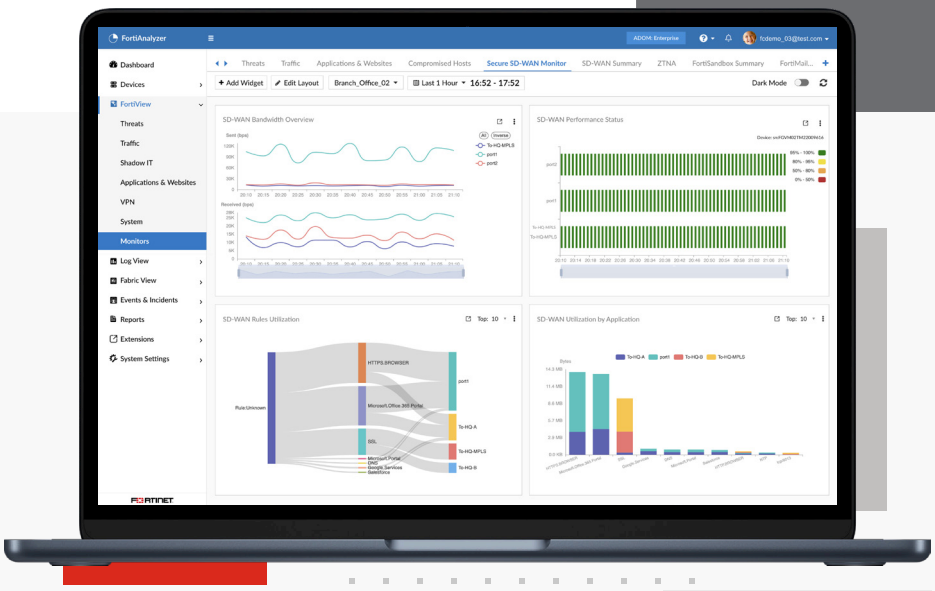
FortiAnalyzer

セキュリティ ファブリック ネットワークの分析



ハイライト

- ネットワークの監視と可視性の一元化
- イベントとログデータの相関による脅威と脆弱性の高度な検知
- 強力な NOC / SOC オペレーションによる、リアルタイムのレスポンス、分析、レポートの実現
- 自動化による、時間の短縮、エラーの軽減、効率化の支援
- クォータ管理機能による、マルチテナントへの対応
- 管理ドメインによる、オペレーションの効率化とコンプライアンスのサポート
- 70 以上のレポートと 2,000 以上のすぐに利用できるデータセット、チャート、マクロ

セキュリティ ファブリックの分析、レポート、コンプライアンス

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。

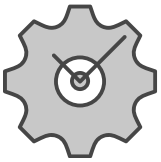
FortiAnalyzer は、フォーティネット セキュリティ ファブリックとの統合により、ネットワークオペレーションとセキュリティオペレーションのチームによるリアルタイムの検知、一元的なセキュリティ分析、エンドツーエンドのセキュリティ態勢の理解を可能にすることで、アナリストが高度な標的型攻撃（APT）を特定し、侵害が発生する前にリスクを減災できるようにします。

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

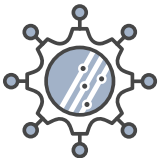
FortiAnalyzer は、すべてのデバイスログのセキュリティ ファブリック分析と、FortiGate NGFW、FortiClient、FortiSandbox、FortiWeb、FortiMail を始めとするフォーティネット製品でのイベントの相関関係と高度な標的型攻撃（APT）、脆弱性、侵害指標（IOC）のリアルタイムの検知を可能にすることで、詳細な可視性と重要かつ実用的なネットワークインテリジェンスを提供します。簡素化されたオーケストレーションと自動化されたワークフローにより、ネットワークセキュリティオペレーションチームは、リアルタイムの通知、レポート、ダッシュボードを利用できるため、一元的な可視性が実現し、実用的な結果を取得できるようになります。



インシデントとイベントの管理

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。

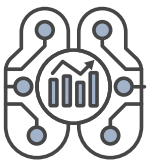
インシデントコンポーネントにより、アナリストは、イベントから作成されたインシデントを使用してインシデント処理とライフサイクルを管理し、影響を受けたアセット、エンドポイント、ユーザー、タイムラインを表示することができます。



