DATA SHEET

FortiAnalyzer

提供形態：

アプライアンス　仮想マシン　クラウド

フォーティネット セキュリティ ファブリックの可視性、分析、自動化による企業の近代化

FortiAnalyzerは、ログ管理、分析、レポート作成のための強力なプラットフォームであり、管理、自動化、オーケストレーション、レスポンスを単一コンソールで可能にすることで、セキュリティオペレーションの簡素化、プロアクティブなリスクの特定と修復、攻撃対象領域全体の完全な可視化を実現します。フォーティネット セキュリティ ファブリックと統合することで、高度な脅威検知機能、一元化されたセキュリティ分析、エンドツーエンドのセキュリティ態勢の認識と制御を実現します。これによりチームはセキュリティ侵害の発生前に脅威を特定して減災できるようになります。

セキュリティツール、人材、プロセスを**オーケストレーション**して、タスクやワークフローの合理的な実行、インシデントの分析とレスポンスを実現し、脅威の検知、ケースの作成と調査、減災とレスポンスに要する時間を直ちに短縮します。

コネクタ、プレイブック、イベントハンドラーを使用してワークフローを**自動化**し、アクションをトリガーすることで、ネットワークセキュリティチームが重要なアラートやイベント、法規制やコンプライアンスの SLA（サービスレベル契約）に対応する能力を向上させます。

脅威インテリジェンス、イベントの相関付け、監視、アラート、レポートを用いて、ネットワークセキュリティへの攻撃、脆弱性、潜在的なセキュリティ侵害に対する警告にリアルタイムで**対応**し、戦術的なレスポンスと減災を迅速に行います。

主な機能と特長

- セキュリティ ファブリックの分析：すべてのログを網羅するイベントの相関付けとリアルタイム検知、および IOC（Indicators of Compromise：侵害指標）サービスと高度な脅威の検知を実現
- フォーティネット セキュリティ ファブリック統合：FortiGate NGFW、FortiClient、FortiSandbox、FortiWeb、FortiMail などとの統合により、ネットワークの細部まで可視化し、重要で実用的なインテリジェンスを提供
- エンタープライズクラスの高可用性：地理的に分散する FortiAnalyzer データベースの自動バックアップによって、ディザスタリカバリに対応
- セキュリティの自動化：REST API、スクリプト、コネクタ、さらにオートメーションステッチ（ワークフローの自動化）を活用して複雑さを解消し、迅速なセキュリティレスポンスと検知時間の短縮を実現
- クォータ管理機能を備えたマルチテナントソリューション：管理ドメイン（ADOM）を活用して顧客データを分離し、ドメインを管理することで、効率的なオペレーションとコンプライアンスを実現
- アプライアンス、VM、ホスティング型、またはパブリッククラウドの柔軟な導入オプションをサポート。AWS、Azure、Google Cloud Platform をクラウドのアーカイブ用 2 次ストレージとして使用

