

Security Fortify Application Defender

アプリケーションのセキュリティへの脅威を確認しましょう。Micro Focus® Security Fortify Application Defender は、ランタイムアプリケーション自己保護 (RASP) ソリューションです。自社製アプリケーションおよびサードパーティ製アプリケーションから生じるリスクを管理し、軽減します。アプリケーションの利用と不正使用について 1 箇所で視覚的に確認でき、ソフトウェア脆弱性の悪用やその他の不正行為に対してリアルタイムで保護を提供します。

製品概要

アプリケーションのソースコードを変更することなく、アプリケーションおよびそのユーザーのセキュリティ運用アクティビティに関して、企業全体について一貫性のあるレポートを作成する機能をアプリケーションに迅速に追加できます。カスタムログ解析ツールは不要です。Application Defender は Java および .NET アプリケーションのソフトウェア脆弱性の悪用をリアルタイムで正確に検出して、安全に防止し

ます。同時に、コード行の脆弱性の詳細を提供して迅速に修復します。アプリケーション自己保護ソリューションは、成熟した Security Fortify ランタイム技術をベースとしており、「サービス」としても「オンプレミス」でも利用できます。

Application Defender は、アプリケーションとユーザーのアクティビティログをキャプチャする機能をアプリケーションに迅速に追加します。また、SQL インジェクション

主な特長

- コードの編集や再コンパイルが不要な、アプリケーションアクティビティに関する一貫した体系的なログ記録
- 既知および未知の脆弱性から、ボタン 1 つをクリックするだけでリアルタイムで保護
- 業界標準のフォーマットに柔軟にイベントを出力し、任意の SIEM またはログ管理ソリューションで可視化、分析、アラート可能
- 完全に再構成された攻撃文字列とコード行の詳細によるイベント詳細に基づき、効率的にトリアージおよび修正
- 設定可能なアラートとレポートによる、組織全体でのリスクの優先度設定と伝達
- 成熟した実績あるランタイムアプリケーション自己保護 (RASP) テクノロジー
- Fortify on Demand のセキュリティテストでは、FoD を終了せずにボタン 1 つをクリックするだけで多数の脆弱性をシームレスに保護可能

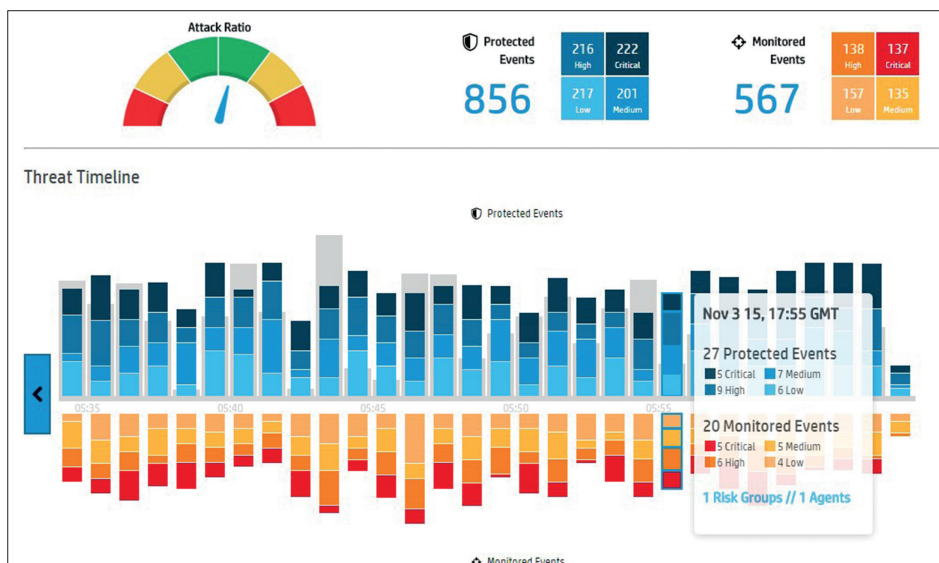


図 1 本番アプリケーションへの脅威を正確に特定し、即座に保護

(SQLi) やクロスサイトスクリプティングなど、多数の脆弱性カテゴリに対する攻撃を検出し、防止します。ログと悪用に関するデータが両方ともセキュリティ/情報/イベント管理 (SIEM) またはログ管理に提供されるため、コンプライアンスやアプリケーションセキュリティを包括的に確認することができます。アプリケーションデータフローと実行ロジックからコンテキストに基づいたインサイトを引き出すことで、悪意のあるクエリを完全に再構成された形で確認できます。これにより、Application Defender は、ネットワークベースのセキュリティでは防止できないような攻撃であっても、確実に特定して防止できます。

主な利点

可視性

- 本番アプリケーションでソフトウェア脆弱性の悪用を即座に検出し、実際の攻撃を継続的に監視して、保護または修復に必要な脆弱性を特定します。
- アプリケーションとそのユーザーのアクティビティを、一貫した方法で自動的に把握します。
- アプリケーションにログの作成機能がない場合でも、ログデータを SIEM またはログマネージャーに送信し、コンプライアンス、相関、可視化、分析、アラートに利用できます。
- 開発者向けのコード行詳細により、脆弱性を迅速に修正できます。

保護

- ソースを変更または再コンパイルすることなく、リアルタイムで、企業全体において既知および未知のアプリケーションセキュリティ脆弱性を検出して保護できます。
- ネットワークベースのセキュリティソリューションでは検出できない攻撃を防止します。
- 実際の攻撃と正当な要求とを正確に見分けます。
- 堅牢なカバレッジ範囲で見逃しのリスクを低減します。