ファブリックの自動化

FortiAnalyzer プレイブックは、インシデントレスポンスを自動化することで、組織のセキュリティチームの調査業務を簡素化し、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。すぐに利用できるプレイブックテンプレートにより、SOC アナリストによるユースケースのカスタマイズ、カスタムプロセスの定義、FortiOS や EMS など他のセキュリティ ファブリックデバイスとのやり取りが容易になります。さらには、ビジュアルプレイブックエディターでのプレイブックやタスクの編集、プレイブックモニターの利用、侵害されたホスト、感染、重大インシデントの調査、アセットビューやアイデンティティビューのデータの迅速な補強により、マルウェアや C&C IP などをブロックできるようになります。

セキュリティ ファブリック分析



分析とレポート

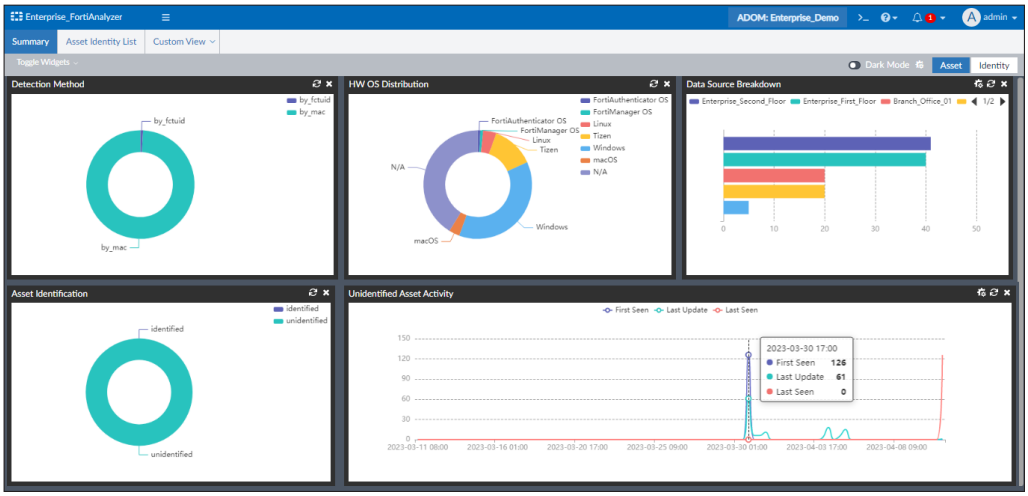
FortiAnalyzer のオートメーションドリブン分析機能は、ネットワークデバイス、システム、ユーザーを短時間で評価できるようにし、FortiGuard 脅威インテリジェンスとログデータを相関付けてリアルタイムや過去のイベントの分析を可能にすることで、ネットワークセキュリティオペレーションチームを強力に支援します。