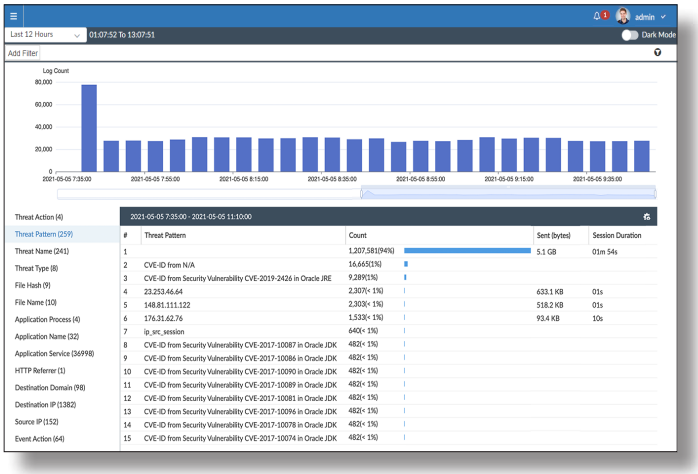
ハイライト

フォーティネット セキュリティ ファブリックで利用可能な機能

インシデントの検知とレスポンス

NOC / SOCを一元的に可視化し、攻撃対象領域を把握

FortiSOC ビューは、詳細なドリルダウン機能を備えた実用的なビューで、ログや脅威データと実用的インテリジェンスの相関付けを可能にすることで、セキュリティやネットワークの運用チームによるネットワーク資産の保護を支援します。リアルタイム通知、レポート、定義済みやカスタマイズしたダッシュボードから、一元的な可視性と実用的な結果が提供されます。FortiAnalyzer のワークフロー自動化を利用して、セキュリティオペレーションのオーケストレーション、脅威や脆弱性の管理、インシデントレスポンスが簡素化されます。脅威追跡ビューで、SIEM の正規化されたログを分析し、異常や脅威をプロアクティブに調査できます。

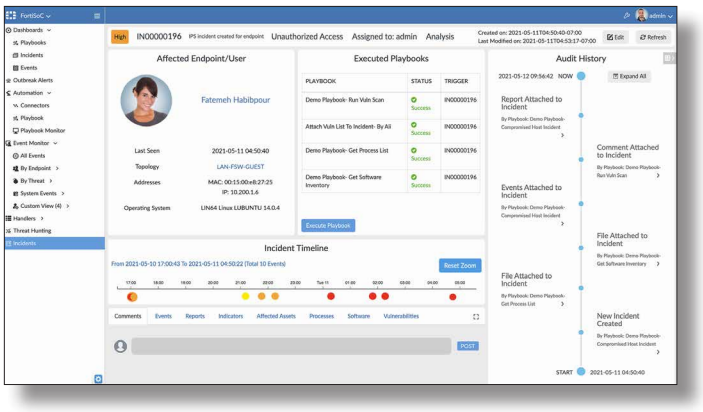


イベント管理

セキュリティチームは、フォーティネットのデバイスからのアラートやイベントログを監視し、アナリストが簡単に理解できるフォーマットでイベントを処理し、相関付けることができます。不審なトラフィックパターンを調査し、定義済みまたはカスタマイズしたイベントハンドラーのフィルターを使用して検索し、NOC や SOC のオペレーション、SD-WAN、SSL VPN、ワイヤレス、シャドー IT、IPS、ネットワークの偵察、FortiClient などのリアルタイムの通知や監視を生成することができます。

インシデント管理

FortiSOC のインシデントコンポーネントによって、セキュリティオペレーションチームは影響を受けたアセット、エンドポイント、ユーザーを表示するためにイベントから作成されたインシデントを使用して、インシデント対応とライフサイクルを管理することができます。アナリストは、インシデントの割り当て、イベントの詳細 / インシデントのタイムラインの表示とドリルダウン、分析コメントの追加、レポートとアーティファクトの添付、完全な監査履歴のためのプレイブック実行の詳細の確認を行うことができます。



FortiAnalyzer のファブリックコネクタを介した FortiSOAR へのインシデントデータのエクスポートをサポートするなど、FortiSOAR との統合によって、インシデントのさらなる調査と脅威の根絶が可能になります。

プレイブックの自動化

FortiAnalyzer プレイブックは、セキュリティチームの調査作業を自動インシデントレスポンスによって簡素化し、リソースを解放してアナリストがより重要なタスクに注力できるようにします。

すぐに活用できるプレイブックテンプレートが提供されているため、SOC アナリストはユースケースを迅速にカスタマイズすることができます。プレイブックには、侵害されたホスト、感染、重大インシデントの調査、ファブリックビューのアセットとアイデンティティビューのデータ補強、マルウェアのブロック、C&C の IP などが含まれます。セキュリティチームは、カスタムプロセスの定義、ビジュアルプレイブックエディターでのプレイブックとタスクの編集、プレイブックモニターを利用したタスク実行の詳細の確認、プレイブックのインポート / エクスポート、他のセキュリティ ファブリックデバイス（FortiOS、FortiClient EMS など）とプレイブックの連携を可能にする内蔵コネクタと **OAuth2** 認証の使用が可能です。新しいコネクタのヘルスチェックは、コネクタが常時接続し機能しているかどうかを確認する指標となります。

