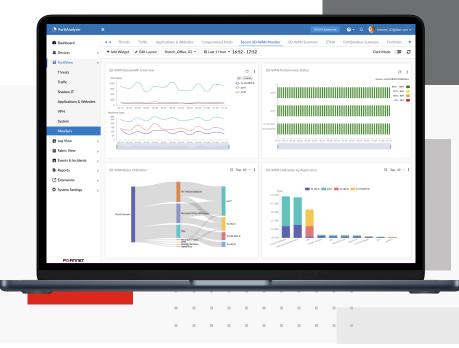


# FortiAnalyzer™

Security Fabric Network Analytics





#### Highlights

- Centralized network monitoring and visibility
- Advanced threat and vulnerability detection with event and log data correlation
- Augmented NOC/SOC operations for real-time response, analytics, and reporting
- Automation to save time, reduce errors, and improve efficiency
- Multi-tenancy solution with quota management
- Administrative domains for operational effectiveness and compliance
- 70+ reports and 2000+ ready-to-use datasets, charts, and macros

#### Analytics, Reports, and Compliance Across the Security Fabric

FortiAnalyzer is a powerful log management, analytics, and reporting platform that provides organizations with a single console to manage, automate, orchestrate, and respond, enabling simplified security operations, proactive identification and remediation of risks, and complete visibility of the entire attack landscape.

Integrated with the Fortinet Security Fabric, FortiAnalyzer enables Network and Security Operations Teams with real-time detection capabilities, centralized security analytics and end-to-end security posture awareness to help analysts identify advanced persistent threats (APTs) and mitigate risks before a breach can occur.

### Capabilities

#### **Incident Detection and Response**

#### Centralized NOC/SOC Visibility for the Attack Surface

FortiAnalyzer provides Security Fabric Analytics across all device logs with event correlation and real-time detection of Advanced Persistent Threats (APTs), vulnerabilities and Indicators of Compromise (IOC) for FortiGate NGFWs, FortiClient, FortiSandbox, FortiWeb, FortiMail and other Fortinet products, for deep visibility and critical network insights. Simplified orchestration and automated workflows provide Network Security Operations teams with real-time notifications, reports, and dashboards for single-pane visibility and actionable results.

#### Incidents and Events Management

Security teams can monitor and manage alerts and event logs from Fortinet devices, with events processed and correlated in a format that analysts can easily understand. Investigate suspicious traffic patterns and search using filters in predefined or custom event handlers to generate real-time notifications and monitoring for NOC and SOC operations, SD-WAN, SSL VPN, wireless, Shadow IT, IPS, network recon, FortiClient, and more.

The Incidents component enables analysts to manage incident handling and life cycle, with incidents generated by events that show affected assets, endpoints, users and timelines.

#### **Fabric Automation**

FortiAnalyzer Playbooks boost an organization's security team abilities to simplify investigation efforts through automated incident response, freeing up resources and allowing analysts to focus on critical tasks. Out-of-the-box playbook templates enable SOC analysts to quickly customize their use cases, define custom processes, interact with other Security Fabric devices like FortiOS and EMS, edit playbooks and tasks in the visual playbook editor and use the Playbook Monitor for investigation of compromised hosts, infections and critical incidents, data enrichment for Assets and Identity views, blocking malware, C&C IPs, and more.

#### **Security Fabric Analytics**

#### **Analytics and Reporting**

FortiAnalyzer automation driven analytics empowers network security operations teams to complete a fast assessment of network devices, systems, and users, with correlated log data and FortiGuard threat intelligence for analysis of real-time and historical events.

- **FortiView** Monitors and Views provide deep insights with context and meaning of network activity, risks, vulnerabilities, attack attempts, indicators of compromise and anomalies, sanctioned and unsanctioned user activity.
- Log View enables analysts to expand their investigation and utilize search filters on managed device logs, drill down on logs, with custom views and log groups, including a SIEM database with normalized logs for Fortinet devices in Fabric ADOMs.
- **Reports** provide comprehensive analysis of your Security Posture, including reports for Operational Technology (OT), security rating, security rating for PCI, Secure SD-WAN, VPN, FortiNDR network anomaly detection, cyber threat assessments, 360 Security Reviews, situational awareness, compliance, auditing, and more.

### Capabilities

#### Assets and Identity

FortiAnalyzer Fabric View with Assets and Identity monitoring provides SOC teams with elevated awareness and visibility into an organization's endpoints and users with dashboards and correlated device and UEBA information, vulnerability detections, EMS tagging, and asset classifications through telemetry with EMS, NAC, Fortinet Fabric Agent, and an OT Dashboard View.

| Ell Enterprise_FortiAnalyzer              |   | ADOM: Enterprise_Demo >_ @ + 🗘 1 + 🔺 admin +                                   |
|---|---|--|
| Summary Asset Identity List Custom View ~ |   |  |
| Toggle Widgets 🗸                          |   | Dark Mode 15 Asset Identity  |
| Detection Method                          | X HW OS Distribution  |  |
|   | Iby fould<br>by max<br>by max | Enterprise_Second_Floor = Enterprise_Floor = Enterprise_Second_Floor = 4 1/2 > |
|   | S ×     Undentified Asset Activity       Initial dentified     Image: Second Control of Control o   | 2 2023-03-03 17:00   |

| Enterprise_FortiAnalyzer   | =                                      | ADOM: Enterprise_Demo >_ 🛛 🕹 🖌  | A admin 🗸 |
|--|--|---|-----------|
| Search Q<br>3CX Supply Chain Attack<br>Microsoft Outlook Elevation c<br>Emotet Malware<br>Realtek SDK Attack |  | REAK ALERTS 🔇   |           |
| Teclib GLPI Remote Code Exe<br>Joomla! CMS Improper Acces!   | Emotet                                 | Malware Resurgence  |           |
| Progress Telerik UI Attack<br>IBM Aspera Faspex Code Exec<br>Cacti Command Injection Vulr                    | First wave of https://en.wikipedia.org | the year 2023<br>wikiEmolet   |           |
| Fortra GoAnywhere MFT RCE<br>VMware ESXi Server Ransom   |  | s distributed via spam emails, has been prevalent since its first appearance in 2014. With a network made up of multiple<br>ontinuously sent out spam emails in campaigns designed to infect users via phishing attacks.  |           |
| Router Malware Attack<br>Outbreak Alert- 2022 Annual<br>CWP Control Web Panel Com                            | Background                             | The EuroPol has considered Emotet as one of the world's most dangerous maiware. It was first discovered on<br>year 2014 as a Banking Trojan. This report focusses specifically on the Emotet maiware protection and IOC<br>detections by the Security Fabric products.                      |           |
| Zerobot Attack<br>VMware Spring Cloud Functic<br>Generic Web Application Fire                                | Announced                              | March 7, 2023: After several months of inactivity, the Emotet botnet resumed email activity and was seen<br>adopting new methods of evasion by using Microsoft OneNote attachments and archive bombs.<br>https://cofense.com/blog/emotel-sending-malicious-emails-after-three-month-hiatus/ |           |

### **Subscriptions and Extensions**

#### Subscription Licenses and FortiGuard Security Services

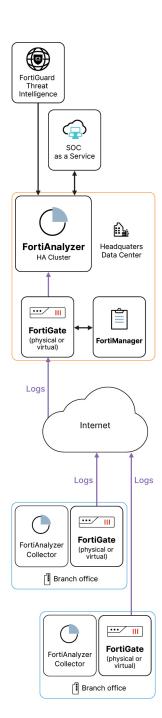
- FortiGuard Outbreak Detection Service delivers automated content package download for detecting the latest malware, including a summary of outbreaks and kill chain mapping for how the malware works. The package includes a FortiGuard Report for the outbreak, Event Handler, and a Report Template to detect outbreaks.
- FortiGuard Indicators of Compromise Service empowers security teams with forensic data from 500 000 IOCs daily, used in combination with FortiAnalyzer analytics to identify suspicious usage and artifacts observed on the network or in an operations system, that have been determined with high confidence to be malicious infections or intrusions, and historical rescan of logs for threat hunting.
- Shadow IT Monitoring Service provides continuous monitoring of unapproved devices, resources, unsanctioned accounts and unauthorized use of SaaS and IaaS, API integration, and third party apps. The service identifies rogue users using personal accounts for managing company assets, using correlated FortiOS and FortiCASB data with a FortiCASB account subscribed for SaaS features.
- **OT Security Service** provides security teams with advanced OT analytics, risk and compliance reports, OT event handlers, and use-case correlation rules.
- Security Rating and Compliance Service helps security teams design, implement, and maintain their security posture, and provides actionable configuration recommendations as well as key performance and risk indicators.
- Security Automation Service subscription enables further automation for incident response with enhanced monitoring and escalation, built-in incident management workflows, connectors, playbooks and more.