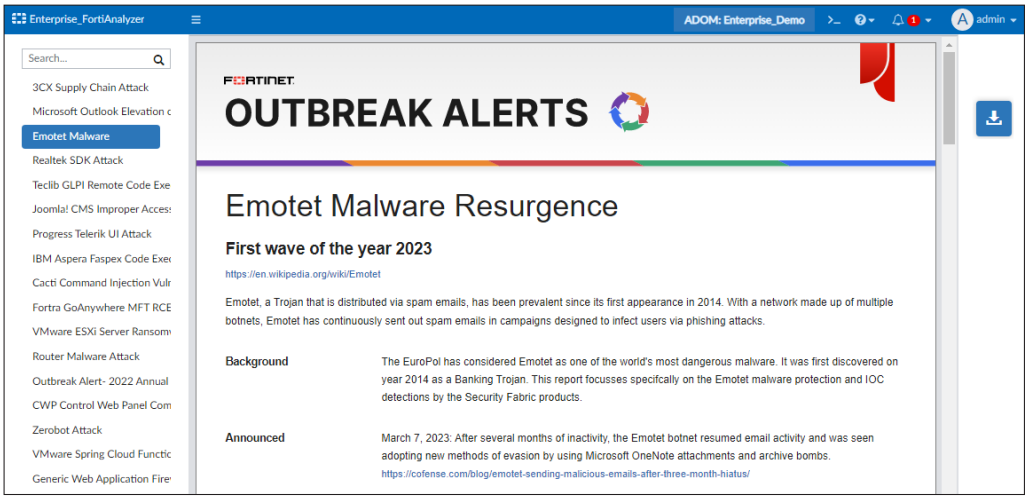
- **FortiView** のモニターとビューは、ネットワークアクティビティ、リスク、脆弱性、攻撃の試行、侵害の指標と異常、承認 / 未承認のユーザーアクティビティについての、コンテキストや意味も含む詳細で実用的なインテリジェンスを提供します。
- **ログビュー**は、SIEM データベースとファブリック ADOM のフォーティネットデバイスの正規化されたログなどのカスタムビューとロググループを提供することで、アナリストによる広範囲の調査を支援し、管理対象デバイスのログでの検索フィルターの利用やドリルダウンを可能にします。
- **レポート**は、オペレーショナルテクノロジー（OT）、セキュリティレーティング、PCI 向けセキュリティレーティング、セキュア SD-WAN、VPN、FortiNDR ネットワーク異常検知、サイバー脅威評価、360 セキュリティレビュー、状況認識、コンプライアンス、監査などのレポートを始めとする、セキュリティ態勢の包括的な分析を提供します。

機能

アセットとアイデンティティ

FortiAnalyzer ファブリックビューでアセットビューとアイデンティティ監視を利用することで、EMS、NAC、フォーティネット ファブリック エージェント、OT ダッシュボードビューとのテレメトリを通じて、相関付けされたデバイスや 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が SOC チームに提供されます。





サブスクリプションと機能拡張

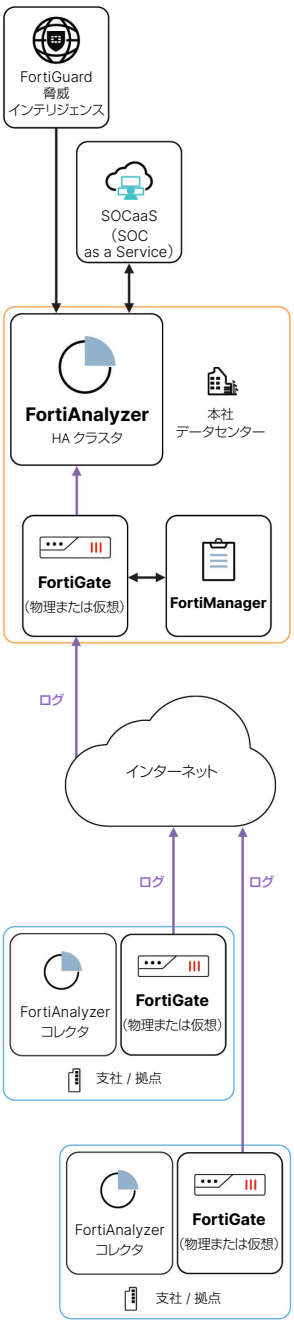
サブスクリプションライセンスと FortiGuard セキュリティサービス

- **FortiGuard アウトブレイク検知サービス：**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）サービス：**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。
- **シャドー IT 監視サービス：**承認されていないデバイスやリソース、許可されていないアカウント、さらには、SaaS や IaaS、API 統合、サードパーティアプリケーションの不正使用を継続的に監視します。このサービスは、SaaS 機能のサブスクリプションを利用している FortiCASB アカウントで相関付けられた FortiOS と FortiCASB のデータを使用して、企業資産の管理に個人アカウントを使用している不正ユーザーを識別します。
- **OT セキュリティサービス：**高度 OT 分析、リスクレポートやコンプライアンスレポート、OT イベントハンドラー、ユースケース相関ルールをセキュリティチームに提供します。
- **セキュリティレーティング / コンプライアンスサービス：**セキュリティチームによるセキュリティ態勢の設計、実装、保守を支援し、構成に関する実用的な推奨事項、重要な性能指標やリスク指標を提供します。
- **セキュリティオートメーションサービス：**サブスクリプションを利用することで、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、プレイブックによるインシデントレスポンスのさらなる自動化が実現します。

