FortiSIEM

統合型のイベント相関とリスク管理を最新のネットワークで実現

もはや情報を保護するだけではセキュリティを確保できません。顧客との信頼関係を維持し、戦略的イニシアチブを確実に成功させるようにすることで企業のブランドと評判を守ることが不可欠です。

セキュリティとコンプライアンスが容易に

企業でセキュリティ侵害が発生すると、顧客は他社と取引するようになり、収益に非常に深刻な影響を及ぼします。新規顧客の獲得に要するコストは、既存顧客の維持の7倍になると試算されています。また、罰金や裁判費用も瞬く間に大変な金額となります。株式を公開している会社では、株価、サプライヤーとの関係、株主からの評価などに長期的なマイナスの影響が及ぶ可能性もあります。以上の点を考慮すると、セキュリティ上の意思決定に以前よりも多くの取締役が関与するようになったのは当然の成り行きだと言えます。FortiSIEMは、IoTからクラウドまでを対象にした総合的で拡張性に優れたソリューションを提供します。ネットワークセキュリティ、パフォーマンス、コンプライアンス標準を確実に管理できる特許取得済の優れた分析機能を備えており、組織全体の一元的な管理が可能です。

NOC 分析と SOC 分析の統合（特許取得済み）

フォーティネットは、ログ、パフォーマンス評価基準、SNMPトラップ、セキュリティアラート、構成変更など多様なソースからの情報に基づいた統合型相互相関分析を可能にするアーキテクチャを開発しました。従来型の分析は個々のサイロで（SOCおよびNOCから）監視されていましたが、FortSIEMではすべてのデータを集約し、組織内で入手可能な脅威データを包括的に表示できるようになります。すべての情報はイベントに変換され、解析された後にイベントベースの分析エンジンで処理され、リアルタイム検索、ルール、ダッシュボード、およびアドホッククエリに使用されます。

ハイライト

- リアルタイムのネットワーク分析
- 即座にセキュリティとコンプライアンスを実現
- ITの一元管理画面
- クラウドスケールのアーキテクチャ
- 自己学習型の資産インベントリ（CMDB）
- マルチテナント環境のサポート
- MSP / MSSP対応
- SOC分析とNOC分析の相互相関
- 仮想または物理アプライアンスとして利用可能

ハイライト

FortiGuard の脅威インテリジェンスと IoC（Indicators of Compromise：侵害指標）を、オープンソースの脅威インテリジェンスフィード、商用のソース、およびカスタムデータソースから送信された外部の脅威インテリジェンス（TI）と容易に統合し、FortiSIEM TI フレームワークに取り込むことができます。このように多様なソースのデータがすべて統合されるため、瞬時に包括的なダッシュボードとレポートを作成し、脅威の根本原因を短時間で特定すること、ならびに修正と将来的な脅威の防止に必要な措置を講じることが可能です。

分散型リアルタイムイベント相関（特許取得済）

分散型のイベント相関は難しい問題です。これは、ルールをトリガーするには、複数のノードが自身の一部の状態をリアルタイムで共有する必要があるためです。多くの SIEM ベンダーが分散データ収集機能と分散検索機能を提供していますが、分散型のリアルタイムイベント相関エンジンを提供しているのはフォーティネットだけです。遅延を最小限に抑え、複雑なイベントパターンをリアルタイムで検知できます。FortiSIEM では、この特許取得済のアルゴリズムにより、イベント発生率が高い場合であっても多数のルールがリアルタイムで処理され、脅威の検知時間が加速します。

自動化されたリアルタイムのインフラストラクチャ検出 / アプリケーション検出エンジン（CMDB）

問題の迅速な解決には、インフラストラクチャコンテキストが必要です。ログ分析 / SIEM ベンダー製品の大半では、すぐに古くなってしまい、人的ミスが発生しがちなコンテキストを手動で提供する管理者を必要としています。フォーティネットは、デバイスやアプリケーションに関して事前知識が一切なくても、認証情報を使用するだけでオンプレミス / パブリッククラウド / プライベートクラウドにおいて物理および仮想インフラストラクチャのトポロジーを検出してマッピングできる、インテリジェントなインフラストラクチャ / アプリケーション検出エンジンを開発しました。

