FURTINET

FortiAnalyzer

In today's dynamic and fast changing security landscape, lack of visibility continues to extend breach and compromise events to an average of more than 100 days. For each day an organization is exposed it's another opportunity for attackers to get to sensitive customer and confidential information. FortiAnalyzer delivers critical insight into threats across the entire attack surface and provides Instant visibility, situation awareness, real-time threat intelligence and actionable analytics, along with NOC-SOC security analysis and operations perspective for Fortinet's Security Fabric.

Centralized Analysis

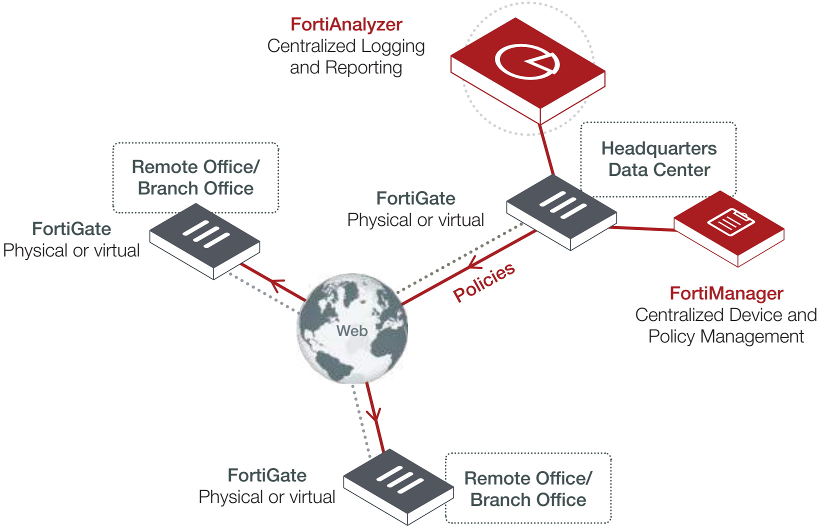
Event Correlation & Advanced Threat Detection - Allows IT administrators to quickly identify and respond to network security threats across the network

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.

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.



Features

- 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.

DATA SHEET

Feature Highlights

Incident Response

FortiAnalyzer's Incident Response capability improves Management & Analytics with focus on event management and identification of compromised endpoints. Use improved default and custom event handlers to detect malicious and suspicious activities on the spot. Integration of events with the FOS automation framework for automated endpoint quarantine. Incident detection and tracking, as well as evidence collection and analysis are streamlined through integration with ITSM platforms, helping to bridge gaps in your Security Operations Center and reinforce your Security Posture.

FortiView — Powerful Network Visibility

Provides a customizable interactive dashboard that helps you rapidly pinpoint problems, with intuitive summary views (Fig. 1) of network traffic, threats, applications and more. FortiView is a comprehensive monitoring system for your network that integrates real-time and historical data into a single view. It can log and monitor threats to networks, filter data on multiple levels, keep track of administrative activity, and more.

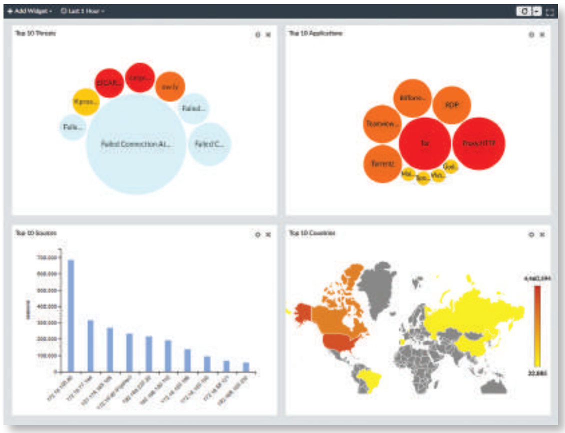


Figure 1

Indicators of Compromise

The Indicators of Compromise (IOC) summary shows end users with suspicious web usage compromises. It provides information such as end users' IP addresses, host name, group, OS, overall threat rating, a Map View, and number of threats. You can drill down to view threat details. To generate the Indicators of Compromise, FortiAnalyzer checks the web filter logs of each end user against its threat database. When a threat match is found, a threat score is given to the end user. FortiAnalyzer aggregates the threat scores of an end user and gives its verdict of the end user's overall Indicators of Compromise. The Indicators of Compromise summary is produced through the UTM web filter of FortiGate devices and FortiAnalyzer subscription to FortiGuard to keep its local threat database synced with the FortiGuard threat database.

