DATA SHEET

FortiAnalyzer BigData

FortiAnalyzer BigData 4500F

ビッグデータ分析
スケーラブルパフォーマンス
組込み済の高可用性

FortiAnalyzer BigData 4500F は、大規模かつ複雑なネットワークにおいてハイパフォーマンスのビッグデータネットワーク分析を可能にします。大規模データセンターや高帯域幅の環境を想定して設計されており、ハイパースケールのデータの取り込みと高速並列データ処理の採用によって、最も高度なサイバー脅威からの保護を実現します。フォーティネットの新しい分散型ソフトウェア / ハードウェアアーキテクチャとハイパフォーマンス次世代ファイアウォールが統合された、この 4RU シャーシのパワフルな FortiAnalyzer BigData 4500F は、驚異的な高速パフォーマンス、エンタープライズグレードのデータ耐障害性、水平方向の拡張性、統合アプライアンス管理を提供します。

優れたパフォーマンス

- 最新のビッグデータ Kafka / Hadoop / Spark テクノロジーの採用により、アーキテクチャの設計を全面的に刷新し、最適化
- 大規模な並列イベントストリーミングとデータ処理により、高速でのデータの取り込み、保存、検索を実現
- 最も優れたパフォーマンスを提供する FortiAnalyzer アプライアンス：導入後すぐに秒あたり 300,000 件のログ記録が可能で、水平方向の拡張性によってペタバイトレベルのストレージにも対応

統合アプライアンス管理

- エンタープライズグレードのビッグデータアプライアンスのハードウェアとソフトウェアを Cluster Manager で監視
- 容易なインストール、更新、拡張、データ管理
- 内蔵のジョブテンプレートによる自動化やカスタマイズが可能

信頼性と拡張性に優れた導入配備

- ソフトウェアとハードウェアのアーキテクチャの全面的な刷新と最適化により、優れた可用性とデータ耐障害性をエンタープライズ環境に提供
- 40Gb/ 秒の高速スイッチモジュールを活用し、複数のビッグデータアプライアンスによる迅速な拡張を実現する設計
- 独自の設計により、フォーティネット セキュリティ ファブリックの可視性強化や拡張を実現

ビッグデータセキュリティ分析

- ネットワーク全体のエンドツーエンドかつ高速の監視と分析を可能にすることで、あらゆる攻撃対象領域、ネットワークトラフィック、アプリケーション、ユーザー、エンドポイントホストの最大限の可視化を実現
- 重要なセキュリティ指標、リンク状態ステータス、アプリケーションステアリングパフォーマンスをリアルタイムで追跡し、インタラクティブダッシュボードや詳細レポートに出力
- カスタマイズ可能なレポートテンプレートを利用した、コンプライアンス、セキュリティ態勢評価、システムパフォーマンスチェックが可能

インシデントの迅速な検知とレスポンス

- イベントやインシデントの直感的なワークフローにより、SOC チームは重要なアラートに注力可能
- 内蔵の相関エンジンによるアラートの自動化とグループ化によって、誤通知を排除
- 容易に利用可能なコネクタと広範な API により、セキュリティチームは反復的タスクの自動化が可能

ハイライト

FortiAnalyzer BigData は、FortiAnalyzer ファミリーのすべての機能とテクノロジーをサポートします。大規模な並列データ処理と列志向データストアプロセスを新たに採用し、飛躍的な拡張性の向上と高速のパフォーマンスを実現します。FortiAnalyzer BigData の使いやすいフロントエンドの UI を利用して、データの取り込み後に分散型ビッグデータ SQL エンジンとやり取りし、データの検索、クエリ、集計を実行できます。

		FortiAnalyzer アプライアンス	FortiAnalyzer BigData 4500F
セキュリティ分析	ログビュー	✓	✓
	インタラクティブ FortiView ダッシュボード	✓	✓
	ファブリックビュー：アセットとアイデンティティ	✓	✓
	すぐに利用可能なレポートテンプレート	✓	✓
インシデントレスポンス	IOC（Indicators of Compromise：侵害指標）サービス	✓	✓
	イベント相関とアラート	✓	✓
	インシデントのエスカレーションワークフローと管理	✓	✓
自動化と統合	セキュリティ ファブリック コネクタ	✓	✓
	セキュリティ ファブリック統合	✓	✓
	REST API	✓	✓
マルチテナント対応とRBAC	管理ドメイン（ADOM）	✓	✓
	ロールベースのアクセス制御	✓	✓
パフォーマンスと拡張性	推奨導入環境	中小規模のエンタープライズ	大規模エンタープライズ、サービスプロバイダー
	高可用性と冗長性	あり：2 台目の装置が必要	あり：高可用性と冗長性を内蔵
	持続ログレート	最大 100,000 ログ / 秒	300,000 ログ / 秒以上
	水平方向の拡張性	—	✓
	ビッグデータ分析エンジン	—	✓
	大規模並列データ処理	—	✓
	分散型アーキテクチャ	—	✓
	列志向データストア	—	✓
アプライアンス管理	シャーシ	—	✓
	Cluster Manager	—	✓

FortiAnalyzerデータシートのダウンロード：https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/ja_jp/FortiAnalyzer_DS.pdf

技術仕様

FortiAnalyzer BigData 4500F	
システム性能	
ログ処理 / 日（RAW ログ）	20 TB
ログ摂取率（ログ / 秒）*	300,000
管理可能なネットワークデバイス 仮想 UTM（VDOM）サポート数（最大）	10,000+
最長分析日数 **	30
サポートするオプション	
FortiGuard IOC（Indicators of Compromise：侵害指標）サービス	✓
ハードウェア仕様	
形状	4 RU
インタフェース	4 x 40 GbE QSFP、8 x 10 GbE SFP+
ストレージ	ブレード 1： 2 x NVMe 750 GB SSD = 1.5 TB ブレード 2 ～ 14： 13 x 2 x 7.68 TB SSD x = 200 TB
利用可能なストレージ	200 TB
リムーバブル HDD	28（最大）SSD、 各ブレード 2 x 2.5 インチ ストレージデバイス
冗長電源（ホットスワップ対応）	✓

サイズ	
高さ x 幅 x 奥行	178 x 447 x 813 mm
重量	108.96 kg
動作環境	
AC 電源	200 ～ 240 VAC、50 ～ 60 Hz
消費電力（平均 / 最大）	4,745.48 W / 5,016.58 W
放熱	16,947.75 BTU/h
最大電流	200 ～ 240 V / 10 ～ 9.8 A
動作温度	10 ℃ ～ 35 ℃
保管温度	-40 ℃ ～ 60 ℃
湿度	8 ～ 90%（結露しないこと）
準拠規格	
準拠規格・認定	FCC Part 15 Class A、RCM、VCCI、CE、UL/cUL、CB

* データベースおよびシステムのパフォーマンスを低下させることなく、最小で 48 時間 FortiAnalyzer プラットフォームが維持可能なログ摂取率の最大値。
** ログを分析用持続レートで継続的に受信する場合に保持できる最大日数。平均ログレートが低いと保持日数は長くなります。

フォーティネットジャパン株式会社

〒106-0032
東京都港区六本木 7-7-7
Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