#### **Management Extension Applications (MEAs)**

The Management Extensions pane allows you to enable licensed applications that are released and signed by Fortinet, which can be installed and run on FortiAnalyzer, including the FortiSIEM and FortiSOAR.

#### **Data Sheet**

### Capabilities



#### Deployments

#### **Deploying FortiAnalyzer**

FortiAnalyzer can be deployed as a physical hardware appliance, virtual machine (VM) and virtual machine subscription (VM-S), as well as private or public cloud instance, with scalability, redundancy and backup, and high availability capabilities.

#### FortiAnalyzer High Availability (HA)

FortiAnalyzer HA provides real-time redundancy to protect organizations by ensuring continuous operational availability. In the event that the primary (active) FortiAnalyzer fails, a secondary (passive) FortiAnalyzer (up to four-node cluster) will immediately take over, providing log and data reliability and eliminating the risk of having a single point of failure.

#### Multi-Tenancy with Flexible Quota Management

FortiAnalyzer provides the ability to manage multiple sub-accounts with each account having its own administrators and users. The time-based archive/analytic log data policy, per Administrative Domain (ADOM), allows automated quota management based on the defined policy, with trending graphs to guide policy configuration and usage monitoring.

#### Analyzer Collector Modes

FortiAnalyzer provides two operation modes: Analyzer and Collector. In Collector mode, the primary task is forwarding logs of the connected devices to an Analyzer and archiving the logs. This configuration greatly benefits organizations with increasing log rates, as the resource intensive log-receiving task is off-loaded to the Collector so that the Analyzer can focus on generating analytics and reports.

Network operations teams can deploy multiple FortiAnalyzers in Collector and Analyzer modes to work together to improve the overall performance of log receiving and processing increased log volumes, providing log storage and redundancy, and rapid delivery of critical network and threat information.

#### FortiAnalyzer Fabric

FortiAnalyzer Fabric allows SOC Administrators to configure two operation modes - Supervisor and Member. This allows viewing of member devices, ADOMs and authorized logging devices, as well as incidents and events created on members. Admins get access to Reports and FortiView across all member FortiAnalyzers, and can perform global search in Log View of logs collected across FortiAnalyzer Fabric members with pre-defined device filters and log drill down for each Member and Member ADOMs and support for .

#### Log Forwarding for Third-Party Integration

Forward logs from one FortiAnalyzer to another FortiAnalyzer unit, a syslog server, or (CEF) server. In addition to forwarding logs to another unit or server, the client FortiAnalyzer retains a local copy of the logs, which are subject to the data policy settings for archived logs. Logs are forwarded in real-time or near real-time as they are received from network devices.

### **Cloud Services**

#### FortiAnalyzer Cloud

FortiAnalyzer Cloud offers customers a PaaS-based delivery option for automation-driven, single pane analytics, providing log management, analytics, and reporting for Fortinet NGFW and SD-WAN with an easily accessible cloud-based solution. FortiAnalyzer Cloud delivers reliable real-time insights into network activity with extensive reporting and monitoring for clear, consistent visibility of an organization's security posture. Customers can easily access their FortiAnalyzer Cloud from their FortiCloud single sign-on portal.

### **Virtual Offerings**

#### FortiAnalyzer VM Subscription

The FortiAnalyzer VM Subscription license model consolidates into one single SKU: VM product SKU, FortiCare Support SKU, FortiGuard IOC and Outbreak Detection Service, Security Automation services, to simplify the product purchase, upgrade, and renewal. FortiAnalyzer-VM S provides organizations 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 and third party devices deliver a simplified, consolidated view of your security posture.

The FortiAnalyzer-VM S series SKUs come in stackable 5, 50, and 500 GB/ day logs licenses, so that multiple units of this SKU can be purchased together providing organizations with the ability and cost-efficiencies to scale and meet their logging needs.

#### FortiAnalyzer VM

Fortinet offers the FortiAnalyzer-VM licensing in a stackable perpetual license model with a-la-carte technical support and subscription services.

This software-based version of the FortiAnalyzer hardware appliance is designed to run on many virtualization platforms, which allows you to expand your virtual solution as your environment expands.

| FORTIANALYZER VIRTUAL APPLIANCES         | FAZ-VM-GB1  | FAZ-VM-GB5 | FAZ-VM-GB25 | FAZ-VM-GB100 | FAZ-VM-GB500 | FAZ-VM-GB2000 |
|--|---|------------|-------------|--------------|--------------|---------------|
| Capacity                                 |   |            |             |              |              |               |
| GB/ day of Logs *                        | +1  | +5         | +25         | +100         | +500         | +2,000        |
| Devices/VDOMs Maximum                    | 10 000  | 10 000     | 10 000      | 10 000       | 10 000       | 10 000        |
| FortiGuard IOC Service                   | $\bigcirc$  |            |             |              |              |               |
| Security Automation Service              | $\odot$   |            |             |              |              |               |
| Hypervisor Support                       | Up-to-date hypervisor support can be found in the release note for each FortiAnalyzer version.<br>Visit <u>https://docs.fortinet.com/product/fortianalyzer/</u> and find the Release Information at the bottom section.<br>Go to "Product Integration and Support" $\rightarrow$ "FortiAnalyzer [version] support" $\rightarrow$ "Virtualization" |            |             |              |              |               |
| vCPU Support (Minimum / Maximum)         | 4 / Unlimited   |            |             |              |              |               |
| Network Interface Support (Min / Max) ** | 1 / 12  |            |             |              |              |               |
| Memory Support (Minimum / Maximum)       | 16 GB / Unlimited for 64-bit  |            |             |              |              |               |

\* Unlimited GB/ day when deployed in collector mode.

\*\* VM supports up to 12 vNIC interfaces/ports. Applicable to 6.4.3+. Actual consumable numbers vary depending on cloud platforms.