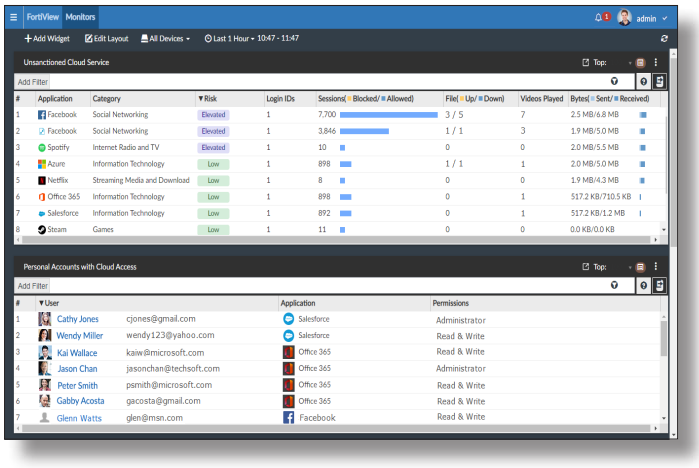
サブスクリプションライセンスとFortiGuardセキュリティサービス

FortiGuard アウトブレイク検知サービスは、マルウェア拡散のサマリーやマルウェアの仕組みを表すキルチェーンマッピングを含むコンテンツパッケージを自動的にダウンロードすることで、最新のマルウェアの検知を可能にします。このパッケージには、アウトブレイクを検知するための FortiGuard レポート、イベントハンドラー、レポートテンプレートが含まれています。

FortiGuard IOC（Indicators of Compromise：侵害指標）サブスクリプションは、毎日 50 万件もの IOC から得られるフォレンジックデータをセキュリティチームに提供します。これを FortiAnalyzer 分析と組み合わせて使用することで、ネットワークやオペレーションシステムで観察された不審な使用や痕跡のうち、悪意のある感染や侵入であると高い確度で判断されたものを特定し、脅威追跡のためのログの履歴再スキャンを行います。

ハイライト

シャドー IT 監視サービスは、FortiOS と FortiCASB の相関付けられたデータや SaaS 機能のサブスクリプションを使用している FortiCASB アカウントの情報を使用して、承認されていないデバイス、リソース、許可されていないアカウント、SaaS や IaaS の不正使用、API 統合、サードパーティアプリケーション、および個人アカウントを使用して企業資産を管理する不正なユーザーなどを継続的に監視します。

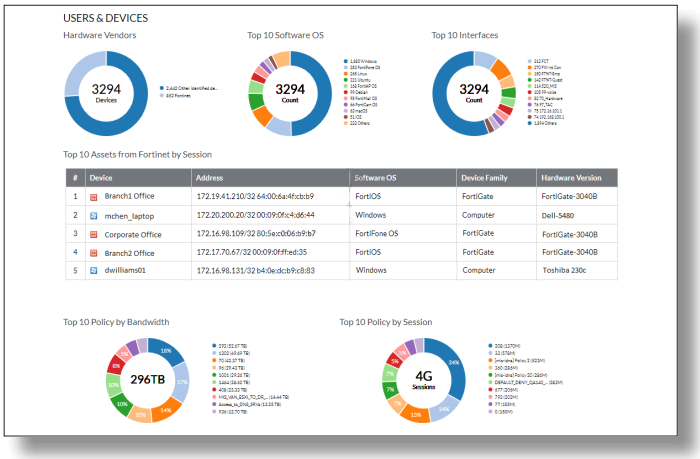


FortiSOC サブスクリプションを含めることで、機能強化されたアラート監視とエスカレーション、組み込まれたインシデント管理ワークフロー、コネクタ、および多数の FortiSOC プレイブックによって、インシデントレスポンスの自動化が強化されます。

