FortiAnalyzer® BigData

DATA SHEET

FortiAnalyzer BigData 4500F

Big Data Analytics
Scalable Performance
Built-in High Availability

The FortiAnalyzer BigData 4500F 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 40Gb/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

Rapid Incident Detection & 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 Collumnar Data Store processes. After the data ingest, the FortiAnalzyzer 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.

		FORTIANALYZER APPLIANCES	FORTIANALYZER BIG DATA 4500F
Security Analytics	Log View	✓	✓
	Interactive FortiView Dashboards	✓	✓
	Fabric View - Assets and Identity	✓	✓
	Out-of-Box Report Templates	✓	✓
Incident Response	Indicators of Compromise Service	✓	✓
	Event Correlation & Alerting	✓	✓
	Incident Escalation Workflow & Management	✓	✓
Automation & Integration	Security Fabric Connectors	✓	✓
	Security Fabric Integration	✓	✓
	REST API	✓	✓
Muti-Tenancy & RBAC	ADOM	✓	✓
	Role-Based Access Control	✓	✓
Performance & Scalability	Deployment	Small, Medium Enterprise	Large Enterprise & 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	—	✓
	Collumnar 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

Specifications

FORTIANALYZER-BIG DATA 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)	✓
Hardware Specifications	
Form Factor	4 RU
Total Interfaces	4x 40 GE QSFP and 8x 10 GE SFP+
Storage Capacity	Blade#1: 2 x NVMe 750 GB SSD = 1.5 TB; Blade#2 ~#14: 13 x 2 x 7.68 TB SSD x = 200 TB
Usable Storage	200 TB
Removable Hard Drives	28 (Max) SSD, each blade 2 x 2.5" Storage Device
Redundant Hot Swap Power Supplies	✓

Dimensions	
Height x Width x Length (inches)	7 x 17.6 x 32
Height x Width x Length (cm)	17.8 x 44.7 x 81.3
Weight	240 lbs (108.96 kg)
Environment	
AC Power Supply	200-240 VAC, 50-60 Hz
Power Consumption (Average / Maximum)	4,745.48 W / 5,016.58 W
Heat Dissipation	16,947.75 (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

* maximum constant log ingestion rate that the FAZ-BD platform can maintain for minimum 48 hours without database and system performance degradation.

** is 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.

Order Information

Product	SKU	Description
FortiAnalyzer-BigData-4500F	FAZ-BD-4500F	FortiAnalyzer high-performance chassis for big data analytics with 14 blade servers, 4x 40-Gbps QSFP Ports, 8x 10Gbps SFP+ Ethernet Ports, 300,000 logs/sec ingestion rate, and 200TB SSD storage in a single system. Horizontally scalable up to petabytes of storage.
IOC Subscription License	FC-10-BD45F-149-02-DD	Subscription license for the FortiGuard Indicator of Compromise (IOC)
24x7 FortiCare Contract	FC-10-BD45F-247-02-DD	24x7 FortiCare Contract

FORTINET®

www.fortinet.com