# **Specifications**

| -  |                                 |                                 |                                 | N2 R 32 R 32 R 32 R             |
|--|---------------------------------|---------------------------------|---------------------------------|---------------------------------|
| FORTIANALYZER APPLIANCES                                 | FAZ-150G                        | FAZ-300G                        | FAZ-800G                        | FAZ-810G                        |
| Capacity and Performance                                 |                                 |                                 |                                 |                                 |
| GB/ day of Logs  | 25                              | 100                             | 200                             | 200                             |
| Analytic Sustained Rate (logs/<br>sec)*                  | 500                             | 2000                            | 4000                            | 4000                            |
| Collector Sustained Rate (logs/<br>sec)*                 | 750                             | 3000                            | 6000                            | 6000                            |
| Devices/VDOMs (Maximum)                                  | 50                              | 180                             | 800                             | 800                             |
| Max Number of Days Analytics**                           | 90                              | 50                              | 50                              | 50                              |
| Options  |                                 |                                 |                                 |                                 |
| FortiGuard IOC and Outbreak<br>Detection Service         | $\bigcirc$                      | $\bigcirc$                      | $\odot$                         | $\bigcirc$                      |
| Security Automation Service                              | $\odot$                         | $\bigcirc$                      | $\odot$                         | $\bigcirc$                      |
| Enterprise Bundle  | $\bigcirc$                      | $\bigcirc$                      | $\bigcirc$                      | $\bigcirc$                      |
| Hardware Bundle  | $\odot$                         | $\odot$                         | $\odot$                         | $\bigcirc$                      |
| OT Security Service                                      | $\bigcirc$                      | $\odot$                         | $\odot$                         | $\odot$                         |
| Security Rating and Compliance<br>Service                | $\bigcirc$                      | $\odot$                         | $\odot$                         | $\odot$                         |
| Hardware Specifications                                  |                                 |                                 |                                 |                                 |
| Form Factor (supports EIA/non-<br>EIA standards)         | Desktop                         | 1 RU Rackmount                  | 1 RU Rackmount                  | 1 RU Rackmount                  |
| Total Interfaces   | 2 x RJ45 GE                     | 4 x RJ45 GE                     | 4 x RJ45 GE, 2 x SFP            | 4x RJ-45 2x GE SFP              |
| Storage Capacity   | 4TB (2× 2TB)                    | 8 TB (2 × 4 TB)                 | 16 TB (4 × 4 TB)                | 16TB (4× 4TB) 3.5 in SAS HDDs   |
| Jsable Storage (After RAID)                              | 2 TB                            | 4 TB                            | 8 TB                            | 8 TB                            |
| Removable Hard Drives                                    | No                              | No                              | $\bigcirc$                      | $\bigcirc$                      |
| RAID Levels Supported                                    | 0/1                             | RAID 0/1                        | RAID 0/1,1s/5,5s/10             | RAID 0/1,1s/5,5s/10             |
| RAID Type  | Software                        | Software                        | Hardware / Hot Swappable        | Hardware / Hot Swappable        |
| Default RAID Level                                       | 1                               | 1                               | 10                              | 10                              |
| Redundant Hot Swap Power<br>Supplies                     | No                              | Optional                        | Optional                        | Optional                        |
| Trusted Platform Module (TPM) ***                        | Gen 2                           | Gen 2                           | $\odot$                         | $\odot$                         |
| Dimensions<br>Height x Width x Length (inches)           | 9.5 × 3.5 × 8                   | 1.73 × 17.24 × 16.38            | 1.73 × 17.32 × 21.65            | 1.73 × 17.32 × 21.65            |
| Height x Width x Length (menes)                          | 24.1 × 8.9 × 20.55              | 4.4 × 43.8 × 41.6               | 4.4 × 44.0 × 55.0               | 4.4 × 44.0 × 55.0               |
| Weight   | 9.35 lbs (4.24 kg)              | 22.5 lbs (10.2 kg)              | 25.75 lbs (11.68 kg)            | 25.75 lbs (11.68 kg)            |
|  |                                 |                                 |                                 |                                 |
| Environment<br>AC Power Supply                           | 100-240V AC, 50-60 Hz           | 100–240V AC, 60–50 Hz           | 100–240V AC, 50–60 Hz           | 100-240Vac, 50~60Hz, 4A max     |
| Power Supply<br>Power Consumption (Average /<br>Maximum) | 36 W / 43 W                     | 90.1 W / 99 W                   | 134 W / 174.2 W                 | 115W / 150W                     |
| Heat Dissipation   | 147.4 BTU/h                     | 337.8 BTU/h                     | 594.4 BTU/h                     | 433 BTU/h                       |
| Operating Temperature                                    | 32°-104° F (0°-40° C)           |
| Storage Temperature                                      | -4°-167° F (-20°-75° C)         | -13°-167° F (-25°-75° C)        | -4°-167° F (-20°-75° C)         | -4°-167° F (-20°-75° C)         |
| Humidity   | 5% to 95% non-condensing        | 20% to 90% non-condensing       | 5% to 95% non-condensing        | 5% to 95% non-condensing        |
| Forced Airflow   | Front to Back                   | Front to Back                   | Front to Back                   | Front to Back                   |
| Operating Altitude                                       | Up to 7400 ft (2250 m)          |
| Compliance<br>Safety Certifications                      | FCC Part 15 Class A, RCM, VCCI, |
| Jarety Cel Incations                                     | CE, UL/cUL, CB                  | CE, BSMI, KC, UL/cUL, CB, GOST  | CE, UL/cUL, CB                  | CE, UL/cUL, CB                  |

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

\*\* The maximum number of days if receiving logs continuously at the sustained analytics log rate. This number can increase if the average log rate is lower.

\*\*\* Gen2 refers to hardware that has been upgraded since initial release.

#### **Data Sheet**

# **Specifications**

|  |  | CVS     III     CVS     IIII     CVS     IIII     CVS </th <th></th> |   |
|--|--|--|---|
| FORTIANALYZER APPLIANCES                       | FAZ-1000F  | FAZ-3000G  | FAZ-3700G   |
| Capacity and Performance                       |  |  |   |
| GB/ day of Logs                                | 660  | 3000   | 8300  |
| Analytic Sustained Rate (logs/sec)*            | 20 000   | 42 000   | 100 000   |
| Collector Sustained Rate (logs/sec)*           | 30 000   | 60 000   | 150 000   |
| Devices/VDOMs (Maximum)                        | 2000   | 4000   | 10 000  |
| flax Number of Days Analytics**                | 34   | 30   | 60  |
| ptions   |  |  |   |
| ortiGuard IOC and Outbreak Detection<br>ervice | $\odot$  | $\odot$  | $\bigcirc$  |
| Security Automation Service                    | $\bigcirc$   | $\odot$  | $\bigcirc$  |
| nterprise Bundle                               | $\bigcirc$   | $\bigcirc$   | $\bigcirc$  |
| lardware Bundle                                | $\bigcirc$   | $\bigcirc$   | $\bigcirc$  |
| OT Security Service                            | $\odot$  | $\bigcirc$   | $\odot$   |
| Security Rating and Compliance Service         | $\bigcirc$   | $\odot$  | $\odot$   |
| lardware Specifications                        |  |  |   |
| orm Factor (supports EIA/non-EIA<br>tandards)  | 2 RU Rackmount                                     | 3 RU Rackmount   | 4 RU Rackmount  |
| otal Interfaces                                | 2 × 10GbE RJ45, 2 × 10GbE SFP+                     | 2 x GE RJ45, 2× 25GE SFP28   | 2× 10GE RJ-45 + 2× 25GE SFP28                             |
| torage Capacity                                | 32 TB (8 × 4 TB)                                   | 64 TB (16 × 4TB)   | 240TB (60 × 4TB) 3.5" HDD + 19.2TB (6:<br>3.2TB) NVMe SSD |
| Jsable Storage (After RAID)                    | 24 TB  | 56 TB  | 224 TB  |
| emovable Hard Drives                           | $\bigcirc$   | $\bigcirc$   | $\bigcirc$  |
| AID Levels Supported                           | RAID<br>0/1,1s/5,5s/6,6s/10/50/60                  | RAID<br>0/1,1s/5,5s/6,6s/10/50/60  | RAID<br>0/1,1s/5,5s/6,6s/10/50/60                         |
| AID Type                                       | Hardware / Hot Swappable                           | Hardware / Hot Swappable   | Hardware / Hot Swappable                                  |
| efault RAID Level                              | 50   | 50   | 50  |
| edundant Hot Swap Power Supplies               | $\bigcirc$   | $\bigcirc$   | $\odot$   |
| rusted Platform Module (TPM) ***               | No   | No   | $\bigcirc$  |
| imensions                                      |  |  |   |
| leight x Width x Length (inches)               | 3.5 × 17.2 × 25.6                                  | 5.2 × 17.2 × 25.5  | 7.0 × 17.2 × 30.2   |
| leight x Width x Length (cm)                   | 8.9 × 43.7 × 65.0                                  | 13.0 × 44.0 × 65.0   | 17.8 × 43.7 × 76.7  |
| Veight   | 34 lbs (15.42 kg)                                  | 66.5 lbs (30.15 kg)  | 118 lbs (53.5 kg)   |
| nvironment                                     |  |  |   |
| C Power Supply                                 | 100-240V AC, 50-60 Hz                              | 100-127V~/10A, 200-240V~/5A  | 2000W AC****  |
| ower Consumption (Average / Maximum)           | 192.5 W / 275 W                                    | 385 W / 500 W  | 850 W / 1423.4 W  |
| eat Dissipation                                | 920 BTU/h  | 1350 BTU/h   | 4858 BTU/h  |
| perating Temperature                           | 50°-95°F (10°-35°C)                                | 32°-104°F (0°-40°C)  | 50°–95°F (10°–35°C)                                       |
| torage Temperature                             | -40°-140°F (-40°-60°C)                             | -4°-167°F (-20°-75°C)  | -40°-158°F (-40°-70°C)                                    |
| umidity  | 8% to 90% non-condensing                           | 5% to 95% (non-condensing)   | 8% to 90% (non-condensing)                                |
| orced Airflow                                  | Front to Back                                      | Front to Back  | Front to Back   |
| perating Altitude                              | Up to 7400 ft (2250 m)                             | Up to 7400 ft (2250 m)   | Up to 7400 ft (2250 m)                                    |
| Compliance                                     |  |  |   |
| Safety Certifications                          | FCC Part 15 Class A, RCM, VCCI, CE, UL/<br>cUL, CB | FCC Part 15 Class A, RCM, VCCI, CE, UL/<br>cUL, CB   | FCC Part 15 Class A, RCM, VCCI, CE, UL,<br>cUL, CB        |

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

\*\* is the max number of days if receiving logs continuously at the sustained analytics log rate. This number can increase if the average log rate is lower.

\*\*\* Gen2 refers to hardware that has been upgraded since initial release.