検出は、広く（Tier 1 / 2 / 3 ベンダーの多くをカバー）かつ深い（システム、ハードウェア、ソフトウェア、実行中のサービス、アプリケーション、ストレージ、ユーザー、ネットワーク構成、トポロジー、デバイスの関係をカバー）範囲が対象です。検出はオンデマンドまたは定期的な実行が可能で、インフラストラクチャの変更をリアルタイムで検出し、追加されたデバイスやアプリケーションをレポートします。これは、コンプライアンス要件を管理するうえで不可欠な要素であり、FortiSIEM が提供できる独自の機能です。最新の CMDB（Centralized Management Database：一元管理データベース）により、検索条件で CMDB オブジェクトを使用する高度なコンテキスト対応イベント分析が可能です。

ユーザー ID の動的マッピング

ログ分析に欠かせないコンテキストは、ネットワーク ID（IP アドレス、MAC アドレス）とユーザー ID（ログ名、フルネーム、組織内の役割（ロール））のつながりです。この情報は、DHCP や VPN 経由でユーザーが新しいアドレスを取得するたびに変化します。

フォーティネットは、動的なユーザー ID マッピングの方法論を開発しました。まず、ユーザーとそのロールが Microsoft Active Directory、Open LDAP などのオンプレミスリポジトリから、または OKTA などのクラウド SSO リポジトリから検出されます。新しいユーザーを検出するためのこの操作は、オンデマンドまたは定期的な実行が可能です。同時に、ファイアウォールネットワーク変換イベント、Active Directory ログオン、VPN ログオン、WLAN ログオン、Host Agent 登録ログなどの重要なネットワークイベントからネットワーク ID が特定されます。最終的に、FortiSIEM はリアルタイムの分散インメモリデータベースにユーザー ID、ネットワーク ID、位置情報 ID を結合することによって、動的なユーザー ID 監査証跡を作成します。これにより、IP アドレスではなくユーザー ID に基づいたポリシーの作成や調査の実施が可能となり、問題が迅速に解決されます。

柔軟で高速なカスタムログ解析フレームワーク（特許取得済）

効果的なログ解析を実現するには、カスタムスクリプトが必要です。しかし、Active Directory やファイアウォールなどの大量のログの場合、解析の実行には時間がかかります。一方、コンパイル済のコードは高速で実行できますが、新しいリリースが必要であるため柔軟性が十分とは言えません。フォーティネットは、高水準のプログラミング言語と同等の機能を有し、簡単に変更できると同時に実行時のコンパイルも可能で、効率に優れた XML ベースのイベント解析言語を開発しました。この特許取得済のソリューションを使用する FortiSIEM の解析ツールは、大半の競合他社の解析ツールに比べていずれも性能が優れており、ノードあたり 10,000EPS 以上での解析が可能です。

構造化 / 非構造化データフィードを活用するハイブリッドデータベースアーキテクチャ

FortiSIEM は、2 つの異なる情報ソースを活用します。検出される情報は構造化データで、従来型のリレーショナルデータベースに適しています。一方、ログやパフォーマンス評価基準などは非構造化データで、NoSQL タイプのデータベースが必要です。フォーティネットは、最適化されたデータベースにデータが格納されるハイブリッドアプローチを開発しました。独自のビジネスレイヤーロジックが組み込まれているため、単一の包括的なデータベース抽象化レイヤーを提供します。

ユーザーは、（リレーショナルデータベースに格納された）CMDB オブジェクトを使用して（NoSQL データベースに格納された）イベントを検索することができます。このアプローチでは、両方のデータベースの長所と利点が活かされます。

ハイライト

大規模な脅威データの統合

FortiGuard Labs の脅威インテリジェンスサービスに加えて、外部のさまざまな脅威データのサブスクリプションをお客様が選択し、ネットワーク内の潜在的脅威からの保護に役立てることができます。しかし、IP アドレス、マルウェアドメイン、ハッシュ、URL などの件数が数百万件に達することも珍しくなく、脅威データが非常に大規模になるケースもあります。また、Web サイトやドメインは次々に閉鎖されては公開されるため、情報は瞬く間に古くなる可能性があります。その結果、脅威インテリジェンスデータの利用者は大きな課題を抱えることになります。フォーティネットは、大量の情報をソースから迅速に取得し、さまざまな FortiSIEM ノードに効果的に分散し、他のプロバイダーよりも高速（ノードあたり 10,000EPS 以上）でのリアルタイム評価を可能にする独自のアルゴリズムを開発しました。