セキュリティ ファブリック分析

分析とレポート

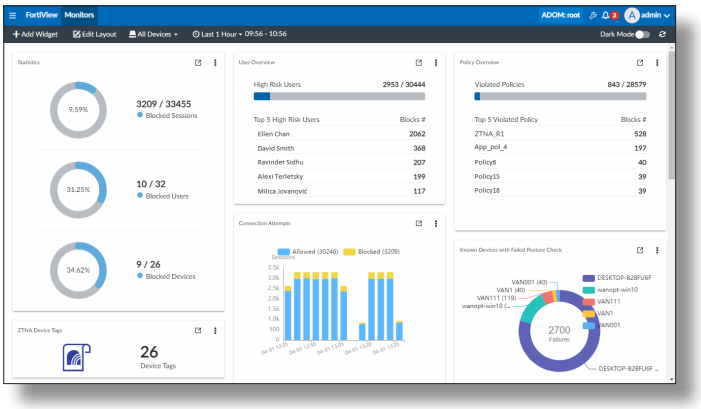
FortiAnalyzer のオートメーションドリブン分析機能は、ネットワークデバイス、システム、ユーザーを完全に可視化し、脅威インテリジェンスとリアルタイムや過去のイベントのログデータを相関付けることで、セキュリティチームを強力に支援します。アナリストは、相関付けられた監視ビューやレポートにアクセスして、ネットワークアクティビティ、リスク、脆弱性、攻撃の試行、オペレーションの異常の調査のコンテキストや意味、SaaS アプリケーションの承認済や未承認のユーザーアクティビティの監視が付加された、詳細で実用的なインテリジェンスに提示することができます。



FortiAnalyzer には、セキュア SD-WAN、VPN、脅威評価、360 セキュリティレビュー、状況認識、自己攻撃、リスク指標などにすぐに利用できる 70 以上のレポートテンプレート、950 以上のデータセット、900 以上のチャート、160 以上のマクロが提供されているため、個々のステークホルダーが必要とするビジネス指標を PDF、HTML、CSV、XML、JSON などの柔軟な表示フォーマットで提供することができます。

FortiView は、ボットネットや C&C といったネットワークの脅威や IOC（Indicators of Compromise：侵害指標）、主なネットワークトラフィックの送信元 / 送信先、主なアプリケーション / Web サイト / SaaS、VPN とシステムの情報、その他ファブリックデバイスのインテリジェンスなど、重要なアラートや情報をリアルタイムにマルチレベルで表示し、概要を提供する包括的な監視ソリューションです。

Monitors ビューでは、オペレーションセンターの複数の画面に表示できるように設計された、カスタマイズ可能な NOC / SOC ダッシュボードとウィジェットをオペレーションチームに提供します。SD-WAN、VPN、Wi-Fi、送受信トラフィック、アプリケーションと Web サイト、FortiSandbox 検知、エンドポイントの脆弱性、ソフトウェアインベントリ、上位の脅威、シャドー IT（監視サービス）、ZTNA など、事前定義されたダッシュボードのビューを介して、イベントをリアルタイムで監視します。



アセットとアイデンティティ

FortiAnalyzer のアセットとアイデンティティの監視機能付きファブリックビューは、EMS、NAC、フォーティネット ファブリックエージェントとのテレメトリを通じて、相関付けされたデバイスと UEBA の情報、脆弱性の検知、EMS のタグ付け、資産の分類など、組織のエンドポイントやユーザーに対する高い可視性をセキュリティチームに提供します。

ログビューにより、アナリストは、ログのドリルダウン、加工済や未加工のログ、ログのインポート / エクスポート、カスタムビューやロググループ、ファブリック ADOM のデバイスの正規化ログなどの SIEM データベースを使用して広範囲の調査を実行し、管理対象デバイスログの検索フィルターを利用することができます。

ハイライト

デプロイメント

FortiAnalyzerのデプロイ

FortiAnalyzer は、フォーティネット セキュリティ ファブリックにおいて極めて重要な役割を果たしており、分析、バックアップ、ディザスタリカバリ、ストレージ、可用性、冗長性、さらにはイベントログが大量発生するネットワークのログ収集やログ転送など、あらゆる組織のニーズを最適にサポートできるよう、さまざまな構成での導入が可能です。