管理機能拡張アプリケーション（MEA）

管理機能拡張画面を利用することで、FortiSIEM や FortiSOAR などのフォーティネットがリリースして署名したライセンス対象アプリケーションを有効にし、FortiAnalyzer にインストールして実行することができます。

デプロイメント



FortiAnalyzer のデプロイ

FortiAnalyzer は、物理ハードウェアアプライアンス、仮想マシン（VM）、仮想マシンサブスクリプション（VM-S）に加えて、プライベートクラウドまたはパブリッククラウドのインスタンスとしての導入も可能で、スケーラビリティ、冗長性、バックアップ、高可用性の機能を提供します。

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 つのノードのクラスタ）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、接続デバイスのログの FortiAnalyzer への転送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。

FortiAnalyzer ファブリック

FortiAnalyzer ファブリックでは、SOC 管理者がスーパーバイザーとメンバーの 2 つの動作モードを構成することができます。これにより、メンバーデバイス、ADOM、認証されたログデバイス、さらには、メンバーに作成されたインシデントやイベントを表示できます。管理者は、すべての FortiAnalyzer メンバーのレポートと FortiView にアクセスでき、FortiAnalyzer ファブリックメンバーで収集されたログを、事前定義済みデバイスフィルターを使用してログビューでグローバル検索し、メンバーやメンバー ADOM にドリルダウンすることができます。

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。

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 サブスクリプション

FortiAnalyzer VM サブスクリプションライセンスモデルは、1 つの SKU（VM 製品 SKU、FortiCare サポート SKU、FortiGuard IOC およびアウトブレイク検知サービス、セキュリティオートメーションサービス）に統合することで、製品の購入、アップグレード、更新を簡素化します。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 ライセンスは積み上げ方式のライセンスモデルで提供されており、テクニカルサポートやサブスクリプションサービ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になります。

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
FortiGuard IOC（Indicators of Compromise：侵害指標）サービス			✓			
セキュリティオートメーションサービス			✓			
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）	16 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 810G	FortiAnalyzer 1000G
システム性能				
ログ処理 GB / 日	25	100	200	660
分析用持続レート（ログ / 秒）*	500	2,000	4,000	20,000
コレクタ用持続レート（ログ / 秒）*	750	3,000	6,000	30,000
管理デバイス数 / VDOM 数（最大）	50	180	800	2,000
最長分析日数 **	90	50	50	60
オプション				
FortiGuard IOC（Indicators of Compromise：侵害指標）/ アウトブレイク検知サービス	✓	✓	✓	✓
セキュリティオートメーションサービス	✓	✓	✓	✓
Enterprise Protection バンドル	✓	✓	✓	✓
ハードウェアバンドル	✓	✓	✓	✓
OT セキュリティサービス	✓	✓	✓	✓
セキュリティレーティング / コンプライアンスサービス	✓	✓	✓	✓
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）	ラックマウント（2 RU）
インタフェース	2 × GbE RJ45	4 × GbE RJ45	4 × GbE RJ45、2 × SFP	2 × 2.5 GbE RJ45 + 2 × 25 GbE SFP28
ストレージ容量	4 TB（2 × 2 TB）	8 TB（2 × 4 TB）	16 TB（4 × 4 TB）3.5 インチ SAS HDD	32 TB（8 × 4 TB）3.5 インチ SAS SED HDD
利用可能なストレージ（RAID 構成時）	2 TB	4 TB	8 TB	24 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）	○（0、1、5、6、10、50、60）
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）	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	50
冗長電源（ホットスワップ対応）	—	オプション	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）***	Gen 2	Gen 2	✓	✓
サイズ				
高さ × 幅 × 奥行	24.1 × 8.9 × 20.55 cm	4.4 × 43.8 × 41.6 cm	4.4 × 44.0 × 55.0 cm	8.8 × 43.8 × 62.0 cm
重量	4.24 kg	10.2 kg	11.68 kg	22.5 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、最大 4 A	100 ～ 240 V AC、50 ～ 60 Hz、最大 4 A
消費電力（平均 / 最大）	36 W / 43 W	90.1 W / 99 W	115 W / 150 W	251.36 W / 302 W
放熱	147.4 BTU/h	337.8 BTU/h	433 BTU/h	857.73 BTU/h
動作温度	0 ～ 40 °C	0 ～ 40 °C	0 ～ 40 °C	0 ～ 40 °C
保管温度	-20 ～ 75 °C	-25 ～ 75 °C	-20 ～ 75 °C	-40 ～ 70 °C
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）	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	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 5,000 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	FCC Part 15 Class A、RCM、VCCI、CE、UL/cUL、CB

