データシート

FortiAnalyzer

集中ロギング/分析/レポート

FortiAnalyzerプラットフォームによるネットワーク可視化の強化

FortiAnalyzerプラットフォームは、ネットワークのロギング/分析/レポートを単一システムに統合し、ネットワーク全体のセキュリティ イベントに関するより高度な情報の把握を可能にします。FortiAnalyzerプラットフォームを導入することにより、あらゆる規模の組織が、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、脆弱性評価などの機能を一元的に利用できるようになります。フォーティネット アプライアンスおよびサードパーティ製機器から、幅広い地域および時系列のセキュリティ データを集中的に収集し、相関性を分析することで、総合的なセキュリティの状況を容易に把握できます。FortiAnalyzer製品ファミリーを通じて、許容可能な使用ポリシーの監視および維持に必要な労力を最小化するとともに、攻撃パターンの特定に基づいてセキュリティ ポリシーを調整し、今後の攻撃阻止に備えることができます。さらに、詳細データを捕捉してフォレンジック分析に利用することで、プライバシーおよび情報セキュリティ侵害の公表に関する法令およびポリシーを厳格に遵守することが可能になります。

セキュリティ イベント情報の管理

FortiAnalyzerプラットフォームをセキュリティ インフラストラクチャに展開することで、セキュリティ イベント、アーカイブ コンテンツ、脆弱性評価を一目で把握でき、貴重な時間をより有効に利用できるようになります。FortiAnalyzerプラットフォームは、フォーティネット ソリューションによるトラフィック、イベント、攻撃、コンテンツ フィルタリング、Eメール フィルタリングなどの幅広いデータに対応します。フォレンジック分析またはネットワーク監査を実施する際に、手作業で数多くのログ ファイルを探し、複数のコンソールを分析する必要はありません。FortiAnalyzerプラットフォームには、データ アーカイブ、ファイル検疫、および脆弱性評価などの機能が一元的に含まれており、企業組織内の様々なセキュリティ活動の管理に要する時間を大幅に節約できます。

脆弱性およびコンプライアンス管理サブスクリプション

FortiAnalyzerOS 4.0のリリースでは、スキャン機能が強化されています。このスキャン機能は、ダイナミックなシグネチャ データセットを使用して脆弱性を検出し、修復を推奨します。オプションのVCM（Vulnerability and Compliance Management；脆弱性およびコンプライアンス管理）サブスクリプションでは、FortiGuardラボが開発したアップデートを頻繁に提供します。このサブスクリプションを通じて、デバイス検出、マッピング、アセット定義、アセット優先順位付け、カスタマイズされたレポートなどの機能が強化されます。

FortiAnalyzerの特色

FortiAnalyzerプラットフォームにより、きめ細かいグラフィカルなレポートに基づく完全なセキュリティ監視を実現できます。幅広いデータ収集機能は、盲点を解消しながらセキュリティ状況の把握を可能にし、また独自のフォレンジック分析ツールは、境界侵害またはデータの喪失/盗難が発生する前に、脅威を発見、分析、緩和することを可能にします。FortiAnalyzerシステムのフォレンジック分析ツールにより、詳細なユーザ アクティビティ レポートが可能となり、さらに脆弱性評価ツールによって、ネットワーク インフラストラクチャに含まれるサーバおよびホストのセキュリティ状況を自動的に確認、登録、および評価できます。

機能	メリット
ネットワーク イベント相関	IT管理者がネットワーク全域でネットワーク セキュリティ脅威をより迅速に発見および対処可能
能率的なグラフィカル レポート	FortiGate®やサードパーティ製機器で発生したイベント、アクティビティ、トレンドに関するネットワーク全体のレポートを提供
スケーラブルなパフォーマンスとキャパシティ	FortiAnalyzerファミリーモデルは、数千単位のFortiGateおよびFortiClient®エージェントをサポート
様々なレコード タイプの集中ログ	トラフィック アクティビティ、システム イベント、ウイルス、攻撃、Webフィルタリング イベント、メッセージ アクティビティ/データなど
フォーティネット製品ポートフォリオとのシームレスな統合	密接な統合によってパフォーマンスが最大化され、FortiAnalyzerリソースをFortiGateまたはFortiManager®ユーザ インタフェースで管理可能