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

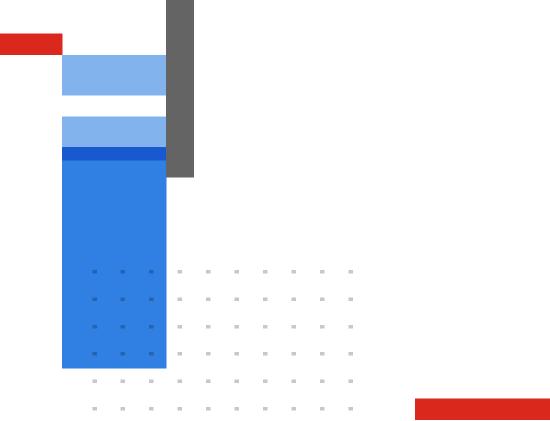
# **Ordering Information**

| FortiAnalyzer     FA2:1500     Centralized log and analysis appliance — 2 x RJ45 GE, 4 TB storage, up to 25 GB/ day of logs.       FA2:3000     Centralized log and analysis appliance — 4 x KB2, 5 TB storage, up to 25 GB/ day of logs.       FA2:8000     Centralized log and analysis appliance — 4 x KB2, 5 TB storage, up to 20 GB/ day of logs.       FA2:8000     Centralized log and analysis appliance — 4 x KB2, 5 TB storage, up to 20 GB/ day of logs.       FA2:8000     Centralized log and analysis appliance — 4 x KB2, 2 x SDE SFP28, 04 TB storage, dual power supplies, up to 600 GB/ day of logs.       FA2:3000     Centralized log and analysis appliance — 2 x FUA5, 2 x SDE SFP28, 04 TB storage, dual power supplies, up to 500 GB/ day of logs.       FA2:3000     Centralized log and analysis appliance — 2 x FUA5, 2 x SDE SFP28, 04 TB storage, dual power supplies, up to 500 GB/ day of logs.       Fort/Analyzer-VM     FO1-10-AZVM5-456-01-DD     Subscription literate to 50 GB/Dby Central Logging and Analytics. Include FortCare Premium support, 100, Security Automation Service, and fortGaun/ Outpack Decicion service.       Fo1-10-AZVM6-465-01-DD     Subscription literate to 50 GB/Dby of Logs.       FA2-W0-681     Upgrade literate for 30 GB/Dby of Logs.       FA2-W0-681     Upgrade literate for adding 180 GB/Dby of Logs.       FA2-W0-685     Upgrade literate fortGam Premium support, 100, Security Automation Service, and fortGam Premium support, 100, Security Automation Service, Security Automation S   |   |                                    |   |
|---|---|------------------------------------|---|
| FA2 3000     Centralized log and analysis appliance — 4 x RJ45 GE, 8 TB storage, up to 200 GB/ day of logs.       FA2 8003     Centralized log and analysis appliance — 4 x RE, 2 x SFP, 16 TB storage, up to 200 GB/ day of logs.       FA2 1006     Centralized log and analysis appliance — 4 x GE, 2 x SFP, 16 TB storage, up to 200 GB/ day of logs.       FA2 1006     Centralized log and analysis appliance — 2 x 10GE RJ45, 2 x 10GE SFP, 32 TB storage, dual power supplicies. Up to 800 GB/ day of logs.       FA2 30000     Centralized log and analysis appliance — 2 x 10GE RJ45, 2 x 10GE SFP, 32 TB storage, dual power supplicies. Up to 800 GB/ day of logs.       FA2 30000     Centralized log and analysis appliance — 2 x 10GE RJ45,   | Product   | SKU                                | Description   |
| FA2:800G     Centralized log and analysis appliance — 4 x GE, 2 x SFP, 16 TB storage, up to 200 GB/ det of log.       FA2:810G     Centralized log and analysis appliance — 4 x GE, 2 x SFP, 16 TB self-encrycting storage, up to 200 GB/ det / log.       FA2:810G     Centralized log and analysis appliance — 4 x GE, 2 x SFP, 16 TB self-encrycting storage, up to 200 GB/ det / log.       FA2:800G     Centralized log and analysis appliance — 2 x 100E FLA5, 2 x 250E SFP28, 64 TB storage, dual power supplies, tp to 300 GB/ det / log.       FA2:300G     Centralized log and analysis appliance — 2 x 10G FLA5, 2 x 250E SFP28, 64 TB storage, dual power supplies, tp to 300 GB/ det / log.       FG14Analyzer-VM Subscription     Centralized log and analysis appliance — 2 x 10G FLA5 x x 25GE SFP28, 64 TB storage, dual power supplies, tp to 300 GB/ det / log.       FG14Analyzer-VM Subscription     Subscription license for 50GD/ Central Logging and Analytics. Include FortCare Premium support, 10C, Security Analytics. Include FortCare Premium support,  | FortiAnalyzer   | FAZ-150G                           | Centralized log and analysis appliance — 2 x RJ45 GE, 4 TB storage, up to 25 GB/ day of logs.   |
| FA2-800     Contraited to g and analysis appliance  |   | FAZ-300G                           | Centralized log and analysis appliance — 4 x RJ45 GE, 8 TB storage, up to 100 GB/ day of logs.  |
| FortLanalyzer-VM     FortLanalyzer-VM Subscription     FortLanalyzer-VM Subscription     FortLanalyzer-VM Subscription       FortLanalyzer-VM Subscription     FortLanalyzer-VM Subscription     FortLanalyzer-VM Subscription     FortLanalyzer-VM Subscription       FortLanalyzer-VM     FortLanalyzer-VM Subscription     FortLanalyzer-VM Subscription     FortLanalyzer-VM Subscription       FortLanalyzer-VM </td <td></td> <td>FAZ-800G</td> <td>Centralized log and analysis appliance — 4 x GE, 2 x SFP, 16 TB storage, up to 200 GB/ day of logs.</td>   |   | FAZ-800G                           | Centralized log and analysis appliance — 4 x GE, 2 x SFP, 16 TB storage, up to 200 GB/ day of logs.   |
| FortiAnalyzer-VM     FAZ-3000G     Controlized log and analysis gaplance - 2 × 0E R145, 2× 25GE SFP28, 04 TB storage, dual power supplies, up to 3000 G8/ day of logs.       FortiAnalyzer-VM Subscription     Energy and analysis gaplance - 2 × 0E R145, 2× 25GE SFP28, 04 TB storage, dual power supplies, up to 3000 G8/ day of logs.       FortiAnalyzer-VM Subscription     Energy and analysis gaplance - 2 × 0DE R1-45 + 2× 25GE SFP28, 04 TB HDD + 19 2TB WMS 520 bod 8/ and on analysis gaplance - 2 × 0DE R1-45 + 2× 25GE SFP28, 04 TB HDD + 19 2TB WMS 520 bod 8/ and on analysis gaplance - 2 × 0DE R1-45 + 2× 25GE SFP28, 04 TB HDD + 19 2TB WMS 520 bod 8/ and on analysis gaplance - 2 × 0DE R1-45 + 2× 25GE SFP28, 04 TB HDD + 19 2TB WMS 520 bod 8/ and on analysis gaplance - 2 × 0DE R1-45 + 2× 25GE SFP28, 04 TB HDD + 19 2TB WMS 520 bod 8/ and on analysis gaplance - 2 × 0DE R1-45 + 2× 25GE SFP28, 04 TB HDD + 19 2TB WMS 520 bod 8/ and on analysis gaplance - 2 × 0DE R1-45 + 2× 25GE SFP28, 04 TB HDD + 19 2TB WMS 520 bod 8/ and on analysis gaplance - 2 × 0DE R1-45 + 2× 25GE SFP28, 04 TB HDD + 19 2TB WMS 520 bod 8/ and on analysis gaplance - 2 × 0DE R1-45 + 2× 25GE SFP28, 04 TB HDD + 19 2TB WMS 520 bod 8/ and analysis part for to 1000 storage by 50 0RD work and the ond analysis gaplance - 1000, gaplan   |   | FAZ-810G                           |   |
| supplies, up to 3000 GP day of logs.       FAZ-3700G     Centralized log and analysis appliance - 2× 10GE RJ-45 + 2× 25GE SFP28 slots, 24OTB HDD + 19.2TB<br>NVMe S5D storage, up to 8300 GP (day of Logs.       FortLanalyzer-VM Subscription<br>Leenee with Support     FGI-10-AZVMS-465-01-DD     Subscription leenes for 50 GP/Day Central Logging and Analytics. Include FortCare Premium support,<br>10C, Security Automation Service, and FortCaure Outpace doubteak Detection service.       FG2-10-AZVMS-465-01-DD     Subscription leenes for 500 GB/Day Central Logging and Analytics. Include FortCare Premium support,<br>10C, Security Automation Service, and FortCaure Outpace doubteak Detection service.       FOrtLanalyzer-VM     FAZ-VM-GB1     Upgrade lienes for 500 GB/Day of Logs.       FAZ-VM-GB1     Upgrade lienes for adding 25 GB/Day of Logs.       FAZ-VM-GB2     Upgrade lienes for adding 20 GB/Day of Logs.       FAZ-VM-GB10     Upgrade lienes for adding 20 GB/Day of Logs.       FAZ-VM-GB10     Upgrade lienes for adding 20 GB/Day of Logs.       FAZ-VM-GB20     Upgrade lienes for adding 20 GB/Day of Logs.       FOrtLanalyzer Cloud Storage     FC1-10-AZCLD-463-01-DD     Soccaas. Include FortCare Premium support, 10C and Security Automation Service.       FOrtLanalyzer Cloud Storage     FC1-10-AZCLD-463-01-DD     Increase FortLanalyzer Cloud storage becamation Service.       FOrtLanalyzer Cloud Storage     FC1-10-AZCLD-463-01-DD     Increase   |   | FAZ-1000F                          |   |
| NVMe SBD strokepingen upfe SBD strokepingen upfer S |   | FAZ-3000G                          |   |