* 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。
** 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。
*** Gen2 とは、最初のリリース以降にアップグレードされたハードウェアを指します。

技術仕様



FortiAnalyzer アプライアンス	FortiAnalyzer 3100G	FortiAnalyzer 3510G	FortiAnalyzer 3700G
システム性能			
ログ処理 GB / 日	3,000	5,000	8,300
分析用持続レート（ログ / 秒）*	42,000	60,000	100,000
コレクタ用持続レート（ログ / 秒）*	60,000	90,000	150,000
管理デバイス数 / VDOM 数（最大）	4,000	10,000	10,000
最長分析日数 **	30	35	60
オプション			
FortiGuard IOC（Indicators of Compromise：侵害指標）/ アウトブレイク検知サービス	✓	✓	✓
セキュリティオートメーション サービス	✓	✓	✓
Enterprise Protection バンドル	✓	✓	✓
ハードウェアバンドル	✓	✓	✓
OT セキュリティサービス	✓	✓	✓
セキュリティレーティング / コンプライアンスサービス	✓	✓	✓
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）	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 × GbE RJ45、 2 × 25 GbE SFP28	2 × 10 GbE RJ45、 2 × 25 GbE SFP28	2 × 10 GbE RJ45 + 2 × 25 GbE SFP28
ストレージ容量	64 TB（16 × 4TB）3.5 インチ SAS SED HDD + 3.84 TB（2 × 1.92 TB）2.5 インチ NVMe SSD	24 × 4 TB（96 TB）+ 2 × 3.84 TB（7.68 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）	56 TB	84 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）
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）
デフォルト RAID レベル	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 × 幅 × 奥行	13.0 × 44.0 × 65.0 cm	17.8 × 43.7 × 69.9 cm	17.8 × 43.7 × 76.7 cm
重量	31.57 kg	29.5 kg	53.5 kg
動作環境			
AC 電源	100 ～ 127 V 以上 / 10 A、200 ～ 240 V 以上 / 5 A	100 ～ 127 V 以上 / 10 A、200 ～ 240 V 以上 / 5 A	2,000 W AC ****
消費電力（平均 / 最大）	395 W / 510 W	983 W / 1278 W	850 W / 1423.4 W
放熱	1740.19 BTU/h	3424 BTU/h	4858 BTU/h
動作温度	0 ～ 40 °C	0 ～ 40 °C	10 ～ 35 °C
保管温度	-20 ～ 70 °C	-20 ～ 75 °C	-40 ～ 70 °C
湿度	5 ～ 95%（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）
エアフロー	前面 ～ 背面	前面 ～ 背面	前面 ～ 背面
動作高度	最高 4,000 m	最高 3,048 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

