

ケーススタディ

テクノロジー大手がカスタマーポータルをセキュリティ保護

● Virsecはグローバル顧客のセキュリティ、データプライバシー及び継続性を確保します

高度なサイバー攻撃の急増に伴い、このグローバルテクノロジーリーダーは自社のカスタマーポータルにおけるセキュリティギャップの可能性について心配していました。

このウェブベースのポータルは、世界中の数千の顧客に重要な製品情報及びサポートサービスを提供しています。

この顧客には、既にエンドポイント保護、WAF製品及びEDR製品、並びに自社のセキュリティ部門から入手できる数十のセキュリティ製品を含む、あらゆる種類の従来のセキュリティテクノロジーがありました。

それにも関わらず、この顧客は、自社のポータル保護には機密データ及び顧客情報を暴露する可能性がある重大なギャップがあると考えていました。

又、この顧客は、既存のセキュリティツールには、新規の脆弱性に後れを取らないようにするためにあまりにも多くのチューニング、ポリシー調整、及び面倒な工数が必要とされており、誤検知も多いと感じていました。

● 従来のツールをしのぐVirsecセキュリティプラットフォーム(VSP)

Virsecは、Java、Node.js、及びNginxウェブサーバを含むカスタマーポータルのフルアプリケーションスタックを保護するVirsecセキュリティプラットフォーム(VSP: Virsec Security Platform)を用いた詳細なPOCに参加しました。

このソリューションは、高度な攻撃からウェブレイヤ、メモレイヤ、及びホストレイヤを保護している間の効果、性能、及び有用性についてテストされました。

POCでは、既存のWAFソリューション、エンドポイントソリューション及びEDRソリューションを回避する広範囲の攻撃を検出・阻止することが分かりました。更にVirsecは、シグネチャ、学習、チューニング、又はポリシー更新を必要としない自動化されたアウトオブボックス検出により、管理がより容易であることも分かりました。

又、VSPは事前知識なしで”ゼロデイ攻撃を検出することができる”ので、この顧客は、Virsecがパッチ適用されていない脆弱性に対する補償制御及び効果的な形態の仮想パッチ適用が可能なることも分かりました。

● 結論

入念な評価の後、保護の深さ、自動化、及びフォールスポジティブ又は無関係なセキュリティアラートがないことを理由としてVSPが選定されました。

このソリューションは、ウェブアプリケーション、ウェブサーバ、サードパーティツール、及びホストシステムを含むカスタマーポータルのフルアプリケーションスタックにわたって100以上のアプリケーションインスタンスを保護するために展開されています。

「Virsecは、如何なるチューニング、微調整又は誤検知もなしに、私達がこれまで見たことがなかった攻撃を検出します。

このことは、私たちが重要な顧客データを保護するのに必要な自信を与えてくれます」

セキュリティアーキテクト  
大手企業

顧客のプロフィール

- ・ 半導体テクノロジー設計・製造の大手
- ・ インフラ、ネットワーク、ソフトウェア、及びセキュリティソリューションのリーダー
- ・ ウェブポータルによってサポートされるグローバル顧客基盤

※Virsecは、広範囲の回避的なサイバー攻撃(既知の攻撃及び未知の攻撃)に対して従来のソリューションとは異なるアプリケーションウェアなワークロード保護を提供し、内部からアプリケーションをセキュリティ保護します。Virsecは、カスタム、COTS、サードパーティ、レガシー、SCADAなどを含む全てのアプリケーションを保護します。また、Virsecソリューションは、オンプレミスサーバ、仮想、クラウド、ハイブリッド、コンテナ、及びエッジを含むあらゆるプラットフォームにわたって保護します。