大規模エンタープライズとマネージドサービスプロバイダーに対応する「マルチテナントアーキテクチャ」

フォーティネットは、大規模な企業やサービスプロバイダーが単一のコンソールから多数の物理 / 論理ドメイン、および重複するシステムやネットワークを管理できるようにする、カスタマイズ性の高いマルチテナントアーキテクチャを開発しました。この環境では、物理 / 論理ドメインおよび個々の顧客のネットワーク上の情報を極めて容易に相互相関することができます。独自のレポート、ルール、およびダッシュボードを容易に作成でき、それらを幅広いレポートドメインや顧客向けに展開できます。また、イベントのアーカイブ化ポリシーをドメイン毎あるいは顧客毎に適用可能です。

機能

迅速なセキュリティ分析を可能にするリアルタイム運用コンテキスト

- 継続的に更新される精度の高いデバイスコンテキスト（構成、インストール済のソフトウェアとパッチ、実行中のサービス）
- システムとアプリケーションのパフォーマンス分析、そして相互関係のコンテキストデータによる、セキュリティ問題の迅速な優先順位付け
- IP アドレス、ユーザー ID の変更、物理的な位置情報データのコンテキストの監査証跡をはじめとする、リアルタイムのユーザーコンテキスト
- 不正なネットワークデバイスやアプリケーション、構成の変更を検出

すぐに利用可能なコンプライアンスレポート

- 次のような幅広いコンプライアンスの監査 / 管理要件を満たし、事前設定済ですぐに利用可能なレポート：PCI-DSS、HIPAA、SOX、NERC、FISMA、ISO、GLBA、GPG13、SANS Critical Controls

パフォーマンスの監視

- 基本的なシステム / 一般的な評価基準を監視
- SNMP、WMI、PowerShell を介したシステムレベル
- JMX、WMI、PowerShell を介したアプリケーションレベル
- VMware、Hyper-V 向けの仮想化監視：ゲスト、ホスト、リソースプール、クラスタレベル
- ストレージ使用、パフォーマンスの監視：EMC、NetApp、Isilon、Nutanix、Nimble、Data Domain
- 専用アプリケーションのパフォーマンス監視
- Microsoft Active Directory と Exchange（WMI、Powershell 経由）
- データベース：Oracle、MS SQL、JDBC 経由の MySQL
- VoIP インフラストラクチャ（IPSLA、SNMP、CDR/CMR 経由）
- フロー分析とアプリケーションパフォーマンス：Netflow、SFlow、Cisco AVC、NBAR
- カスタム評価基準を追加する機能
- ベースライン評価基準と重大な逸脱の検出

可用性の監視

- システムのアップ / ダウンの監視：Ping、SNMP、WMI、アップタイム分析、クリティカルインタフェース、クリティカルプロセスとサービス、BGP / OSPF / EIGRP ステータスの変化、ストレージポートのアップ / ダウンに基づく
- Synthetic Transaction Monitoring を介したサービスの可用性モデリング：Ping、HTTP、HTTPS、DNS、LDAP、SSH、SMTP、IMAP、POP、FTP、JDBC、ICMP、トレースルート、一般的な TCP/UDP ポート
- 保守期間のスケジューリングに役立つ保守カレンダー
- SLA の算出：「通常」の業務時間と時間外を留意

機能

構成変更のリアルタイム監視

- バージョン管理されたリポジトリに保存されているネットワーク構成ファイルを収集
- バージョン管理されたリポジトリに保存されているインストール済ソフトウェアのバージョンを収集
- ネットワーク構成およびインストール済ソフトウェアの変更を自動検出
- 変更したユーザー、変更内容をはじめとする、ファイル / フォルダ（Windows および Linux）の変更の自動検出
- 承認済構成ファイルの変更の自動検出
- FortiSIEM Windows エージェントを介した Windows レジストリの変更の自動検出

デバイスやアプリケーションのコンテキスト

- スイッチ、ルータ、無線 LAN などのネットワークデバイス
- セキュリティデバイス：ファイアウォール、ネットワーク IPS、Web / 電子メールゲートウェイ、マルウェア対策、脆弱性スキャナ
- Windows、Linux、AIX、HP UX などのサーバー
- DNS、DHCP、DFS、AAA、ドメインコントローラ、VoIP などのインフラストラクチャサービス
- Web サーバー、アプリケーションサーバー、メール、データベースなど、ユーザーが直接使用するアプリケーション
- NetApp、EMC、Isilon、Nutanix、Data Domain などのストレージデバイス
- AWS、Box.com、Okta、Salesforce.com などのクラウドアプリケーション
- AWS などのクラウドインフラストラクチャ
- UPS、HVAC、デバイスハードウェアなどの周辺デバイス
- VMware ESX、Microsoft HyperV などの仮想化インフラストラクチャ