- 自社製または商用アプリケーション、または基盤プラットフォームで、ゼロデイから保護します。

シンプルさ

- オンプレミスでも SaaS (software as a service) でも、希望の方法で導入できます。
- シンプルなインストールと、構成済みの脆弱性検出ルールで、わずか数分間でアプリケーションをすばやく容易に保護できます。
- Fortify on Demand (FoD) で検出された脆弱性は、ボタンをクリックするだけで対策できます。
- 効率的に管理、報告、拡張できます。

アプリケーション自己保護を使用する理由

- **アプリケーションの使用と不正使用に対する一元化されたカスタマイズ可能な情報表示**：アプリケーションを標的とするサイバー攻撃は止むことがなく、Security Operations Centre (SOC) がアプリケーションの動作と弱点を把握できないことがよくあります。Application Defender を使用すると、ログを作成するようにアプリケーションが開発されていなくても、アプリケーションに機能を追加できます。ソースコードを変更しなくても、ログや悪用の記録が SIEM やログマネージャーに送信されるため、状況が把握しやすくなります。
- **脆弱な自社製またはサードパーティ製アプリケーションの管理を軽減**：セキュリティチームの業務目標と予算は、アプリケーションセキュリティへの対処に移りつつあります。しかし、限定されたリソースと新たな脆弱性は、これからも変わらず課題となります。Application Defender を利用すると、アプリケーションのテスト中に予期されなかった新しい脆弱性が発生したり、既知の脆弱性が本番環境に移行したりしても、本番アプリケーションを即座に保護できます。この保護は、脆弱性が修正されるまで、あるいはレガシーアプリケーションまたはサードパーティ

製アプリケーションの場合は無期限に適用されます。管理の軽減が必要となるのは、次のようなケースです。

- 修復に必要なリソースや時間よりも脆弱性が多いアプリケーション
- 基盤の脆弱性を修正できない、サードパーティまたはレガシーのアプリケーション
- アプリケーションまたは基盤プラットフォームのゼロデイ脆弱性

- **シンプルな導入と使用**：Security Fortify Application Defender ソリューションにより、企業の規模を問わず、エージェントおよびアプリケーションセキュリティポリシーの適用、設定、管理が容易になります。実績のある Security Fortify ランタイム技術をアプリケーションのランタイム環境にインストールすることで、対象のアプリケーションをリアルタイムで監視して保護します。一元化された管理と分析で、追加のエージェントを任意の Java または .NET アプリケーション上に、迅速かつスケーラブルに導入できます。

- **多層防御**：ネットワークセキュリティが防御の重要な層であることは変わらない一方、署名ベースの防御は、フィルター、推論、統計を利用して既知の悪用行為を探します。たとえば、攻撃者は悪意のあるクエリのエンコーディングを変更して SQLi の脆弱性を悪用できます。ネットワークおよび境界の防御は、悪意のあるクエリを部分的にしか認識できません。

クエリ全体が構成されて完全に実行可能な形になるのは、アプリケーション内部だけです。Application Defender はアプリケーションプログラムのフローと使用の試行をリアルタイムで確認できるので、ユーザーによる要求を分析して、実際の攻撃と正当な要求とを見分け、アプリケーション自己保護ソリューションの精度を大幅に向上します。そして、攻撃に対して具体的に制御可能な措置が取られ、攻撃をリアルタイムで防止し、悪意のないアクティビティが影響を受けないようにします。

主な特長

- コードの編集や再コンパイルが不要な、アプリケーションアクティビティに関する一貫した系統的なログ記録
- 既知および未知の脆弱性から、ボタン1つをクリックするだけでリアルタイムで保護
- 業界標準のフォーマットに柔軟にイベントを出力し、任意のSIEMまたはログ管理ソリューションで可視化、分析、アラート可能
- 完全に再構成された攻撃文字列とコード行の詳細によるイベント詳細に基づき、効率的にトリアージおよび修正
- 設定可能なアラートとレポートによる、組織全体でのリスクの優先度設定と伝達
- 成熟した実績あるランタイムアプリケーション自己保護 (RASP) テクノロジー

- Fortify on Demand のセキュリティテストでは、FoD を終了せずにボタン1つをクリックするだけで多数の脆弱性をシームレスに保護可能

Security Fortify Application Defender を選ぶ理由

- アプリケーションセキュリティリーダーによる実績あるアプリケーション自己保護テクノロジー (Gartner MQ)
- ツールに統合されたエンドツーエンドのアプリケーションセキュリティ機能
- 業界をリードするセキュリティ調査に裏付けられた、包括的な脆弱性カテゴリ
- アプリケーション内から即座に利用できる、徹底的で正確な情報
- エージェントのポリシー管理 (ポリシーの実行がクラウド接続に依存しない)

- オンプレミスでもサービスとしても柔軟に導入可能

Security Fortify について

Security Fortify は、業界をリードするセキュリティ調査に基づき、ランタイムアプリケーションの監視および保護とともに、極めて包括的な静的および動的アプリケーションセキュリティテストテクノロジーを提供します。当ソリューションは社内にデプロイすることもサービスとしてデプロイすることもできるため、今日の IT 組織の進化するニーズを満たす、拡張性に優れた機敏なソフトウェアセキュリティ保証プログラムを構築できます。

詳細情報はこちら：

<https://software.microfocus.com/en-us/products/application-defender/overview>

お問い合わせ先：
www.microfocus.com

マイクロフォーカスエンタープライズ株式会社
jp-info-enterprise@microfocus.com
www.microfocus-enterprise.co.jp