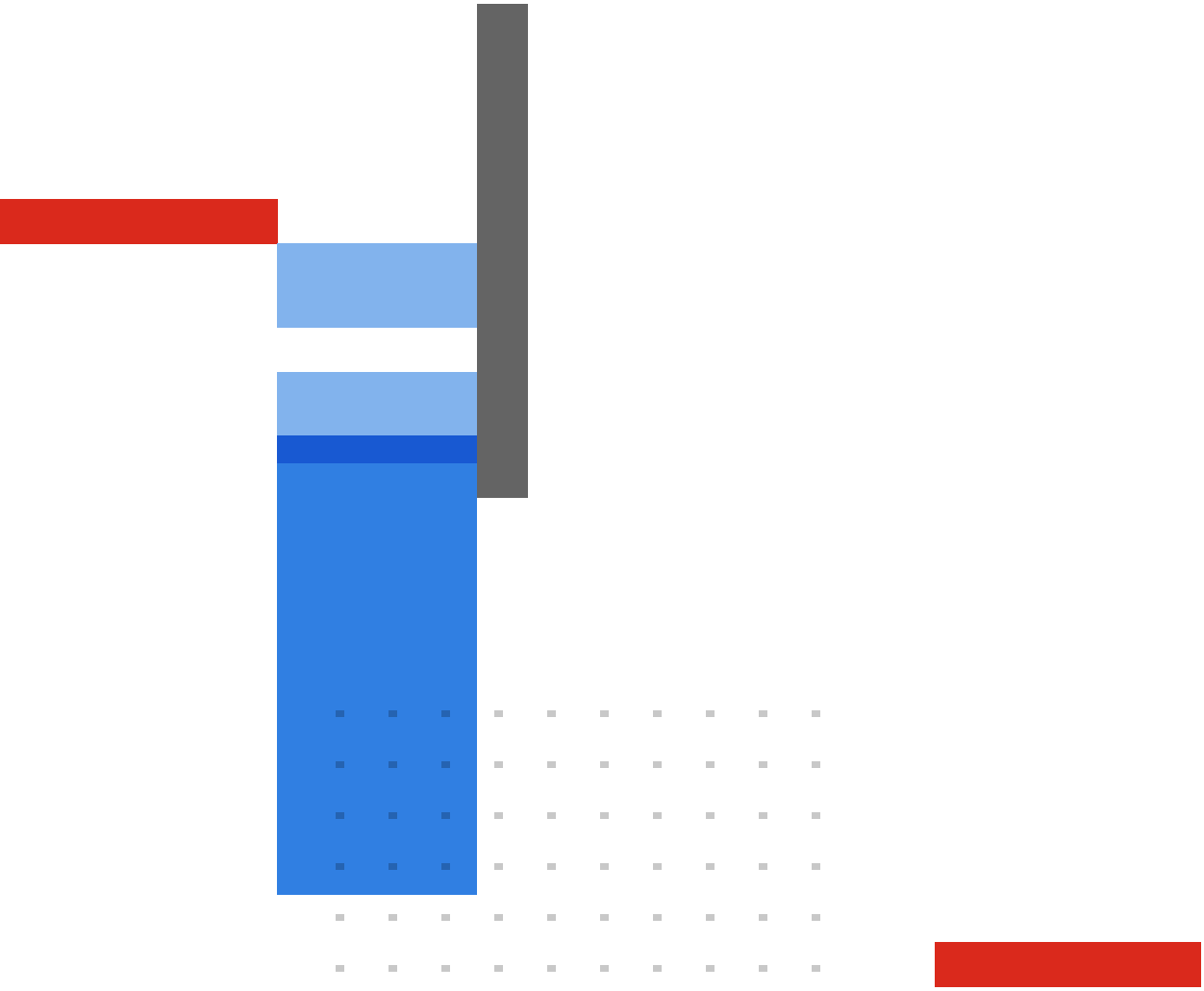
* 持続レート：SQL データベースおよびシステムのパフォーマンスを低下させることなく、最小で 48 時間 FortiAnalyzer プラットフォームが維持可能なログメッセージレートの最大値。
** ログを分析用持続レートで継続的に受信する場合に保持できる最大日数。平均ログレートが低いと保持日数は長くなります。
*** Gen2 とは、最初のリリース以降にアップグレードされたハードウェアを指します。
**** 3700G は、200 V ～ 240 V の電源に接続する必要があります。