FortiAnalyzer HA（高可用性）

FortiAnalyzer HA はリアルタイムの冗長性を提供し、オペレーションの継続的な可用性を確保することで組織を保護します。プライマリ（アクティブ）の FortiAnalyzer に障害が発生した場合には、セカンダリ（パッシブ）の FortiAnalyzer（最大 4 つのノードクラスタ）が直ちに引き継ぎ、ログとデータの信頼性を提供し、単一障害点のリスクを排除します。

柔軟なクォータ管理機能により、マルチテナントに対応

FortiAnalyzer は、複数のサブアカウントを管理する機能を備えており、各アカウントにはそれぞれ管理者とユーザーが割り当てられています。管理ドメイン（ADOM）別に、時間に基づくログデータのアーカイブおよび分析ポリシーを設定できるため、定義済みポリシーに基づくクォータの自動管理が可能です。また、ポリシーの構成や使用状況監視の指針となるトレンドグラフが提供されます。

アナライザモードとコレクタモード

FortiAnalyzer には、アナライザモードとコレクタモードという 2 つの動作モードがあります。コレクタモードでの主なタスクは、接続デバイスからログを収集することとログのアーカイブです。この構成では、大量のリソースを消費するログ受信タスクがコレクタにオフロードされるため、アナライザは分析やレポート生成に集中することができ、ログレートが増加している組織に多大なメリットをもたらします。

ネットワークオペレーションチームは、複数の FortiAnalyzer をコレクタモードとアナライザモードで導入して連携させることで、ログ受信と増加したログボリュームの処理の総合的パフォーマンスが向上します。これにより、ログの保存と冗長性が実現し、ネットワークと脅威に関する重要な情報を迅速に届けることができます。

サードパーティ製品との統合を可能にするログ転送機能

1 台の FortiAnalyzer ユニットから、別の FortiAnalyzer ユニット、syslog サーバー、あるいは CEF サーバーにログを転送できます。クライアントとなる FortiAnalyzer は、別のユニットやサーバーにログを転送するだけでなく、アーカイブされたログのデータポリシー設定に基づいてログのローカルコピーも保持します。ネットワークデバイスから受信したログは、リアルタイム、またはほぼリアルタイムで転送されます。

トラステッドプラットフォームモジュール（TPM）暗号化

FortiAnalyzer G シリーズは、暗号鍵の生成、保存、認証を TPM で実行して物理ネットワークアプライアンスを堅牢化する専用のマイクロコントローラーモジュールを搭載しています。このハードウェアベースのセキュリティメカニズムが、悪意のあるソフトウェアやフィッシング攻撃からユーザーを保護します。

クラウドサービス

FortiAnalyzer Cloud

FortiAnalyzer Cloud は、自動化 / 一元化された分析を実現する PaaS ベースのデリバリーオプションをお客様に提供します。この簡単にアクセスできるクラウドベースのソリューションでは、Fortinet NGFW と SD-WAN のログ管理、分析、レポート作成を実行できます。

FortiAnalyzer Cloud は、広範なレポートと監視を通じてネットワークアクティビティに関する信頼性の高い実用的インテリジェンスを提供し、組織のセキュリティ態勢を明確で一貫性のある方法で可視化します。

FortiAnalyzer Cloud には FortiCloud のポータルからシングルサインオンで簡単にアクセスいただけます。

仮想マシン

FortiAnalyzer VM

FortiAnalyzer VM（仮想マシン）は、ハードウェアアプライアンスの仮想版であり、数多くの仮想プラットフォーム上で動作してFortiAnalyzer アプライアンスの最新機能をすべて提供するように設計されています。FortiAnalyzer VM によって、ログの一元管理と分析ソリューションの簡素化、ワークフローの自動化、NOC チームや SOC チームによる脅威の特定と対応が可能になります。FortiAnalyzer VM は、サブスクリプションと永続ライセンスの両方で提供されます。

FortiAnalyzer VM Sシリーズ

FortiAnalyzer VM S シリーズは、FortiAnalyzer VM の新しいサブスクリプション型ライセンスモデルです。VM 製品の SKU と FortiCare サポートの SKU に加えて、IOC サービスと FortiAnalyzer SOC サービスも 1 つの SKU に統合されており、製品の購入、アップグレード、更新が簡素化されます。