拡張性と柔軟性を兼ね備えたログ収集機能

- ノードあたり 10,000 イベント / 秒を超える高速でセキュリティログを収集、解析、標準化、保存
- オンプレミスとクラウドの両方で幅広いセキュリティシステムとベンダー API を標準サポート
- ファイルの完全性の監視、インストール済みソフトウェアの変更とレジストリの変更の監視など、Windows エージェントが優れた拡張性と徹底したイベント収集機能を提供
- Linux エージェントによるファイル整合性監視
- 稼働中のシステムにおいてダウンタイムやイベントロスを発生させることなく、GUI から解析ツールを変更して再配備
- 統合解析ツール開発環境を介して新しい解析ツール（XML テンプレート）を作成し、エクスポート / インポート機能を通じてユーザー間で共有
- あらゆる場所のユーザーおよびデバイスのイベントをセキュアに、そして確実に収集

通知とインシデント管理

- ポリシーベースのインシデント通知フレームワーク
- 指定したインシデントが発生した場合に修正スクリプトを開始
- 外部のチケット発行システム（ServiceNow、ConnectWise、Remedy）との API ベースの統合
- チケット発行システムを内蔵
- インシデントレポートの構造化により、ビジネスクリティカルなサービスやアプリケーションに最高の優先度を設定可能
- 複雑なイベントパターンを検知すると、リアルタイムで分析を開始

機能豊富でカスタマイズ可能なダッシュボード

- KPI を表示する「スライドショー」のスクロール機能を搭載し、カスタマイズにも対応するリアルタイムダッシュボード
- 組織全体およびユーザー間で共有可能なレポートと分析結果
- 色分けにより重大な問題を瞬時に識別
- 高速表示：インメモリ計算による更新
- ビジネスサービス、仮想インフラストラクチャ、専用アプリケーションに特化した多層型ダッシュボード

外部の脅威インテリジェンスとの統合

- 外部の脅威インテリジェンスとの統合用 API：マルウェアドメイン、IP、URL、ハッシュ、Tor ノード
- 一般的な脅威インテリジェンスソースとの統合機能：ThreatStream、CyberArk SANS、Zeus
- 大規模な脅威データを処理するテクノロジー：クラスタ内での逐次ダウンロードと共有、ネットワークトラフィックとのリアルタイムパターンマッチング

パワフルでスケーラブルな分析機能

- インデックス化を必要としないリアルタイムでのイベント検索
- キーワードおよびイベントベースの検索
- 履歴イベントの検索：ブール値フィルタ条件を使用した SQL 類似のクエリ、関連アグリゲーションによるグループ化、時刻フィルタ、正規表現の一致、計算式 — GUI および API
- 検出した CMDB オブジェクト、ユーザー / ID と位置データを検索とルールで使用
- レポートをスケジューリングし、主要な関係者に結果を電子メールで送信
- 組織全体または物理 / 論理レポートドメインにわたってイベントを検索
- 深刻な違反者を追跡するための動的な監視リスト（監視リストは任意のレポートルールで使用可能）
- ダウンタイムを発生させることなくワーカーノードの追加が可能なため、分析フィードを拡張可能

機能

ベースラインの設定と統計的異常の検出

- ベースラインエンドポイント / サーバー / ユーザーのビヘイビア：時刻、平日 / 週末の粒度
- 高度な柔軟性：任意のキーや評価基準を「ベースラインに設定」可能
- 統計的異常に対する内蔵型でカスタマイズ可能なトリガー

外部テクノロジーとの統合

- 任意の外部 Web サイトとの統合による IP アドレスの検索
- API ベースの統合による外部の脅威インテリジェンスソースの活用
- ヘルプデスクシステムとの API ベースの双方向統合：ServiceNow、ConnectWise、Remedy を短時間でシームレスにサポート
- 外部 CMDB との API ベースの双方向統合：ServiceNow、ConnectWise を短時間でシームレスにサポート
- Kafka のサポートにより、拡張分析レポート機能との統合が可能：ELK、Tableau、Hadoop など
- プロビジョニングシステムとの統合を容易にする API
- 組織の追加、認証情報の作成、検出の開始、監視イベントの変更を可能にする API