| License with Support     IOC, Security Automation Service, and FortiQuard Outbreak Detection service.       FC2-10-AZVMS-465-01-DD     Subscription license for 50 GB/Day Central Logging and Analytics. Include FortiCare Premium support,<br>IOC, Security Automation Service, and FortiQuard Outbreak Detection service.       FortiAnalyzer-VM     FAZ-VM-GB1     Upgrade license for 500 GB/Day Central Logging and Analytics. Include FortiCare Premium support,<br>IOC, Security Automation Service, and FortiQuard Outbreak Detection service.       FortiAnalyzer-VM     FAZ-VM-GB1     Upgrade license for adding 1 GB/Day of Logs.       FAZ-VM-GB25     Upgrade license for adding 20 BJ/Day of Logs.       FAZ-VM-GB20     Upgrade license for adding 20 BJ/Day of Logs.       FAZ-VM-GB20     Upgrade license for adding 20 BJ/Day of Logs.       FortiAnalyzer Oldud Storage     FC1-0-AZCLD-463-01-DD     Increase FortiAnalyzer Cloud storage by 50 GB/Day for Central Logging and Analytics and FortiCloud<br>SOCasS. Include FortiCare Premium support, IOC and Security Automation Service.       FortiAnalyzer Cloud storage by 50 GB/Day for Central Logging and Analytics and FortiCloud<br>SOCasS. Include FortiCare Premium support, IOC and Security Automation Service.       FortiAnalyzer Cloud with SOCasS.     FortiCare Premium support, IOC and Security Automation Service.       FortiAnalyzer Cloud with SOCasS.     FortiCare Premium support, IOC and Security Automation Service.       FortiAnalyzer Oldud with SOCasS.     FortiO-FAZOU-28   |   | FAZ-3700G                          |   |
| FortiAnalyzer-VM     Forti-Az/VMS-465-01-DD     Subscription license for 500 GB/Day Central Logging and Analytics. Include FortiCare Premium support,<br>ICO, Security Automation Service, and FortiGuard Outbreak Detection service.       FortiAnalyzer-VM     FAZ-VM-GB1     Upgrade license for adding 1 GB/Day of Logs.       FAZ-VM-GB2     Upgrade license for adding 25 GB/Day of Logs.       FAZ-VM-GB2     Upgrade license for adding 25 GB/Day of Logs.       FAZ-VM-GB200     Upgrade license for adding 25 GB/Day of Logs.       FAZ-VM-GB200     Upgrade license for adding 200 GB/Day of Logs.       FOrtiAnalyzer Cloud Storage     FO1-0-AZCLD-463-01-DD       Storage for Foldanal Durberse     Fo1-0-AZCLD-463-01-DD       Increase FortiAnalyzer Cloud storage by 50 GB/Day for Central Logging and Analytics and FortiCloud<br>Stocass. Include FortiCare Permium support, ICC and Security Automation Service.       FO1-0-AZCLD-463-01-DD     Increase FortiAnalyzer Cloud storage by 50 GB/Day for Central Logging and Analytics and FortiCloud<br>Stocass. Include FortiCare Permium support, ICC and Security Automation Service.       FortiAnalyzer Cloud with SOCas     Fo1-0-AZCLD-463-01-DD     Increase FortiAnalyzer Cloud storage by 50 GB/Day for Central Logging and Analytics and FortiCloud<br>Stocass. Include FortiCare Permium support, ICC and Security Automation Service.       FortiAnalyzer Cloud with SOCas     Fo1-0-AZCLD-463-01-DD     FortiAnalyzer Cloud storage connector service for 10TB data transfer to publi  | FortiAnalyzer-VM Subscription<br>License with Support   | FC1-10-AZVMS-465-01-DD             |   |
| FortiAnalyzer-VM     FA-VM-GB1     Upgrade license for adding 5 GB/Day of Logs.       FA-VM-GB5     Upgrade license for adding 5 GB/Day of Logs.       FA2-VM-GB5     Upgrade license for adding 5 GB/Day of Logs.       FA2-VM-GB50     Upgrade license for adding 5 GB/Day of Logs.       FA2-VM-GB50     Upgrade license for adding 50 GB/Day of Logs.       FA2-VM-GB50     Upgrade license for adding 50 GB/Day of Logs.       FA2-VM-GB200     Upgrade license for adding 50 GB/Day of Logs.       FOrtiAnalyzer Cloud Storage     FC1-10-A2CLD-463-01-DD     Increase FortiAnalyzer Cloud storage by 5 GB/Day for Central Logging and Analytics and FortiCloud SOCaas. Include FortiCare Premium support, IOC and Security Automation Service.       FO2-10-A2CLD-463-01-DD     Increase FortiAnalyzer Cloud storage by 50 GB/Day for Central Logging and Analytics and FortiCloud SOCaas. Include FortiCare Premium support, IOC and Security Automation Service.       FortiAnalyzer Cloud with SOCaas     FC10-FA2CD-266-02-DD     Increase FortiAnalyzer Cloud storage by 50 GB/Day for Central Logging and Analytics and FortiCloud Service.       Socaas. Include FortiCare Premium support, IOC and Security Automation Service.     FOrtiAnalyzer Cloud with SOCaas       FortiAnalyzer Cloud with SOCaas     FC10-fA2C0-266-02-DD     One year subscription Increase fortiAnalyzer Cloud with SOCaas       FortiAnalyzer Cloud with SOCaas     FO-10-Model Code]-661-02-DD  |   | FC2-10-AZVMS-465-01-DD             |   |
| FAZ-VM-085     Upgrade license for adding 5 GB/Day of Logs.       FAZ-VM-08100     Upgrade license for adding 100 GB/Day of Logs.       FAZ-VM-08100     Upgrade license for adding 100 GB/Day of Logs.       FAZ-VM-08100     Upgrade license for adding 500 GB/Day of Logs.       FAZ-VM-08100     Upgrade license for adding 500 GB/Day of Logs.       FAZ-VM-08200     Upgrade license for adding 500 GB/Day of Central Logging and Analytics and FortiCloud SoCas.       FAZ-VM-08200     Upgrade license for adding 500 GB/Day of Central Logging and Analytics and FortiCloud SoCas.       Subscription     FC1-10-AZCLD-463-01-DD     Increase FortiAnalyzer Cloud storage by 500 GB/Day for Central Logging and Analytics and FortiCloud SoCas.       FC2-10-AZCLD-463-01-DD     Increase FortiAnalyzer Cloud storage by 500 GB/Day for Central Logging and Analytics and FortiCloud SoCas.       FortiAnalyzer - Backup to Cloud     FC1-0-FAZ00-286-02-DD     One year subscription to FortiAnalyzer cloud storage by 500 GB/Day for Central Logging and Analytics and FortiCloud SoCas.       FortiAnalyzer Cloud with SOCas     FC-10-(Model Code)-365-02-DD     FortiAnalyzer Cloud storage by 500 GB/Day for Central Logging and Analytics and FortiCloud SoCas.       FortiAnalyzer Cloud with SOCas     FC-10-(Model Code)-365-02-DD     FortiAnalyzer Cloud storage by 500 GB/Day for Central Logging and Analytics.       FortiAnalyzer Cloud with SOCas     FC-10-(Model Code)  |   | FC3-10-AZVMS-465-01-DD             | Subscription license for 500 GB/Day Central Logging and Analytics. Include FortiCare Premium support,<br>IOC, Security Automation Service, and FortiGuard Outbreak Detection service. |
| FAZ-WA-GB25     Upgrade license for adding 25 GB/Day of Logs.       FAZ-WA-GB100     Upgrade license for adding 25 GB/Day of Logs.       FAZ-WA-GB500     Upgrade license for adding 500 GB/Day of Logs.       FAZ-WA-GB500     Upgrade license for adding 25 BB/Day for Central Logging and Analytics and FortiCloud<br>SoCass. Include FortiCare Premium support, IOC and Security Automation Service.       FortiAnalyzer Cloud Storage<br>Subscription     FC1-10-AZCLD-463-01-DD     Increase FortiAnalyzer Cloud storage by 50 GB/Day for Central Logging and Analytics and FortiCloud<br>SoCass. Include FortiCare Premium support, IOC and Security Automation Service.       FortiAnalyzer - Backup to Cloud     FC2-10-A2CLD-463-01-DD     Increase FortiAnalyzer Cloud storage by 50 GB/Day for Central Logging and Analytics and FortiCloud<br>SoCass. Include FortiCare Premium support, IOC and Security Automation Service.       FortiAnalyzer - Backup to Cloud     FC-10-FAZ00-286-02-DD     One year subscription to FortiAnalyzer Storage connector service for 10TB data transfer to public cloud.<br>SoCass. Include FortiCare Premium support, IOC and Security Automation Service.       FortiAnalyzer Cloud with SOCass     FC-10-[Model Code]-486-02-DD     FortiAnalyzer Cloud storage by 50 GB/Day for Central Logging and Analytics. Include All FortiGate log<br>types, IOC service, Security Automation Service - FortiGuard Outbreak Service and SOCass.       FortiAnalyzer Cloud with SOCass     FC-10-[Model Code]-485-02-DD     Sotscription license for Security Automation Service - Appliance.       FC10A <td>FortiAnalyzer-VM</td> <td>FAZ-VM-GB1</td> <td>Upgrade license for adding 1 GB/Day of Logs.</td>   | FortiAnalyzer-VM  | FAZ-VM-GB1                         | Upgrade license for adding 1 GB/Day of Logs.  |