技術仕様	FortiAnalyzer-200D	FortiAnalyzer-400C	FortiAnalyzer-1000C*	FortiAnalyzer-2000B*	FortiAnalyzer-4000B
インタフェースとモジュール					
GbE SFP インタフェース	–	–	–	–	2
10/100/1000 インタフェース	4	4	4	6	2
HDD数	1	1	1 (最大4)	2 (最大6)	6 (最大24)
ストレージ	1 x 1 TB	1 x 2 TB	1 x 2 TB (最大8TB)	2 x 2 TB (最大12TB)	6 x 1 TB (最大24TB)
RAIDストレージ管理	–	–	RAID 0、1、10 (追加HDD装着時)	RAID 0、1、5、10、50	RAID 0、1、5、6、 10、50、60
システム仕様					
ログパフォーマンス (ログ/秒:スタンドアローンモード)	350	625	1,000	3,000	6,000
データ受信レート	1.4 Mbps	2.5 Mbps	4 Mbps	12 Mbps	24 Mbps
ライセンス承諾 ネットワーク機器数**	150	200	2,000	2,000	2,000
FortiClient管理数	100	2,000	無制限	無制限	無制限
仮想管理 (ADOM)	1	10	50	100	250
ハードウェア仕様					
高さ	4.5 cm	4.4 cm	4.3 cm	8.6 cm	17.5 cm
幅	43.3 cm	43.5 cm	43.4 cm	44.3 cm	48.5 cm
奥行	35.2 cm	36.4 cm	62.7 cm	68.1 cm	69.0 cm
重量	6.1 kg	6.7 kg	15.9 kg	28.6 kg	43 kg
形状	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 (1 RU)	ラックマウント (2 RU)	ラックマウント (3 RU)
AC電源	100 - 240 VAC、 50 - 60 Hz	100 - 240 VAC、 50 - 60 Hz、4 A (最大)	100 - 240 VAC、 50 - 60 Hz、7.5 A (最大)	100 - 240 VAC、 50 - 60 Hz、9A (最大)	100 - 240 VAC、 50 - 60 Hz、11.5 A (最大)
消費電力 (平均)	60 W	100 W	189 W	200 W	420 W (6 HDD)
冗長電源 (ホットスワップ対応)	–	–	–	○	○
動作環境					
動作温度	0 ～ 40℃	10 ～ 35℃	0 ～ 35℃	10 ～ 35℃	0 ～ 40℃
保管温度	-25 ～ 70 ℃	-25 ～ 70 ℃	-40 ～ 65 ℃	-40 ～ 65 ℃	-25 ～ 70 ℃
湿度	5 ～ 95% (結露しないこと)	10 ～ 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)	5 ～ 95% (結露しないこと)
準拠規格					
準拠規格	FCC Part 15 Class A、 UL/CUL、CE、C Tick、 VCCI、CB	FCC Part 15 Class A、 UL/CUL、CE、C Tick、 VCCI、CB	FCC Part 15 Class A、 UL/CUL、CE、C Tick、 VCCI、CB、BSMI、NOM、 GOST	FCC Part 15 Class A、 UL/CUL、CE、 C Tick、VCCI、CB、 BSMI、GOST、KC	FCC Part 15 Class A、 UL/CUL、CE、C Tick、 VCCI、CB、BSMI

* ハードウェア Generation 2 の値です。

** ライセンス許諾ネットワーク機器の定義は次の通りです。

VDOM (仮想UTM) モードをイネーブルにしていない1台のFortiGateユニット
または FortiGateユニットを複数VDOMモードで実行している場合1つのVDOM
または 1台のサードパーティ製Syslog互換機器

グラフィック レポート

FortiAnalyzerシステムが備える、グラフィカルな標準レポートの総合的なセットおよびそれらをフレキシブルにカスタマイズする機能により、ネットワークまたはセキュリティの管理者はネットワーク保護に必要な情報を確保し、より高度なネットワーク管理を実現できます。またネットワーク情報をアーカイブ、フィルタリング、およびデータマイニングすることにより、法令遵守または履歴分析のために活用できます。

きめ細かな情報

FortiAnalyzerユーザインタフェースにより、セキュリティ ログ データを特定範囲に絞って詳しく調査し、ネットワークの状況を理解するために必要なきめ細かいレポートを入手できます。時系列のビューまたはリアルタイムのビューを活用することで、ログおよびコンテンツ情報、さらにネットワーク トラフィックを分析できます。また高度なフォレンジック分析ツールにより、コンテンツレベルでのユーザ活動の追跡が可能となります。

リアルタイム ログ ビューア

ネットワーク、トラフィック、およびユーザ イベントのリアルタイムによる監視、または特定イベントの履歴データのブラウズが可能なことにより、ネットワークのセキュリティ脅威、パフォーマンス、およびユーザ行動に関する高度な洞察を得ることができます。

サポート対象機器

- FortiGate
- FortiMail
- FortiClient
- FortiManager
- Syslog互換全機器

機能詳細

一般システム機能

プロファイル ベースの管理
FortiAnalyzerサーバおよびFortiGate機器間の通信および認証を暗号化する、セキュアなWebベースのユーザ インタフェース
メールサーバ アラート出力
FortiAnalyzerの接続/同期
SNMPトラップ
Syslogサーバ サポート
RAID構成、RAIDレベルの変更/表示
NAS(Network Attached Storage)のサポート
起動管理モジュール
起動管理コンソール
基本システム設定
オンライン ヘルプ
FortiGate機器の追加/変更/削除
機器グループの表示
ブロックされた機器の表示
アラート/アラート イベントの表示
アラート メッセージ コンソール
FortiManager接続ステータスの表示
システム情報/リソースの表示
統計の表示
オプション履歴の表示
セッション情報の表示
バックアップ/リストア
工場出荷時システム設定のリストア
ログ ディスクのフォーマット
FortiAnalyzerから他へのデータ移行

