DATA SHEET

FortiAnalyzer Big Data

Big Data Analytics

Scalable Performance

Built-in High Availability

Available in:

Appliance Virtual Machine

FortiAnalyzer Big Data delivers high-performance big data network analytics for large and complex networks. It is designed for large-scale data center and high-bandwidth deployments, offering the most advanced cyber threat protection by employing hyperscale data ingestion and accelerated parallel data processing. Together with its new distributed software and hardware architecture and Fortinet's high performance next generation firewalls, this powerful 4RU chassis offers blazing fast performance, enterprise-grade data resiliency, built-in horizontal scalability, and consolidated appliance management.

High Performance

- Totally redesigned and optimized architecture, employing the newest Big Data Kafka/ Hadoop/ Spark technologies
- Massive Parallel event streaming and data processing for high-speed ingestion, data storage, and search capabilities
- The highest performing FortiAnalyzer appliance: 300 000 logs/sec out-of-box, horizontally scalable to petabytes of storage

Unified Appliance Management

- Enterprise-grade Big Data Appliance with consolidated hardware and software monitoring through the Cluster Manager
- Simple installation, updating, expansion, and data management
- Built-in automation and customizable job templates

Reliable and Scalable Deployment

- Built-in enterprise high availability and data resiliency based on a newly optimized software and hardware architecture
- Designed for rapid scalability with multiple Big Data appliances using high speed 40 Gb/s built-in switch modules
- Specifically designed to accelerate the visibility and expansion of the Fortinet Security Fabric

Big Data Security Analytics

- Monitor and analyze your entire network from end-to-end at an accelerated rate, maximizing the visibility of your entire attack surface, network traffic, applications, users, and end-point hosts
- Interactive dashboards and informative reports using real-time tracking of key security metrics, link health status, and application steering performance
- Ready to use and customizable report templates for compliance, security posture assessments, and system performance checks
- Use log analytics to query IPFIX log messages collected, when Ingestion is configured in Flow mode

Rapid Incident Detection and Response

- Intuitive event and incident workflow for SOC teams to focus on critical alerts
- The built-in correlation engine automates and groups alerts to remove false positives
- Out-of-box connectors and extensive APIs for security teams to automate repetitive tasks

HIGHLIGHTS

FortiAnalyzer Big Data supports all of the features and technologies of FortiAnalyzer family. FortiAnalyzer Big Data also provides additional scalability and high-speed performance using new massive parallel data processing and Columnar Data Store processes. After the data ingest, the FortiAnalyzer Big Data provides an easy to use front-end UI that interacts with the distributed big data SQL engine to search, query, and aggregate the data.

SERVICE CATEGORY	ACTIVITY	FORTIANALYZER APPLIANCES	FORTIANALYZER BIG DATA 4500F
Security Analytics	Log View	✓	✓
	Interactive FortiView Dashboards	✓	✓
	Fabric View - Assets and Identity	✓	✓
	Out-of-Box Report Templates	✓	✓
	Global Search across all Big Data clusters	—	✓
	IPFIX Support	—	✓
Incident Response	Indicators of Compromise Service	✓	✓
	Event Correlation and Alerting	✓	✓
	Incident Escalation Workflow and Management	✓	✓
Automation and Integration	Security Fabric Connectors	✓	✓
	Security Fabric Integration	✓	✓
	REST API	✓	✓
Multi-Tenancy and RBAC	ADOM	✓	✓
	Role-Based Access Control	✓	✓
Performance and Scalability	Deployment	Small, Medium Enterprise	Large Enterprise and Service Providers
	High Availability and Redundancy	Yes, requires a second unit	Yes, built-in HA and redundancy
	Sustained Rate	Up to 100 000 logs/sec	Start at 300 000 logs/sec
	Horizontal Scalability	—	✓
	Big Data Analytics Engine	—	✓
	Massive Parallel Data Processing	—	✓
	Distributed Architecture	—	✓
	Columnar Data Store	—	✓
Appliance Management	Chassis	—	✓
	Cluster Manager	—	✓

To download the FortiAnalyzer Datasheet, please visit - https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortianalyzer.pdf

FortiAnalyzer Big Data Virtual Machines

Fortinet offers FortiAnalyzer Big Data in a stackable Virtual license model, with a-la-carte services available for 24×7 FortiCare support and subscription licenses for the FortiGuard Indicator of Compromise (IOC), FortiAnalyzer SOC component, and FortiGuard Outbreak Detection Service.