オーダー情報

Product	SKU	Description
FortiAnalyzer	FAZ-150G	Centralized log and analysis appliance — 2x RJ45 GE, 4 TB storage, up to 25 GB/ day of logs.
	FAZ-300G	Centralized log and analysis appliance — 4x RJ45 GE, 8 TB storage, up to 100 GB/ day of logs.
	FAZ-810G	Centralized log and analysis appliance — 4x GE, 2x SFP, 16 TB self-encrypting storage, up to 200 GB/ day of logs.
	FAZ-1000G	Centralized logging and analysis appliance - 2× 2.5GbE RJ45 + 2× 25GbE SFP28, 32TB storage, up to 660 GB/Day of Logs.
	FAZ-3100G	Centralized log and analysis appliance — 2x GE RJ45, 2× 25GE SFP28, 64 TB storage, dual power supplies, up to 3000 GB/ day of logs.
	FAZ-3510G	Centralized log and analysis appliance — 2× 10GbE RJ45, 2× 25GbE SFP28, 96 TB storage, up to 5000 GB/ day of logs.
	FAZ-3700G	Centralized log and analysis appliance - 2× 10GE RJ-45 + 2× 25GE SFP28 slots, 240TB HDD + 19.2TB NVMe SSD storage, up to 8300 GB/ day of Logs.
FortiAnalyzer-VM Subscription License with Support	FC1-10-AZVMS-465-01-DD	Subscription license for 5 GB/Day Central Logging and Analytics. Include FortiCare Premium support, IOC, Security Automation Service, and FortiGuard Outbreak Detection service.
	FC2-10-AZVMS-465-01-DD	Subscription license for 50 GB/Day Central Logging and Analytics. Include FortiCare Premium support, IOC, Security Automation Service, and FortiGuard Outbreak Detection service.
	FC3-10-AZVMS-465-01-DD	Subscription license for 500 GB/Day Central Logging and Analytics. Include FortiCare Premium support, IOC, Security Automation Service, and FortiGuard Outbreak Detection service.
FortiAnalyzer-VM	FAZ-VM-GB1	Upgrade license for adding 1 GB/Day of Logs.
	FAZ-VM-GB5	Upgrade license for adding 5 GB/Day of Logs.
	FAZ-VM-GB25	Upgrade license for adding 25 GB/Day of Logs.
	FAZ-VM-GB100	Upgrade license for adding 100 GB/Day of Logs.
	FAZ-VM-GB500	Upgrade license for adding 500 GB/Day of Logs.
	FAZ-VM-GB2000	Upgrade license for adding 2 TB/Day of Logs.
FortiAnalyzer Cloud Storage Subscription	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 500 GB/Day for Central Logging and Analytics and FortiCloud SOCaaS. Include FortiCare Premium support, IOC and Security Automation Service.
FortiAnalyzer - Backup to Cloud 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 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.
	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.
	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).
Hardware Bundle	FAZ-[Hardware Model]-BDL-466-DD	Hardware plus FortiCare Premium and FortiAnalyzer Enterprise Protection.

フォーティネット CSR ポリシー

フォーティネットは、サイバーセキュリティを通じてあらゆるお客様の進歩と持続可能性を推進し、人権を尊重する倫理的な方法でビジネスを遂行し、常に信頼できるデジタル世界を実現することをお約束します。お客様には、フォーティネットの製品およびサービスを使用して、違法な検閲、監視、拘留、または過剰な武力行使などの人権の侵害または乱用に関与したり、何らかの形で支援したりしないことをフォーティネットに表明し、保証していただくことになります。フォーティネット製品の利用にあたっては、フォーティネットのEULA（エンドユーザー使用許諾契約）を遵守し、EULA に違反すると疑われる場合は、フォーティネット不正告発規定に概要が記載されている手順で報告する必要があります。



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

販売代理店
図研ネットウエイブ株式会社
本社 〒222-8505 神奈川県横浜市港北区新横浜3-1-1
TEL : 045-470-5303 FAX : 045-473-1782
中日本営業所 〒460-0003 愛知県名古屋市中区錦2-4-15 ORE錦二丁目ビル6F
TEL : 052-218-5415
西日本支店 〒530-0002 大阪市北区曽根崎新地1-4-20 桜橋IMビル8F
TEL : 06-6450-0860
MAIL : ft-info@znw.co.jp URL : https://www.znw.co.jp

DS-FAZ-R85-202406-R1