Reports

You can generate custom data reports from logs by using the Reports feature. FortiAnalyzer provides 30+ built-in templates that are ready to use, with sample reports to help identify the right report for you. Run reports on-demand or on a schedule with automated email notifications, uploads and a easy to manage calendar view. Create custom reports with the 300+ built-in charts and datasets ready for creating your own custom reports, with flexible report formats include PDF, HTML, CSV and XML.

Monitor and Alert

Event handlers define what messages to extract from logs and display in Event Management. You must enable an event handler to start generating events. You can configure event handlers to generate events for a specific device, for all devices, or for the local FortiAnalyzer unit. You can create event handlers for FortiGate, FortiCarrier, FortiCache, FortiMail, FortiManager, FortiWeb, FortiSandbox devices, and syslog servers. You can configure the system to send you alerts for event handlers via email address, SNMP community, or syslog server.

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

FortiAnlyzers NOC-SOC is a management center that helps you secure your overall network by providing actionalble log and threat data. The SOC helps you protect your network, web sites, applications, databases, servers and data centers, and other technologies, with centralized monitoring and awareness of the threats, events and network activity, using the predefined FAZ dashboards and widgets, or customize your own, delivered through a single-pane-of-glass interface for easy integration into your Security Fabric. (fig 2.)

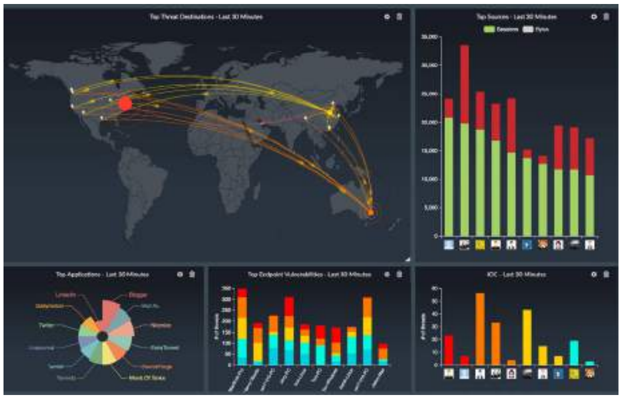

Top Threat Destinations - Last 30 Minutes
Top Sources - Last 30 Minutes
Sessions
Bytes
Top Applications - Last 30 Minutes
Top Endpoint Vulnerabilities - Last 30 Minutes
IOC - Last 30 Minutes

Figure 2.

Log Fetch for Forensic Analysis

Log fetching is used to retrieve archived logs from one FortiAnalyzer device to another. This allows administrators to run queries and reports against historic data, which can be useful for forensic analysis. A FortiAnalyzer device can be either the fetch server or the fetching client, and it can perform both roles to retrieve the log data for a specified device and time period, based on specified filters. The retrieved data are then indexed, and can be used for data analysis and reports.

Log Forwarding for Third-Party Integration

You can forward logs from a FortiAnalyzer unit to another FortiAnalyzer unit, a syslog server, or a Common Event Format (CEF) server. The client is the FortiAnalyzer unit that forwards logs to another device. The server is the FortiAnalyzer unit, syslog server, or CEF server that receives the logs. In addition to forwarding logs to another unit or server, the client retains a local copy of the logs. The local copy of the logs is subject to the data policy settings for archived logs. Logs are forwarded in real-time or near real-time as they are received. Forwarded content files include: DLP files, antivirus quarantine files, and IPS packet captures.

Analyzer-Collector mode

You can deploy in Analyzer mode and Collector mode on different FortiAnalyzer units and make the units work together to improve the overall performance of log receiving, analysis, and reporting. When FortiAnalyzer is in Collector mode, its primary task is forwarding logs of the connected devices to an Analyzer and archiving the logs. The Analyzer offloads the log receiving task to the Collector so that the Analyzer can focus on data analysis and report generation. This aximizes the Collector's log receiving performance. (Figure 3)

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, and trending graphs to guide policy configuration and usage monitoring.