FortiAnalyzer VM S シリーズを利用することで、組織はセキュリティイベント分析、フォレンジック分析、レポート、コンテンツアーカイブ、データマイニング、悪意のあるファイルの隔離、脆弱性の評価などの機能を一元的に利用できるようになります。

また、フォーティネットやサードパーティ製のデバイスからの地理的、時間的に異なるセキュリティデータの収集、相関付け、分析の一元化によって、セキュリティ態勢の簡素化された統合ビューが提供されます。

本サービスは、1 日あたり 5 GB、50 GB、500 GB のログに対応する積み上げ方式のライセンスであるため、一度に複数の SKU を購入することで、組織のログ要件に応じた拡張性とコスト効率を実現します。

FortiAnalyzer VM

FortiAnalyzer VM は積み上げ方式のライセンスモデルで提供されており、FortiCare Premium サポートや FortiGuard IOC（Indicators of Compromise：侵害指標）のサブスクリプションライセンスも個別に利用できます。

FortiAnalyzer ハードウェアアプライアンスのソフトウェア版であるこのバージョンは、多くの仮想化プラットフォームで動作するように設計されており、ご利用中の環境の拡張に伴って仮想ソリューションの柔軟な拡張が可能です。

技術仕様

FortiAnalyzer 仮想アプライアンス	FortiAnalyzer VM-GB1	FortiAnalyzer VM-GB5	FortiAnalyzer VM-GB25	FortiAnalyzer VM-GB100	FortiAnalyzer VM-GB500	FortiAnalyzer VM-GB2000
システム性能						
ログ処理 GB / 日 *	+ 1	+ 5	+ 25	+ 100	+ 500	+ 2,000
管理デバイス数 /VDOM 数（最大）	10,000	10,000	10,000	10,000	10,000	10,000
シャーシ管理	✓	✓	✓	✓	✓	✓
仮想マシン						
FortiGuard IOC（Indicators of Compromise：侵害指標）サービス				✓		
SOC サブスクリプション				✓		
仮想マシン						
サポートするハイパーバイザー	最新のハイパーバイザーのサポートは、FortiAnalyzer の各バージョンのリリースノートをご確認ください。 https://docs.fortinet.com/product/fortianalyzer/ にアクセスし、一番下のセクションにある「Release Notes」に進み、「Product Integration and Support」→「FortiAnalyzer [version] support」→「Virtualization」よりご参照ください。					
仮想 CPU 数（最小 / 最大）	4 / 無制限					
仮想 NIC 枚数（最小 / 最大）**	1 / 12					
メモリ（最小 / 最大）	8 GB / 無制限（64-bit の場合）					

* コレクタモードの場合は無制限
** VM は、最大 12 の vNIC インタフェースをサポートします。6.4.3 以降を実行している場合。実際に使用可能なインタフェース数は、クラウドプラットフォームにより異なります。

