h	920 BTU/h	1840 BTU/h
Operating Temperature	32–104°F (0–40°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

FortiAnalyzer 400E

FortiAnalyzer 1000E

FortiAnalyzer 2000E

SPECIFICATIONS

	FORTIANALYZER 3000F	FORTIANALYZER 3500F	FORTIANALYZER 3900E
Capacity and Performance			
GB/Day of Logs	1,600	5,000	4,000
Analytic Sustained Rate (logs/sec)	35,000	60,000	48,000
Collector Sustained Rate (logs/sec)	52,500	90,000	75,000
Devices/VDOMs/ADOMs (Maximum)	4,000	10,000	10,000
Options Supported			
FortiGuard Indicator of Compromise (IOC)	Yes	Yes	Yes
FortiManager Capabilities (up to 20 devices)	Yes	Yes	Yes
Hardware Specifications			
Form Factor	3 RU Rackmount	4 RU Rackmount	2 RU Rackmount
Total Interfaces	4x GE, 2x 10GE SFP+	2x GE, 2x GE SFP	2x GE, 2x 10GE SFP+
Storage Capacity	48 TB (16x 3 TB)	72 TB (24x 3TB)	15 TB SSD (15x 1 TB SSD)
Removable Hard Drives	Yes	Yes	Yes
RAID Storage Management	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
Redundant Hot Swap Power Supplies	Yes	Yes	Yes
Dimensions			
Height x Width x Length (inches)	5.2 x 17.2 x 25.5	6.9 x 19.0 x 27.2	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	8.9 x 43.7 x 68.4
Weight	76 lbs (34.5 kg)	93.74 lbs (42.52Kg)	52 lbs (23.6 kg)
Environment			
AC Power Supply	100–240V AC, 60–50 Hz	100–240V AC, 60–50 Hz	100–240V AC, 50–60 Hz, 11.5 Amp Maximum
Power Consumption (Average)	465 W	465 W	470 W for 15 HDD
Heat Dissipation	1904 BTU/h	1,904 BTU/h	1637 BTU/h
Operating Temperature	50–95°F (10–35°C)	32–104°F (0–40°C)	50–95°F (10–35°C)
Storage Temperature	-40–158°F (-40–70°C)	-13–158°F (-25–70°C)	-40–60°C (-40–140°F)
Humidity	8–90% non-condensing	10–90% 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 7,400 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

FortiAnalyzer 3000F

FortiAnalyzer 3500F

FortiAnalyzer 3900E

	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
Options Supported							
FortiGuard Indicator of Compromise (IOC)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
FortiManager Capabilities (up to 20 devices)	No	No	No	No	No	No	No
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)	1 / Unlimited						
Memory Support (Minimum / Maximum)	1 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 75 GB/day of logs.
FortiAnalyzer 1000E	FAZ-1000E	Centralized log and analysis appliance — 2x GE RJ45, 24 TB storage, dual power supplies, up to 300 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 500 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 1,600 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 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 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).