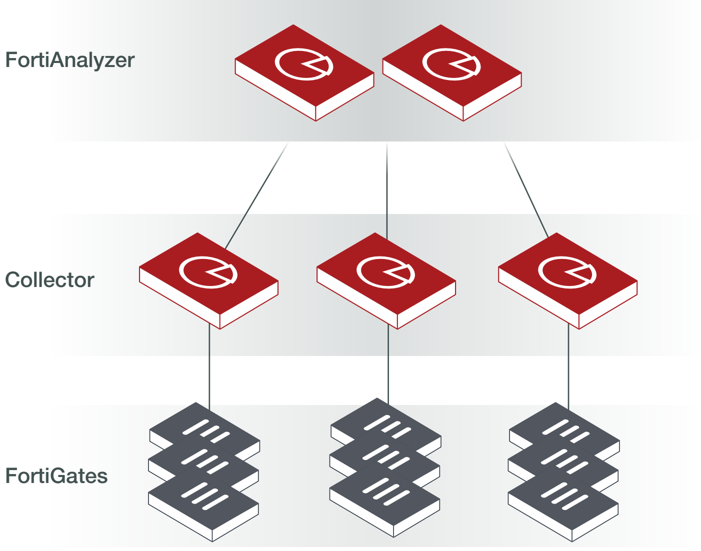


Figure 3.

FortiAnalyzer VM

FortiAnalyzer-VM integrates network logging, analysis, and reporting into a single system, delivering increased knowledge of security events throughout a network. Utilizing virtualization technology, FortiAnalyzer-VM is a software-based version of the FortiAnalyzer hardware appliance and is designed to run on many virtualization platforms. It offers all the features of the FortiAnalyzer hardware appliance.

FortiAnalyzer-VM provides organizations of any size with centralized security event analysis, forensic research, reporting, content archiving, data mining, malicious file quarantining and vulnerability assessment. Centralized collection, correlation, and analysis of geographically and chronologically diverse security data from Fortinet appliances and third-party devices deliver a simplified, consolidated view of your security posture.

Specifications

Specifications	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/VDOMs (Maximum)	10,000	10,000	10,000	10,000	10,000	10,000	10,000
FortiGuard Indicator of Compromise (IOC)	✓	✓	✓	✓	✓	✓	✓
HYPERVISOR REQUIREMENTS							
Hypervisor Support	VMware ESX/ESXi 5.0/5.1/5.5/6.0/6.5, Microsoft Hyper-V 2008 R2/2012/2012 R2/2016, Citrix XenServer 6.0+ and Open Source Xen 4.1+, KVM on Redhat 6.5+ and Ubuntu 17.04, 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

Specifications

	FORTIANALYZER 200F	FORTIANALYZER 300F	FORTIANALYZER 400E
CAPACITY AND PERFORMANCE			
GB/Day of Logs	100	150	200
Analytic Sustained Rate (logs/sec)	3000	4500	6,000
Collector Sustained Rate (logs/sec)	4500	6,750	9,000
Devices/VDOMs (Maximum)	150	180	200
Max Number of Days Analytics	40	28	30
OPTIONS SUPPORTED			
FortiGuard Indicator of Compromise (IOC)	✓	✓	✓
FortiManager Capabilities (up to 20 devices)	No	No	No
HARDWARE SPECIFICATIONS			
Form Factor	1 RU Rackmount	1 RU Rackmount	1 RU Rackmount
Total Interfaces	2xRJ45 GE	2xRJ45 GE, 2xSFP	4x GE
Storage Capacity	4 TB (1 x 4 TB)	8 TB (2 x 4TB)	12 TB (4x 3 TB)
Usable Storage (After RAID)	4 TB	4 TB	6TB
Removable Hard Drives	No	No	✓
RAID Levels Supported	N/A	RAID 0/1	RAID 0/1/5/10
RAID Type	N/A	Software	Software
Default RAID Level	N/A	1	10
Redundant Hot Swap Power Supplies	No	No	No
DIMENSIONS			
Height x Width x Length (inches)	1.75 x 17.0 x 15.0	1.75 x 17.0 x 15.0	1.7 x 17.2 x 19.8
Height x Width x Length (cm)	4.4 x 43.2 x 38.1	4.4 x 43.2 x 38.0	4.3 x 43.7 x 50.3
Weight	17.1 lbs (7.8 kg)	18.9 lbs (8.6 kg)	31 lbs (14.1 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 (Max / Average)	49 W / 114W	65W / 130W	93 W / 133W
Heat Dissipation	390 BTU/h	445 BTU/h	456 BTU/h
Operating Temperature	32 - 104° F (0 - 40° C)	32 - 104° F (0 - 40° C)	41–95°F (5–35°C)
Storage Temperature	95 - 158° F (-35 - 70° C)	95 - 158° F (-35 - 70° C)	-40–140°F (-40–60°C)
Humidity	20 to 90% non-condensing	20 to 90% non-condensing	8– 90% non-condensing
Operating Altitude	Up to 7,400 ft (2,250 m)	Up to 7,400 ft (2,250 m)	Up to 9,842 ft (3,000 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