技術仕様



FortiAnalyzer アプライアンス	FortiAnalyzer 150G	FortiAnalyzer 300G	FortiAnalyzer 800G
システム性能			
ログ処理 GB / 日	25	100	200
分析用持続レート（ログ / 秒）[1]	500	2,000	4,000
コレクタ用持続レート（ログ / 秒）[1]	750	3,000	6,000
管理デバイス数 / VDOM 数（最大）	50	180	800
最長分析日数[2]	90	50	50
オプション			
FortiGuard IOC（Indicators of Compromise：侵害指標）サービス	✓	✓	✓
SOC サブスクリプション	✓	✓	✓
FortiGuard アウトブレイク検知サービス	✓	✓	✓
Enterprise Protection バンドル	✓	✓	✓
ハードウェアバンドル	✓	✓	✓
ハードウェア仕様			
形状（EIA 規格およびその他の 19 インチラック適合）	デスクトップ	ラックマウント（1 RU）	ラックマウント（1 RU）
インタフェース	2 x GbE RJ45	4 x GbE RJ45	4 x GbE RJ45、2 x SFP
ストレージ容量	4 TB（2 × 2 TB）	8 TB（2 × 4 TB）	16 TB（4 × 4 TB）
利用可能なストレージ（RAID 構成時）	2 TB	4 TB	8 TB
リムーバブル HDD	—	—	✓
RAID ストレージ管理	0 / 1	○（0、1）	○（0、1、1s、5、5s、10）
RAID タイプ	ソフトウェア	ソフトウェア	ハードウェア（ホットスワップ対応）
デフォルト RAID レベル	1	1	10
冗長電源（ホットスワップ対応）	—	オプション[4]	オプション
トラステッドプラットフォームモジュール（TPM）	✓[3]	✓[4]	✓
サイズ			
高さ x 幅 x 奥行	24.1 × 8.9 × 20.55 cm	4.4 × 43.8 × 41.6 cm	4.4 × 44.0 × 55.0 cm
重量	4.24 kg	10.2 kg	11.68 kg
動作環境			
AC 電源	100 ～ 240 V AC、50 ～ 60 Hz	100 ～ 240 V AC、50 ～ 60 Hz	100 ～ 240 V AC、50 ～ 60 Hz
消費電力（平均 / 最大）	36 W / 43 W	90.1 W / 99 W	134 W / 174.2 W
放熱	147.4 BTU/h	337.8 BTU/h	594.4 BTU/h
動作温度	0 ～ 40 ºC	0 ～ 40 ºC	0 ～ 40 ºC
保管温度	-20 ～ 75 ºC	-25 ～ 75 ºC	-20 ～ 75 ºC
湿度	5 ～ 95 %（結露しないこと）	20 ～ 90 %（結露しないこと）	5 ～ 95 %（結露しないこと）
エアフロー	前面 ～ 背面	前面 ～ 背面	前面 ～ 背面
動作高度	最高 2,250 m	最高 2,250 m	最高 2,250 m
準拠規格・認定			
準拠規格	FCC Part 15 Class A、RCM、VCCI、CE、UL/cUL、CB	FCC Part 15 Class A、RCM、VCCI、CE、BSMI、KC、UL/cUL、CB、GOST	FCC Part 15 Class A、RCM、VCCI、CE、UL/cUL、CB

[1] 持続レート：SQL 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メッセージレートの最大値。
[2] 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。
[3] 2022 年第 3 四半期以降の出荷分より順次対応
[4] 2022 年第 1 四半期以降の出荷分より順次対応