DLPアーカイブ/データ マイニング

情報漏洩の検出と分析を行うための、追加ツールによるログ分析&レポートの全機能
トラフィックの種類ごとに表示
次のようなコンテンツの表示:HTTP(Web URL)、FTP(ファイル名)、Eメール(テキスト)、およびインスタント メッセージング(テキスト)
セキュリティ イベント サマリの表示
トラフィック サマリの表示
トラフィックの最大生成者の表示

ネットワーク アナライザ

リアルタイム トラフィック ビューア
トラフィック履歴ビューア
カスタマイズ可能なトラフィック アナライザログ
ネットワーク トラフィック ログの検索

ログの分析およびレポート

ログの表示/検索/管理
自動ログ監視
プロファイル ベースのレポート
300超の定義済みレポート、カスタマイズ可能
レポート例:
攻撃:FortiGateユニット別、時刻別、カテゴリー別、上位の攻撃源別
ウイルス:上位検出ウイルス、プロトコル別の検出ウイルス
イベント:ファイアウォールによる、トリガされた全イベント、トリガされたセキュリティ イベント、曜日別のトリガされたイベント
メール利用状況:インバウンド/アウトバウンド Web利用レポートによる上位メール ユーザ
Web利用状況:上位Webユーザ、ブロックされた上位サイト、ブロックされたサイトに接続を試みた上位クライアント
帯域利用:上位帯域ユーザ、日付および時刻別の帯域利用、プロトコルファミリー別の帯域利用
プロトコル:上位使用プロトコル、上位FTPユーザ、上位Telnetユーザ
WAN最適化ログ情報
ログを集約しFortiAnalyzerに一元化
FortiClient個別レポート

集中隔離

隔離設定の構成
隔離されたファイルのリストの表示
ファイルの種類ごとの隔離サマリ、検出された理由、最初と最後の検出時刻、ユニークな検出ファイルの総数、各種類および理由ごとの検出総数

フォレンジック分析

ユーザ名、メール アドレス、またはIM名によるユーザ活動の追跡
FortiGuard Webコンテンツ フィルタリングレポートを通じて、ユーザごとのWebサイト アクセスおよびブロックされたWebサイトを表示
設定可能な次のようなレポート パラメータ:プロファイル、デバイス、範囲、種類、フォーマット、スケジュール、アウトプット
カスタマイズされたレポートの出力
オンデマンドでのレポート
レポート閲覧

ログ ブラウザおよびリアルタイム ログ ビューワ

リアルタイム ログ ビューア
ログ履歴ビューア
カスタマイズされたログ ビューア
ログ フィルタリング、検索、ローリング
トップ ユーザ
Web、Eメール、FTPトラフィックの表示
インスタント メッセージングおよびP2Pトラフィックの表示
フィルタ トラフィック サマリ
機器サマリ
次のようなトラフィック レポート:イベント(管理監査)、検出されたウイルス、攻撃(IPS攻撃)、Webコンテンツ フィルタリング、Eメール フィルタリング、コンテンツ(Web、Eメール、IM)

脆弱性およびコンプライアンス管理スキャン

脆弱性シグネチャの基本セット、オプションのサブスクリプションでアップデート
脆弱性の検出/修復の推奨
アセット クラスによるグループ/レポート
CVE名による検索とのCVE互換
PCI DSSスキャンおよびレポート

FortiCareサポートサービス: 全てのフォーティネット製品においてグローバルサポートを提供するサービスです。FortiCareサポートによりフォーティネット製品を最適にご利用いただくことが可能になります。サポートプランには、Technical Assistant Center (TAC)を通じて、製品サポート(ソフトウェア、ハードウェア)を当社の1次代理店様にご提供します。また、万一のハードウェア不良時に備え、センドバック方式によるハードウェアRMA交換サービス(良品、後出し)を含む平日の9時間サポートから、オプションとして、プレミアムサポート、プレミアムRMA交換サービス、プロフェッショナルサービス等もございます。 *FortiCareサポートサービスは、当社の1次代理店様経由でご提供させていただきます。

FortiGuardサブスクリプションサービス: フォーティネット製品に対して、動的な自動セキュリティアップデート配信を提供するサービスです。フォーティネットのグローバルセキュリティ研究チームが開発するこれらのセキュリティアップデートにより、巧妙な脅威に対する最新のプロテクションが確保できます。サブスクリプションには、アンチウイルス、不正侵入検知/防御Webコンテンツフィルタリング、アンチスパム、脆弱性/コンプライアンス管理、アプリケーション制御、Webアプリケーションファイアウォール、データベースセキュリティサービスなどが含まれます。

FORTINET

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 7-18-18
住友不動産六本木通ビル 8 階
TEL:03-6434-8531/8533
www.fortinet.co.jp

お問い合わせ