| FA2-VM-GB100     Upgrade license for adding 100 GB/Day of Logs.       FA2-VM-GB500     Upgrade license for adding 500 GB/Day of Logs.       FA2-VM-GB2000     Upgrade license for adding 2 TB/Day of Logs.       FortiAnalyzer Cloud Storage     FC1-10-AZCLD-463-01-DD     Increase FortiAnalyzer Cloud storage by 5 GB/Day for Central Logging and Analytics and FortiCloud SOCaaS. Include FortiCare Premium support, IOC and Security Automation Service.       FC2-10-AZCLD-463-01-DD     Increase FortiAnalyzer Cloud storage by 50 GB/Day for Central Logging and Analytics and FortiCloud SOCaaS. Include FortiCare Premium support, IOC and Security Automation Service.       FC3-10-AZCLD-463-01-DD     Increase FortiAnalyzer Cloud storage by 50 GB/Day for Central Logging and Analytics and FortiCloud SorCaaS. Include FortiCare Premium support, IOC and Security Automation Service.       FOrtiAnalyzer Cloud with SOCaaS     FC-10-FAZOD-286-02-DD     One year subscription to FortiAnalyzer Cloud storage by 50 GB/Day for Central Logging and Analytics and FortiCloud SorCaaS. Include FortiCare Premium support, IOC and Security Automation Service.       FortiAnalyzer Cloud with SOCaaS     FC-10-FMOdel Code]-464-02-DD     One year subscription to FortiAnalyzer Cloud storage by 50 GB/Day for Central Logging and Analytics. Include AII FortiGate Iog types, IOC service, Security Automation Service FortiGate Premium support, IOC and Security Automation Service for TOTB data transfer to public cloud.       FortiAnalyzer Cloud with SOCaaS     FC-10-[Model Code]-464-02-DD     FortiAnalyzer Cloud storage by 50 GB/Day for Centra  |   | FAZ-VM-GB5                         | Upgrade license for adding 5 GB/Day of Logs.  |
| FAZ-VM-GBS00     Upgrade license for adding 500 GB/Day of Logs.       FAZ-VM-GB2000     Upgrade license for adding 2 TB/Day of Logs.       FortiAnalyzer Cloud Storage     FC1-10-AZCLD-463-01-DD     Increase FortiAnalyzer Cloud storage by 5 GB/Day for Central Logging and Analytics and FortiCloud SOCaas. Include FortiCare Premium support, IOC and Security Automation Service.       FC2-10-AZCLD-463-01-DD     Increase FortiAnalyzer Cloud storage by 50 GB/Day for Central Logging and Analytics and FortiCloud SOCaas. Include FortiCare Premium support, IOC and Security Automation Service.       FC3-10-AZCLD-463-01-DD     Increase FortiAnalyzer Cloud storage by 50 GB/Day for Central Logging and Analytics and FortiCloud SOCaas. Include FortiCare Premium support, IOC and Security Automation Service.       FC3-10-AZCLD-463-01-DD     Increase FortiAnalyzer Cloud storage by 500 GB/Day for Central Logging and Analytics and FortiCloud SOCaas. Include FortiCare Premium support, IOC and Security Automation Service.       FOrtiAnalyzer Cloud with SOCaas     FC-10-FAZ00-286-02-DD     One year subscription to FortiAnalyzer cloud with SOCaasS: cloud-based central logging and analytics. Include All FortiGate log types, IOC service, Security Automation Service.       FortiAnalyzer Cloud with SOCaas     FC-10-fModel Code]-385-02-DD     FortiAnalyzerCloud: cloud-based central logging and analytics. Include all FortiGate log types, IOC service, Security Automation Service.       FortiGard Outbreak     FC-10-fModel Code]-335-02-DD     Subscription license for Security Automation Service.  |   | FAZ-VM-GB25                        | Upgrade license for adding 25 GB/Day of Logs.   |
| FAZ-WA-GB2000     Upgrade license for adding 2 TB/Day of Logs.       FortiAnalyzer Cloud Storage     FC1-10-AZCLD-463-01-DD     Increase FortiAnalyzer Cloud storage by 5 GB/Day for Central Logging and Analytics and FortiCloud SOCaaS. Include FortiCare Premium support, IOC and Security Automation Service.       FC2-10-AZCLD-463-01-DD     Increase FortiAnalyzer Cloud storage by 50 GB/Day for Central Logging and Analytics and FortiCloud SOCaaS. Include FortiCare Premium support, IOC and Security Automation Service.       FC3-10-AZCLD-463-01-DD     Increase FortiAnalyzer Cloud storage by 50 GB/Day for Central Logging and Analytics and FortiCloud SOCaaS. Include FortiCare Premium support, IOC and Security Automation Service.       FOrtiAnalyzer Cloud with SOCaaS     FC-10-FAZ00-286-02-DD     One year subscription to FortiAnalyzer storage connector service for 10TB data transfer to public cloud SOCaaS. Include FortiCare Premium support, IOC and Security Automation Service.       FortiAnalyzer Cloud with SOCaaS     FC-10-[Model Code]-464-02-DD     FortiAnalyzer Cloud with SOCaaS. Include all FortiGate log types, IOC service, Security Automation Service, FortiGuard Outbreak Service and SOCaaS.       Servitanalyzer Cloud     FC-10-[Model Code]-355-02-DD     Subscription license for Security Automation Service, - Appliance.       FortiGate IO and Outbreak     FC-10-[Model Code]-355-02-DD     Subscription license for Security Automation Service - Appliance.       FortiGate IO and Outbreak     FC-10-[Model Code]-661-02-DD     Subscription license for FortiGuard IOC and Outb  |   | FAZ-VM-GB100                       | Upgrade license for adding 100 GB/Day of Logs.  |
| FortiAnalyzer Cloud Storage<br>Subscription     FC1-10-AZCLD-463-01-DD     Increase FortiAnalyzer Cloud storage by 5 GB/Day for Central Logging and Analytics and FortiCloud<br>SCCaaS. Include FortiCare Premium support, IOC and Security Automation Service.       FC2-10-AZCLD-463-01-DD     Increase FortiAnalyzer Cloud storage by 50 GB/Day for Central Logging and Analytics and FortiCloud<br>SCCaaS. Include FortiCare Premium support, IOC and Security Automation Service.       FC3-10-AZCLD-463-01-DD     Increase FortiAnalyzer Cloud storage by 50 GB/Day for Central Logging and Analytics and FortiCloud<br>SCCaaS. Include FortiCare Premium support, IOC and Security Automation Service.       FortiAnalyzer - Backup to Cloud<br>Service     FC-10-FAZ00-286-02-DD     One year subscription to FortiAnalyzer storage connector service for 10TB data transfer to public cloud.<br>Service, Security Automation Service.       FortiAnalyzer Cloud with SOCaaS     FC-10-[Model Code]-464-02-DD     FortiAnalyzer Cloud with SOCaaS: cloud-based central logging and analytics. Include All FortiGate log<br>types, IOC service, Security Automation Service, FortiGuard Outbreak Service and SOCaaS.       FortiAnalyzer Cloud     FC-10-[Model Code]-585-02-DD     Subscription license for Security Automation Service - Appliance.       FC10-IModel Code]-02-DD     Subscription license for Security Automation Service - Appliance.     FC10-IModel Code]-661-02-DD       FortiAnalyzer Cloud outbreak     FC-10-IModel Code]-661-02-DD     Subscription license for FortiGuard IOC and Outbreak Detection Service - Appliance.       FC10E(BD ay Code]-1  |   | FAZ-VM-GB500                       | Upgrade license for adding 500 GB/Day of Logs.  |