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

SPECIFICATIONS

FORTIANALYZER BIG DATA VIRTUAL APPLIANCES	FAZ-BD-VM
Capacity	
Storage Capacity	200 TB
Log Ingestion Rate (logs/sec)	150 000 (up to 500 000)
Devices/VDOMs Maximum	10 000+
Chassis Management	✓
Virtual Machine	
FortiGuard Indicator of Compromise (IOC)	✓
SOC Subscription	✓
FortiGuard Outbreak Alert Service	✓
Virtual Machine	
Hypervisor Support	Up-to-date hypervisor support information can be found in the release notes for each FortiAnalyzer Big Data version. Visit https://docs.fortinet.com/product/fortianalyzer-bigdata/ and find the Release Information at the bottom section. Go to "Product Integration and Support" → "FortiAnalyzer BigData [version] support" → "Virtualization"

FORTIANALYZER BIG DATA APPLIANCES	FAZ-BD-4500F
Capacity and Performance	
GB/Day of Logs (raw logs)	20 TB
Log Ingestion Rate (logs/sec)	300 000
Devices/VDOMs (Maximum)	10 000+
Max Number of Days Analytics*	30
Options Supported	
FortiGuard Indicator of Compromise (IOC)	✓
SOC Subscription	✓
FortiGuard Outbreak Alert Service	✓
Hardware Specifications	
Form Factor	4 RU
Total Interfaces	4× 40 GE QSFP and 8× 10 GE SFP+
Storage Capacity	Blade#1: 2 x NVMe 750 GB SSD = 1.5 TB; Blade#2 ~#14: 13 × 2 × 7.68 TB SSD x = 200 TB
Usable Storage	200 TB
Removable Hard Drives	28 (Max) SSD, each blade 2 × 2.5" Storage Device
Redundant Hot Swap Power Supplies**	✓
Dimensions	
Height x Width x Length (inches)	7 × 17.6 × 32
Height x Width x Length (cm)	17.8 × 44.7 × 81.3
Weight	240 lbs (108.96 kg)
Environment	
AC Power Supply**	200-240 VAC, 50-60 Hz
Power Consumption (Average / Maximum)	4739.74 W / 4967.1 W
Heat Dissipation	16 983.51 (BTU/h)
Max Current	200-240 V / 10-9.8A
Operating Temperature	10°C ~ 35°C (50°F ~ 95°F)
Storage Temperature	-40°C to 60°C (-40°F to 140°F)
Humidity	8% to 90% (non-condensing)
Compliance	
Safety Certifications	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB

* The max number of days if receiving logs continuously at the sustained log ingestion rate. This number can increase if the average log rate is lower.
** All four power supplies must be installed and plugged in to a reliable power source when the device is turned on / powered up. Three power supplies are required for the device to fully operate, which allows hot swap of one power supply at a time. The max power consumption of the unit is 4967 W and each PSU supports 2200 W. The fourth power supply provides redundancy.

ORDER INFORMATION

PRODUCT	SKU	DESCRIPTION
FortiAnalyzer-BigData-4500F	FAZ-BD-4500F	FortiAnalyzer high-performance chassis for big data analytics with 14 blade servers, 4× 40 GE QSFP Ports, 8× 10 GE SFP+ Ports, 300 000 logs/sec ingestion rate, and 200TB SSD storage in a single system. Horizontally scalable up to petabytes of storage.
Hardware Bundle	FAZ-BD-4500F-BDL-466-DD	Hardware plus 24×7 FortiCare and FortiAnalyzer Enterprise Protection.
Enterprise Protection Bundle	FC-10-BD45F-466-02-DD	Enterprise Protection (24×7 FortiCare plus Indicators of Compromise Service, SOC Subscription license, and FortiGuard Outbreak Alert service).
SOC Subscription License	FC-10-BD45F-335-02-DD	Subscription license for the FortiAnalyzer SOC component.
IOC Subscription License	FC-10-BD45F-149-02-DD	Subscription license for the FortiGuard Indicator of Compromise (IOC).
Outbreak Alert Subscription License	FC-10-BD45F-462-02-DD	Subscription license for FortiGuard Outbreak Alert Service.
24×7 FortiCare Contract	FC-10-BD45F-247-02-DD	24×7 FortiCare Contract.
FortiAnalyzer-BigData-VM	FAZ-BD-VM	FortiAnalyzer-BD virtual appliance with 150 000 logs/sec ingestion rate and 200TB storage capacity to start. Support add-on to scale up performance and storage.
FortiAnalyzer-BigData-VM Add-On *	FAZ-BD-VM-UG	FortiAnalyzer-BD virtual appliance ADD-ON to add additional capacity with 50 000 logs/sec ingestion rate and 50TB storage. Multiple ADD-ONs can be stacked together to scale up the ingestion rate and storage.
Enterprise Protection Bundle VM	FC-10-ZBDVM-575-02-DD	Enterprise Protection (24×7 FortiCare plus Indicators of Compromise Service, SOC Subscription license, and FortiGuard Outbreak Detection service).
SOC Subscription License VM	FC-10-ZBDVM-335-02-DD	Subscription license for the FortiAnalyzer SOC component.
IOC Subscription License VM	FC-10-ZBDVM-149-02-DD	Subscription license for the FortiGuard Indicator of Compromise (IOC).
Outbreak Alert Subscription License VM	FC-10-ZBDVM-462-02-DD	Subscription license for FortiGuard Outbreak Detection Service.
24×7 FortiCare Contract VM	FC-10-ZBDVM-248-02-DD	24×7 FortiCare Contract.

* FortiAnalyzer-BD virtual appliance ADD-ON can stack up to a maximum of 500 000 logs/sec

FBD-DAT-R6-20220524