技術仕様




FortiAnalyzer アプライアンス	FortiAnalyzer 1000F	FortiAnalyzer 3000G	FortiAnalyzer 3500G	FortiAnalyzer 3700G
システム性能				
ログ処理 GB / 日	660	3,000	5,000	8,300
分析用持続レート（ログ / 秒）[1]	20,000	42,000	60,000	100,000
コレクタ用持続レート（ログ / 秒）[1]	30,000	60,000	90,000	150,000
管理デバイス数 / VDOM 数（最大）	2,000	4,000	10,000	10,000
最長分析日数[2]	34	30	38	60
オプション				
FortiGuard IOC（Indicators of Compromise：侵害指標）サービス	✓	✓	✓	✓
SOC サブスクリプション	✓	✓	✓	✓
FortiGuard アウトブレイク検知サービス	✓	✓	✓	✓
Enterprise Protection バンドル	✓	✓	✓	✓
ハードウェアバンドル	✓	✓	✓	✓
ハードウェア技術仕様				
形状（EIA 規格およびその他の 19 インチラック適合）	ラックマウント（2 RU）	ラックマウント（3 RU）	ラックマウント（4 RU）	ラックマウント（4 RU）
インタフェース	2 × 10 GbE RJ45、2 × 10 GbE SFP+	2 x GbE RJ45、2 × 25 GbE SFP28	2 x GbE RJ45、2 × 25 GbE SFP28	2 × 10 GbE RJ45 + 2 × 25 GbE SFP28
ストレージ容量	32 TB（8 × 4 TB）	64 TB（16 × 4TB）	96 TB（24 × 4 TB）	240 TB（60 × 4 TB）3.5 インチ HDD + 19.2 TB（6 × 3.2 TB）NVMe SSD
利用可能なストレージ（RAID 構成時）	24 TB	56 TB	80 TB	224 TB
リムーバブル HDD	✓	✓	✓	✓
RAID ストレージ管理	○（0、1、1s、5、5s、6、6s、10、50、60）	○（0、1、1s、5、5s、6、6s、10、50、60）	○（0、1、1s、5、5s、6、6s、10、50、60）	○（0、1、1s、5、5s、6、6s、10、50、60）
RAID タイプ	ハードウェア（ホットスワップ対応）	ハードウェア（ホットスワップ対応）	ハードウェア（ホットスワップ対応）	ハードウェア（ホットスワップ対応）
デフォルト RAID レベル	50	50	50	50
冗長電源（ホットスワップ対応）	✓	✓	✓	✓
トラステッドプラットフォームモジュール（TPM）	—	—	—	✓
サイズ				
高さ x 幅 x 奥行	8.9 × 43.7 × 65.0 cm	13.0 × 44.0 × 65.0 cm	17.8 × 43.7 × 66.0 cm	17.8 × 43.7 × 76.7 cm
重量	15.42 kg	30.15 kg	41.2 kg	53.5 kg
動作環境				
AC 電源	100 ～ 240 V AC、50 ～ 60 Hz	100 ～ 127 V 以上 / 10 A、200 ～ 240 V 以上 / 5 A	100 ～ 240 V AC、50 ～ 60 Hz	2,000 W AC[3]
消費電力（平均 / 最大）	192.5 W / 275 W	385 W / 500 W	629.5 W / 677.3 W	850 W / 1423.4 W
放熱	920 BTU/h	1350 BTU/h	2345.07 BTU/h	4858 BTU/h
動作温度	10 ～ 35 ºC	0 ～ 40 ºC	5 ～ 35 ºC	10 ～ 35 ºC
保管温度	-40 ～ 60 ºC	-20 ～ 75 ºC	-40 ～ 60 ºC	-40 ～ 70 ºC
湿度	8 ～ 90 %（結露しないこと）	5 ～ 95 %（結露しないこと）	8 ～ 90 %（結露しないこと）	8 ～ 90 %（結露しないこと）
エアフロー	前面 ～ 背面	前面 ～ 背面	前面 ～ 背面	前面 ～ 背面
動作高度	最高 2,250 m	最高 2,250 m	最高 2,250 m	最高 2,250 m
準拠規格・認定				
準拠規格	FCC Part 15 Class A、RCM、VCCI、CE、UL/cUL、CB	FCC Part 15 Class A、RCM、VCCI、CE、UL/cUL、CB	FCC Part 15 Class A、RCM、VCCI、CE、UL/cUL、CB	FCC Part 15 Class A、RCM、VCCI、CE、UL/cUL、CB

[1] 持続レート：SQL 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メッセージレートの最大値。
[2] 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。
[3] 3700G は、200 V ～ 240 V の電源に接続する必要があります。

オーダー情報

Product	Description
FortiAnalyzer	Centralized log and analysis appliance — 2 x RJ45 GE, 4 TB storage, up to 25 GB/ day of logs.
	Centralized log and analysis appliance — 4 x RJ45 GE, 8 TB storage, up to 100 GB/ day of logs.
	Centralized log and analysis appliance — 4 x GE, 2 x SFP, 16 TB storage, up to 200 GB/ day of logs.
	Centralized log and analysis appliance — 2 × 10GE RJ45, 2 × 10GbE SFP+, 32 TB storage, dual power supplies, up to 660 GB/ day of logs.
	Centralized log and analysis appliance — 2 x GE RJ45, 2× 25GE SFP28, 64 TB storage, dual power supplies, up to 3,000 GB/ day of logs.
	Centralized log and analysis appliance — 2 x GbE RJ45, 2 x SFP28, 96 TB storage, dual power supplies, up to 5,000 GB/ day of logs.
	Centralized log & analysis appliance - 2× 10GE RJ-45 + 2× 25GE SFP28 slots, 240TB HDD + 19.2TB NVMe SSD storage, up to 8300 GB/ day of Logs.

フォーティネットジャパン合同会社

〒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