| Subscription     SOCaaS. Include FortiCare Premium support, IOC and Security Automation Service.       FC2-10-AZCLD-463-01-DD     Increase FortiAnalyzer Cloud storage by 50 GB/Day for Central Logging and Analytics and FortiCloud SOCaaS. Include FortiCare Premium support, IOC and Security Automation Service.       FC3-10-AZCLD-463-01-DD     Increase FortiAnalyzer Cloud storage by 500 GB/Day for Central Logging and Analytics and FortiCloud SOCaaS. Include FortiCare Premium support, IOC and Security Automation Service.       FortiAnalyzer - Backup to Cloud     FC-10-FAZ00-286-02-DD     One year subscription to FortiAnalyzer storage connector service for 10TB data transfer to public cloud.       Service     FC-10-IModel Code]-464-02-DD     FortiAnalyzer Cloud with SOCaaS: cloud-based central logging and analytics. Include All FortiGate log types, IOC service, Security Automation Service, FortiGuard Outbreak Service and SOCaaS.       FortiAnalyzer Cloud     FC-10-IModel Code]-585-02-DD     FortiAnalyzerCloud: cloud-based central logging and analytics. Include All FortiGate log types, IOC service, Security Automation Service, FortiGuard Outbreak Service and SOCaaS.       FortiAnalyzer Cloud     FC-10-IModel Code]-585-02-DD     Subscription license for Security Automation Service - Appliance.       FortiGuard IOC and Outbreak Detection Service     FC-10-IModel Code]-385-02-DD     Subscription license for Security Automation Service - Virtual Machine.       FortiGuard IOC and Outbreak     FC-10-IModel Code]-385-02-DD     Subscription license for FortiGuard IOC and Outbr  |   | FAZ-VM-GB2000                      | Upgrade license for adding 2 TB/Day of Logs.  |
| SOCaaS. Include FortiCare Premium support, IOC and Security Automation Service.       FC3-10-AZCLD-463-01-DD     Increase FortiAnalyzer Cloud storage by 500 GB/Day for Central Logging and Analytics and FortiCloud SOCaaS. Include FortiCare Premium support, IOC and Security Automation Service.       FortiAnalyzer - Backup to Cloud     FC-10-FAZ00-286-02-DD     One year subscription to FortiAnalyzer storage connector service for 10TB data transfer to public cloud.       FortiAnalyzer Cloud with SOCaaS     FC-10-[Model Code]-464-02-DD     FortiAnalyzer Cloud with SOCaaS: cloud-based central logging and analytics. Include All FortiGate log types, IOC service, Security Automation Service, FortiGuard Outbreak Service and SOCaaS.       FortiAnalyzer Cloud     FC-10-[Model Code]-585-02-DD     FortiAnalyzerCloud: cloud-based central logging and analytics. Include All FortiGate log types, IOC service, Security Automation Service, FortiGuard Outbreak Service and SOCaaS.       Security Automation Service     FC-10-[Model Code]-335-02-DD     Subscription license for Security Automation Service - Appliance.       FC1GB Day Code]-10-LV0VM-335-02-DD     Subscription license for Security Automation Service - Appliance.       FC10-[Model Code]-661-02-DD     Subscription license for Security Automation Service - Appliance.       FC10-[Model Code]-10-LV0VM-661-02-DD     Subscription license for FortiGuard IOC and Outbreak Detection Service - Virtual Machine.       FOrtiAnalyzer Security Rating and     FC-10-[Model Code]-159-02-DD     Subscription license for FortiGu   | FortiAnalyzer Cloud Storage<br>Subscription             | FC1-10-AZCLD-463-01-DD             |   |
| SOCaaS. Include FortiCare Premium support, IOC and Security Automation Service.       FortiAnalyzer - Backup to Cloud<br>Service     FC-10-FAZ00-286-02-DD     One year subscription to FortiAnalyzer storage connector service for 10TB data transfer to public cloud.       FortiAnalyzer Cloud with SOCaaS     FC-10-[Model Code]-464-02-DD     FortiAnalyzer Cloud with SOCaaS: cloud-based central logging and analytics. Include All FortiGate log<br>types, IOC service, Security Automation Service, FortiGuard Outbreak Service and SOCaaS.       FortiAnalyzer Cloud     FC-10-[Model Code]-585-02-DD     FortiAnalyzerCloud: cloud-based central logging and analytics. Include all FortiGate log types, IOC<br>service, Security Automation Service, FortiGuard Outbreak Detection Service.       Security Automation Service     FC-10-[Model Code]-335-02-DD     Subscription license for Security Automation Service - Appliance.       FortiGard IOC and Outbreak<br>Detection Service     FC-10-[Model Code]-661-02-DD     Subscription license for FortiGuard IOC and Outbreak Detection Service - Appliance.       FOrtiGard IOC and Outbreak<br>Detection Service     FC-10-[Model Code]-10-LV0VM-661-02-DD     Subscription license for FortiGuard IOC and Outbreak Detection Service - Virtual Machine.       OT Security Service     FC-10-[Model Code]-159-02-DD     Subscription license for FortiGuard IOC and Outbreak Detection Service - Virtual Machine.       FOrtiAnalyzer Security Rating and<br>CroleB bay Code]-10-LV0VM-661-02-DD     Subscription license for FortiGuard IOC and Outbreak Detection Service - Virtual Machine. <td></td> <td>FC2-10-AZCLD-463-01-DD</td> <td></td>   |   | FC2-10-AZCLD-463-01-DD             |   |
| Service     FortiAnalyzer Cloud with SOCaaS     FC-10-[Model Code]-464-02-DD     FortiAnalyzer Cloud with SOCaaS: cloud-based central logging and analytics. Include All FortiGate log types, IOC service, Security Automation Service, FortiGuard Outbreak Service and SOCaaS.       FortiAnalyzer Cloud     FC-10-[Model Code]-585-02-DD     FortiAnalyzerCloud: cloud-based central logging and analytics. Include All FortiGate log types, IOC service, Security Automation Service, FortiGuard Outbreak Detection Service.       Security Automation Service     FC-10-[Model Code]-335-02-DD     Subscription license for Security Automation Service - Appliance.       FortiGuard IOC and Outbreak     FC-10-[Model Code]-661-02-DD     Subscription license for Security Automation Service - Virtual Machine.       FortiGuard IOC and Outbreak     FC-10-[Model Code]-661-02-DD     Subscription license for FortiGuard IOC and Outbreak Detection Service - Appliance.       FC[GB Day Code]-10-LV0VM-661-02-DD     Subscription license for FortiGuard IOC and Outbreak Detection Service - Virtual Machine.       OT Security Service     FC-10-[Model Code]-159-02-DD     Subscription license for FortiGuard IOC and Outbreak Detection Service - Virtual Machine.       FortiAnalyzer Security Rating and Compliance Service     FC-10-[Model Code]-175-02-DD     Subscription license for FortiGuard OIC and Outbreak Detection Service, security, exercite and compliance Service       FortiAnalyzer Security Rating and Compliance Service     FC-10-[Model Code]-175-02-DD     Subscrip   |   | FC3-10-AZCLD-463-01-DD             |   |
| types, IOC service, Security Automation Service, FortiGuard Outbreak Service and SOCaaS.FortiAnalyzer CloudFC-10-[Model Code]-585-02-DDFortiAnalyzerCloud: cloud-based central logging and analytics. Include all FortiGate log types, IOC<br>service, Security Automation Service, FortiGuard Outbreak Detection Service.Security Automation ServiceFC-10-[Model Code]-335-02-DDSubscription license for Security Automation Service - Appliance.FortiGuard IOC and Outbreak<br>Detection ServiceFC-10-[Model Code]-61-02-DDSubscription license for Security Automation Service - Virtual Machine.FortiGuard IOC and Outbreak<br>Detection ServiceFC-10-[Model Code]-159-02-DDSubscription license for FortiGuard IOC and Outbreak Detection Service - Appliance.FortiGuard ServiceFC-10-[Model Code]-159-02-DDSubscription license for FortiGuard IOC and Outbreak Detection Service - Virtual Machine.OT Security ServiceFC-10-[Model Code]-159-02-DDOT Security Service including advanced OT analytics, risk and compliance reports, event handlers, and<br>use-case correlation rulesFortiAnalyzer Security Rating and<br>Compliance ServiceFC-10-[Model Code]-175-02-DDSubscription license for FortiAnalyzer Security Rating and Compliance Service, Security Automation<br>Service, and FortiGuard Outbreak Detection service).Enterprise Protection BundleFC-10-[Model Code]-466-02-DDEnterprise Protection (FortiCare Premium plus Indicators of Compromise Service, Security Automation<br>Service, and FortiGuard Outbreak Detection service).  | FortiAnalyzer - Backup to Cloud<br>Service              | FC-10-FAZ00-286-02-DD              | One year subscription to FortiAnalyzer storage connector service for 10TB data transfer to public cloud.  |