シンプルで柔軟な管理

- Web ベースの GUI
- 機能豊富なロールベースのアクセス制御により、GUI とデータへのアクセスをさまざまなレベルで制限
- モジュール間の全通信を HTTPS で保護
- FortiSIEM の全ユーザーアクティビティの監査証跡
- 最小限のダウンタイムとイベントロスで容易なソフトウェアアップグレードを実現
- FortiSIEM ナレッジベース（解析ツール、ルール、レポート）の迅速な更新が可能
- ポリシーベースのアーカイブ化
- 否認不可や整合性検証時に有効なログのハッシュ化
- 柔軟なユーザー認証：Microsoft AD と OpenLDAP 経由でのローカル、外部、Okta 経由のクラウド SSO / SAML
- リモート SSH トンネル経由で FortiSIEM GUI からコレクタの背後でリモートサーバーにログインする機能

容易にスケールアウト可能なアーキテクチャ

- 以下のハイパーバイザー上で、オンプレミスまたはパブリック / プライベートクラウド環境向けに仮想マシンとして導入可能：VMware ESX、Microsoft Hyper-V、KVM、Amazon Web Services AMI、OpenStack
- パフォーマンスレベルの異なる複数の物理アプライアンスモデルにより、多様な導入オプションに対応
- Collector を複数導入することで、大規模データ収集が可能
- FortiSIEM Supervisor との接続が不可の場合、Collector はイベントのバッファリングが可能
- Worker を複数導入することで、大規模分析が可能
- Collecrot を介してリモートサイトからイベントを収集する、ロードバランスアーキテクチャを内蔵

FortiSIEM Windows エージェント

フォーティネットは、情報収集の効率に優れたエージェントレステクノロジーを開発しました。しかし、ファイル整合性の監視データなどの一部の情報は、リモートから収集するにはコストがかかります。FortiSIEM には、フォーティネットのエージェントレステクノロジーと新たに開発された高性能エージェントが統合されており、データ収集機能が大幅に向上しています。

	エージェントレス テクノロジー	アドバンスド エージェント
エージェントレス		
検出	•	
パフォーマンスの監視	•	
（低パフォーマンスの）システム、アプリケーションおよびセキュリティログ収集	•	
エージェント		
（高パフォーマンスの）システム、アプリケーションおよびセキュリティログ収集		•
DNS、DHCP、DFS、IISログ収集		•
1つのエージェントマネージャにつき最大10,000エージェント		•
ローカルでの解析と時間の正規化		•
インストール済ソフトウェアの検出		•
レジストリ変更の監視		•
ファイルの整合性監視		•
顧客ログファイルの監視		•
WMIコマンド出力の監視		•
PowerShellコマンド出力の監視		•

技術仕様

	FortiSIEM 500F “Collector”	FortiSIEM 2000F “supervisor”	FortiSIEM 3500F “supervisor”
ハードウェア仕様			
オールインワンのライセンス数	—	最大500	最大2,000
EPS性能	5,000	最大5,000	最大20,000
メモリ	DDR3 16 GB（2 x 8 GB）	DDR3 32 GB（4 x 8 GB）	DDR3 64 GB（8 x 8 GB）
ネットワークインタフェース	4 x GbE RJ45 インタフェース	4 x GbE RJ45 インタフェース	2 x GbE RJ45インタフェース、2 x SFPインタフェース
管理コンソールインタフェース	DB-9	DB-9	DB-9
USBインタフェース	2 x USB 2.0、2 x USB 3.0	2 x USB 2.0、2 x USB 3.0	4 x USB 2.0
ストレージ	3 TB（1 x 3 TB）	36 TB（12 x 3 TB）	72 TB（24 x 3 TB）
サイズ			
高さ x 幅 x 奥行	43 x 437 x 503 mm	89 x 437 x 648 mm	178 x 437 x 660 mm
重量	14.06 kg	26.30 kg	44.28 kg
形状	1 RU	2 RU	2 RU
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
動作温度	10 ～ 35 ℃	10 ～ 35 ℃	5 ～ 35 ℃
保管温度	-40 ～ 70 ℃	-40 ～ 70 ℃	-40 ～ 60 ℃
湿度	8 ～ 90%（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）

FortiSIEM 500F

FortiSIEM 2000F

FortiSIEM 3500F

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.co.jp/contact

お問い合わせ