Specifications

	 FORTIANALYZER **800F**	 FORTIANALYZER **1000E**	 FORTIANALYZER **2000E**
CAPACITY AND PERFORMANCE			
GB/Day of Logs	300	600	1,000
Analytic Sustained Rate (logs/sec)	8,250	18,000	30,000
Collector Sustained Rate (logs/sec)	12,000	27,000	45,000
Devices/VDOMs (Maximum)	800	2,000	2,000
Max Number of Days Analytics	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	4 x GE, 2x SFP	2x GE	4x GE, 2 x SFP+
Storage Capacity	16 TB (4x 4 TB)	24 TB (8x 3 TB)	36 TB (12x 3TB)
Usable Storage (After RAID)	8TB	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
Raid Type	Software	Hardware / Hot Swappable	Hardware / Hot Swappable
Default RAID Level	10	50	50
Redundant Hot Swap Power Supplies	No	✓	✓
DIMENSIONS			
Height x Width x Length (inches)	1.75 x 17.44 x 22.16	3.5 x 17.2 x 25.2	3.5 x 17.2 x 25.6
Height x Width x Length (cm)	4.4 x 44.3 x 56.3	8.9 x 43.7 x 68.4	8.9 x 43.7 x 64.8
Weight	28.6 lbs (13.0 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 / Maximum)	108W / 186W	192.5 W / 275W	293.8 W / 354W
Heat Dissipation	634 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	95 - 158° F (-35 - 70° C)	-40–140°F (-40–60°C)	-40–158°F (-40–70°C)
Humidity	20 to 90% non-condensing	8–90% non-condensing	8–90% 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

Specifications

	 FORTIANALYZER 3000F	 FORTIANALYZER 3500F	 FORTIANALYZER 3700F
CAPACITY AND PERFORMANCE			
GB/Day of Logs	3,000	5,000	8,300
Analytic Sustained Rate (logs/sec)	42,000	63,000	100,000
Collector Sustained Rate (logs/sec)	60,000	90,000	150,000
Devices/VDOMs (Maximum)	4,000	10,000	10,000
Max Number of Days Analytics	30	30	60
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
Total Interfaces	4x GE, 2 x SFP+	2x GE, 2x SFP ports	2xSFP+, 2x1GE
Storage Capacity	48 TB (16x 3 TB – 48 TB max)	72 TB (24x 3TB)	240 TB (60x4TB SAS HDDs)
Usable Storage (After RAID)	42 TB	63 TB	216TB
Removable Hard Drives	✓	✓	✓
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 Type	Hardware / Hot Swappable	Hardware / Hot Swappable	Hardware / Hot Swappable
Default RAID Level	50	50	50
Redundant Hot Swap Power Supplies	✓	✓	✓ *
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
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
Weight	76 lbs (34.5 kg)	93.74 lbs (42.52Kg)	118 lbs (53.5Kg)
ENVIRONMENT			
AC Power Supply	100–240V AC, 50–60 Hz, 11.5 Amp Maximum	100–240V AC, 60–50 Hz	100-240V AC, 60-50 Hz
Power Consumption (Average / Maximum)	449 W / 541W for 12 HDD	465 W / 558W	850 W / 1423.4W
Heat Dissipation	1846.5 BTU/h	1,904 BTU/h	4858 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)	-40–158°F (-40–70°C)
Humidity	8–90% non-condensing	10–90% non-condensing	8% to 90% (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 (2133 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

* 3700F must connect to a 200V - 240V power source.

Order Information

PRODUCT	SKU	DESCRIPTION
FortiAnalyzer 200F	FAZ-200F	Centralized log and analysis appliance — 2xRJ45 GE, 4 TB storage, up to 100 GB/day of logs.
FortiAnalyzer 300F	FAZ-300F	Centralized log and analysis appliance — 2xRJ45 GE, 8 TB storage, up to 150 GB/day of logs.
FortiAnalyzer 400E	FAZ-400E	Centralized log and analysis appliance — 4x GE RJ45, 12 TB storage, up to 200 GB/day of logs.
FortiAnalyzer 800F	FAZ-800F	Centralized log and analysis appliance — 4 x GE, 2x SFP, 16 TB storage, up to 300 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, 2 x 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, 2 x 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 SFP ports, 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, up to 8,300 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 all supported 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 AWS On-Demand	https://aws.amazon.com/marketplace/pp/B01N5K7210/ref=portal_asin_url
	FortiAnalyzer Azure On-Demand	https://azuremarketplace.microsoft.com/en-us/marketplace/apps/fortinet.fortianalyzer
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).