| Security Automation Service     FC-10-[Model Code]-335-02-DD     Subscription license for Security Automation Service - Appliance.       FC[GB Day Code]-10-LV0VM-335-02-DD     Subscription license for Security Automation Service - Virtual Machine.       FortiGuard IOC and Outbreak Detection Service     FC-10-[Model Code]-661-02-DD     Subscription license for FortiGuard IOC and Outbreak Detection Service - Appliance.       Detection Service     FC-10-[Model Code]-661-02-DD     Subscription license for FortiGuard IOC and Outbreak Detection Service - Appliance.       Detection Service     FC-10-[Model Code]-159-02-DD     Subscription license for FortiGuard IOC and Outbreak Detection Service - Virtual Machine.       OT Security Service     FC-10-[Model Code]-159-02-DD     OT Security Service including advanced OT analytics, risk and compliance reports, event handlers, and use-case correlation rules       FortiAnalyzer Security Rating and Compliance Code]-175-02-DD     Subscription license for FortiAnalyzer Security Rating and Compliance Service       Enterprise Protection Bundle     FC-10-[Model Code]-466-02-DD     Enterprise Protection (FortiCare Premium plus Indicators of Compromise Service, Security Automation Service, and FortiGuard Outbreak Detection service).  | FortiAnalyzer Cloud with SOCaaS                         | FC-10-[Model Code]-464-02-DD       |   |
| FC[GB Day Code]-10-LV0VM-335-02-DD   Subscription license for Security Automation Service - Virtual Machine.     FortiGuard IOC and Outbreak   FC-10-[Model Code]-661-02-DD   Subscription license for FortiGuard IOC and Outbreak Detection Service - Appliance.     Detection Service   FC[GB Day Code]-10-LV0VM-661-02-DD   Subscription license for FortiGuard IOC and Outbreak Detection Service - Virtual Machine.     OT Security Service   FC-10-[Model Code]-159-02-DD   OT Security Service including advanced OT analytics, risk and compliance reports, event handlers, and use-case correlation rules     FortiAnalyzer Security Rating and Compliance Service   FC-10-[Model Code]-175-02-DD   Subscription license for FortiAnalyzer Security Rating and Compliance Service     Enterprise Protection Bundle   FC-10-[Model Code]-466-02-DD   Enterprise Protection (FortiGare Premium plus Indicators of Compromise Service, Security Automation Service, and FortiGuard Outbreak Detection service).   | FortiAnalyzer Cloud                                     | FC-10-[Model Code]-585-02-DD       |   |
| FortiGuard IOC and Outbreak<br>Detection Service     FC-10-[Model Code]-661-02-DD     Subscription license for FortiGuard IOC and Outbreak Detection Service - Appliance.       Detection Service     FC[GB Day Code]-10-LV0VM-661-02-DD     Subscription license for FortiGuard IOC and Outbreak Detection Service - Virtual Machine.       OT Security Service     FC-10-[Model Code]-159-02-DD     OT Security Service including advanced OT analytics, risk and compliance reports, event handlers, and use-case correlation rules       FortiAnalyzer Security Rating and Compliance Service     FC-10-[Model Code]-175-02-DD     Subscription license for FortiCare Premium plus Indicators of Compromise Service, Security Automation Service, and FortiGuard Outbreak Detection service).   | Security Automation Service                             | FC-10-[Model Code]-335-02-DD       | Subscription license for Security Automation Service - Appliance.   |
| Detection Service     FC[GB Day Code]-10-LV0VM-661-02-DD     Subscription license for FortiGuard IOC and Outbreak Detection Service - Virtual Machine.       OT Security Service     FC-10-[Model Code]-159-02-DD     OT Security Service including advanced OT analytics, risk and compliance reports, event handlers, and use-case correlation rules       FortiAnalyzer Security Rating and Compliance Service     FC-10-[Model Code]-175-02-DD     Subscription license for FortiAnalyzer Security Rating and Compliance Service       Enterprise Protection Bundle     FC-10-[Model Code]-466-02-DD     Enterprise Protection (FortiCare Premium plus Indicators of Compromise Service, Security Automation Service, and FortiGuard Outbreak Detection service).   |   | FC[GB Day Code]-10-LV0VM-335-02-DD | Subscription license for Security Automation Service - Virtual Machine.   |
| FC[GB Day Code]-10-LV0VM-661-02-DD   Subscription license for FortiGuard IOC and Outbreak Detection Service - Virtual Machine.     OT Security Service   FC-10-[Model Code]-159-02-DD   OT Security Service including advanced OT analytics, risk and compliance reports, event handlers, and use-case correlation rules     FortiAnalyzer Security Rating and Compliance Service   FC-10-[Model Code]-175-02-DD   Subscription license for FortiAnalyzer Security Rating and Compliance Service     Enterprise Protection Bundle   FC-10-[Model Code]-466-02-DD   Enterprise Protection (FortiCare Premium plus Indicators of Compromise Service, Security Automation Service, and FortiGuard Outbreak Detection service).   | FortiGuard IOC and Outbreak<br>Detection Service        | FC-10-[Model Code]-661-02-DD       | Subscription license for FortiGuard IOC and Outbreak Detection Service - Appliance.   |
| FortiAnalyzer Security Rating and<br>Compliance Service   FC-10-[Model Code]-175-02-DD   Subscription license for FortiAnalyzer Security Rating and Compliance Service     Enterprise Protection Bundle   FC-10-[Model Code]-466-02-DD   Enterprise Protection (FortiCare Premium plus Indicators of Compromise Service, Security Automation<br>Service, and FortiGuard Outbreak Detection service).  |   | FC[GB Day Code]-10-LV0VM-661-02-DD | Subscription license for FortiGuard IOC and Outbreak Detection Service - Virtual Machine.   |
| Compliance Service   Enterprise Protection Bundle   FC-10-[Model Code]-466-02-DD   Enterprise Protection (FortiCare Premium plus Indicators of Compromise Service, Security Automation Service, and FortiGuard Outbreak Detection service).   | OT Security Service                                     | FC-10-[Model Code]-159-02-DD       |   |
| Service, and FortiGuard Outbreak Detection service).  | FortiAnalyzer Security Rating and<br>Compliance Service | FC-10-[Model Code]-175-02-DD       | Subscription license for FortiAnalyzer Security Rating and Compliance Service   |
| Hardware Bundle     FAZ-[Hardware Model]-BDL-466-DD     Hardware plus FortiCare Premium and FortiAnalyzer Enterprise Protection.  | Enterprise Protection Bundle                            | FC-10-[Model Code]-466-02-DD       |   |
|   | Hardware Bundle   | FAZ-[Hardware Model]-BDL-466-DD    | Hardware plus FortiCare Premium and FortiAnalyzer Enterprise Protection.  |

#### Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including

those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.



# F:RTINET.

www.fortinet.com

Copyright © 2023 Fortinet, Inc. All rights reserved. Fortinet\*, FortiGate\*, FortiCare\* and FortiGate\*, FortiCare\* and FortiGate\*, FortiCare\* and Certain other marks are registered trademarks of Fortinet, Inc., 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. Nothing metric perspective commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortine tenters a binding written contract, signal by Fortinet. Soluties and uncertainties, whether express or implied, except to the extent Fortine tenters a binding written contract, signal by Fortinet. Soluties canditions and actual performance metrics 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 on Fortinet. For absolute darity, any such warrants will be limited to performance in the same ideal conditions as in Fortinet is internal lab tests. 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.