● **主な課題**

**Virsecを使用する前には、このテクノロジー大手には複数のセキュリティ課題(下記)がありました。**

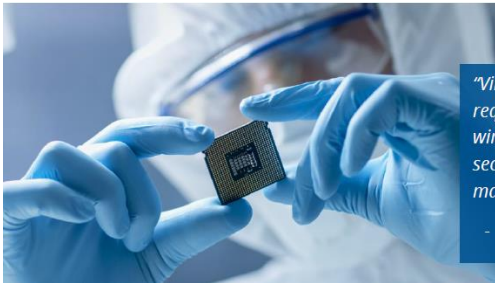
- ・グローバルカスタマーポータルアプリケーションの整合性及びデータプライバシーに対する懸念
- ・既存、又は従来のセキュリティツールにおけるセキュリティカバレッジのギャップ及びブラインドスポット
- ・あまりにも多くの異なるポイントソリューションがあり、各ソリューションには限定された範囲及び可視性しかない
- ・WAFソリューション及びEDRソリューションにおける多数のポリシー更新、チューニング、及び誤検知
- ・サイバーセキュリティの監視及び維持を支援するITリソース及びセキュリティスペシャリストが限られている
- ・脆弱性のパッチ適用に遅れないでいることが難しい

● **Virsecを用いたことによる決定的結果**

- ・ウェブレイヤ、メモレイヤ及びホストレイヤを含む“全てのアプリケーションスタック”を保護します
- ・自動化された展開及びアウトオブボックス保護により、数百のアプリの保護まで拡張可能です
- ・**EDRソリューション及びWAFソリューションを回避するメモリベースの攻撃、ファイルレスエクスプロイトを含む、既存のツールを回避する脅威を阻止します**
- ・チューニング、ポリシー更新又は誤検知の解析を不要にして管理時間を短縮します
- ・補償制御を提供して、“パッチが適用されていない場合でも脆弱性エクスプロイトを防止”します

**VSPは、以下の理由(業界初)により、この大手顧客によって選定・展開されました。**

- ・Javaアプリ、Node.js、及びNginxウェブサーバを含むポータルアプリケーションのフルスタックを保護します
- ・Nutanixプラットフォームと完全統合されました
- ・自動化された計装により、100以上のアプリケーションインスタンスに自動的に展開することができました
- ・シグネチャ、チューニング、学習、ポリシー更新又は人的介入なしに、高度な脅威に対するアウトオブボックス保護を提供します
- ・プロセスメモリの他に類を見ないランタイム可視性を実現して、メモリベースの脅威、ファイルレスマルウェア、及び未知の攻撃又はゼロデイ攻撃を防止します
- ・パッチのステータスに関わらず、脆弱性エクスプロイトに対する効果的な補償制御を提供します



**「Virsecは展開が容易で、カスタマイズが不要でした。これは私達にとってウインウインであり、以前のツールよりも少ない管理労力で、より良いセキュリティカバレッジを提供してくれます」**

ITセキュリティ担当ディレクター

● **Virsecは、従来のソリューションとは異なり(特許による)内部からフルアプリケーションスタックを保護します。**

実績の一部

Raytheon

AVEVA



Schneider Electric

"We're deploying Virsec in mission-critical areas and seeing very good success." - Julian Zottl, Cyber & Information Ops, Raytheon

● **Virsec Systems, Inc.(米国、サンノゼ)について**

Virsecは、巧妙化した攻撃、未知の攻撃及びゼロデイサイバー攻撃を決定的に防止するセキュリティソリューションを提供しています。

Virsecの高度なテクノロジーは、クリティカルアプリケーションに対する複雑で巧妙化した攻撃をほぼ100%の精度でリアルタイムに阻止する脅威検出のための画期的な決定論的手法を使用します。

**世界で最もクリティカルなアプリケーションをセキュリティ保護**

Virsecは世界中に展開されており、金融サービス、ヘルスケア、政府、防衛、電力、石油&ガス、輸送、電気通信、テクノロジーなどを含む業界におけるミッションクリティカルなアプリケーション及びインフラを保護しています。

Virsecのテクノロジーの詳細については、弊社までご連絡ください。

詳細については、www.virsec.comをご覧ください。

コーネットソリューションズ株式会社  
 Cornet Solutions (TEL) 03-5817-3655 (代)  
 www.cornet-solutions.co.jp