CUSTOMER CASE STUDY

高度なモバイル脅威対策で知的財産を保護する Samsung Research America

チェック・ポイントのマルチベクター・セキュリティでモバイル・デバイスを保護

SAMSUNG RESEARCH AMERICA

お客様概要

Samsung Research Americaは、個人および法人向けの革新的な電子機器の研究・開発に従事しているグローバル企業です。

課題

- マルウェア感染デバイスによるネットワーク・アクセス、データ・アクセスを防止する
- ネットワークでの感染拡大を防ぐ
- 1つのソリューションでiOS搭載デバイスとAndroid搭載デバイスの両方を保護する

解決策

- Mobile Threat Prevention
- AirWatch by VMwareのMDMとの統合
- SplunkのSIEMとの統合

利点

- iOS/Android搭載デバイスを100%保護
- 高いユーザ利用率を実現
- 管理作業を簡素化、IT担当者の負担を軽減

「Check Point Mobile Threat Preventionは、モバイル・デバイス向けのゼロデイ・マルウェア対策として最良の選択肢です。未知のマルウェア対策には、多層防御のセキュリティが最も大きな効果を発揮します。Check Point Mobile Threat Preventionに任せれば、知的財産の保護は万全です」

スティーブン・レンツ氏（CISSP、CIPP/US）
Samsung Research America、情報セキュリティ担当ディレクター

概要

マルチベクターの脅威対策で万全のセキュリティを実現

Samsung Research Americaは、Samsung Electronics Company（サムスン電子）の完全子会社です。Samsung製品の競争力を支える中核技術の研究開発を主な事業としています。米国シリコンバレーに本社を構え、北米地域の主要なテクノロジー・センターに複数の拠点を設けています。

ビジネス課題

社外で使用されるモバイル・デバイスの保護

業界有数の消費者向け電子機器メーカー、Samsung。将来を見据えた先進技術の開発に力を入れる同社は、競合他社の先を行く新製品を次々と市場投入しています。このような同社の先進性を支えているのは、膨大な特許技術、つまり知的財産です。人事、法務、研究開発の担当者は、製品開発計画など機密性の高い内部情報を日常的に取り扱っています。万一、情報漏洩が発生した場合には、市場における優位性を失い、収益の大幅低下を招くおそれがあります。このような重要情報の流出は、何としても避けなければなりません。

多くの企業と同様、Samsung Research Americaでも、スマートフォンやタブレット端末、私物のデバイスを業務に利用する社員が増えており、IT部門では、会社支給のデバイスを約800台、私物のデバイスを約400台サポートする必要に迫られています。Samsung Research Americaで情報セキュリティ担当ディレクターを務め、CISSPとCIPP/USの資格を持つスティーブン・レンツ（Steven Lentz）氏は、数年前のある時点で、モバイル・デバイスから機密情報が漏洩したら大変な事態を招きかねないと気付きました。

「社内のデスクトップPCやノートPC、サーバとは異なり、モバイル・デバイスはネットワーク・セキュリティ・ソリューションで保護されていません」とレンツ氏は自身の懸念を説明します。「特に社外で使用されるモバイル・デバイスは、社内ネットワークに侵入するための踏み台として悪用される可能性があります。残念ながら、既存のモバイル・ファイアウォールでは、電子メールやアプリケーション経由での侵入を防ぐことができません」

レンツ氏は、この問題の解決には2方向のアプローチが必要だと考えました。モバイル・デバイスからの情報漏洩を未然に防ぎ、さらにフィッシング・メールなどを利用した外部からの侵入を阻止するという両方向の対策です。同氏は、この2つの難しい要件を満たすソリューションを探し始めました。

まず重要なのは、マルウェア感染デバイスによる社内ネットワークへの接続をブロックし、業務アプリケーションや機密データへアクセスできないようにする機能です。また、ネットワークへの接続を許可されたクリーンなデバイスへの感染拡大を阻止する必要もあります。さらに、複数のモバイル・オペレーティング・システムへの対応や、すでに使用しているAirWatch by VMwareのモバイル・デバイス管理（MDM）ソリューションおよびSplunkのセキュリティ情報/セキュリティ・イベント管理（SIEM）プラットフォームとの統合に対応している点も条件に挙げました。モバイル脅威を完全に可視化し、セキュリティ・ポリシーを全社規模で自動的に実施するためには、各ソリューションとの統合が欠かせないからです。

「高度なモバイル脅威は、従来のアンチウイルス・ソリューションでは検出できません。そのため、多層防御の仕組みが必要となります。アプリケーション・ベースのマルウェア検出、エンタープライズ統合、ゼロデイのモバイル・マルウェアに対応したファイアウォールなどの重要機能で、複数の保護レイヤを構成する必要があるのです」（レンツ氏）

「チェック・ポイントからは、最新のマルウェアに関する情報がいち早く自動配信されます」

スティーブン・レンツ氏
（CISSP、CIPP/US）

解決策

新しい多層防御

レンツ氏のチームは、個人向け、企業向けを問わず、さまざまなアンチウイルス・ソリューションを検討しました。しかし、要件を満たす製品はなかなか見つかりません。そこで、同業他社のセキュリティ責任者に勧められた、高度な脅威対策ソリューションの検討を開始。その中に含まれていたのが、Check Point Mobile Threat Preventionでした。Check Point Mobile Threat Preventionは、エクスプロイトや標的型攻撃、モバイル・マルウェアに加え、スパイ活動やデータ窃取に使用される商用のリモート・アクセス型トロイの木馬（mRAT）に対する多層防御を実現する製品です。早速デモ導入したところ、複数のマルウェア感染デバイスが直ちに確認されました。アプリケーション・ベースのゼロデイ・マルウェアをはじめ、各種脅威への対応が確認され、Check Point Mobile Threat Preventionの導入が正式に決定しました。

「チェック・ポイントからは、最新のマルウェアに関する情報がいち早く自動配信されます。Check Point Mobile Threat Preventionは、モバイル・デバイス向けのゼロデイ対策として最も理想に近いソリューションです。期待どおり、また期待を上回る働きを見せてくれる製品はなかなかありません。私にとってCheck Point Mobile Threat Preventionは、まさにそのような製品です」（レンツ氏）

AirWatch by VMwareのMDMやSplunkのSIEMプラットフォームともシームレスに統合可能なCheck Point Mobile Threat Preventionを導入した レンツ氏は、モバイル脅威の完全な可視化と、セキュリティ・ポリシーの全社規模での自動的な実施を実現しています。

効果的な保護機能

Check Point Mobile Threat Preventionは、フィッシング・メールやテキスト・メッセージ、Webブラウザ経由で侵入を試みるセキュリティ脅威に、デバイス・レベル、アプリケーション・レベル、ネットワーク・レベルで対処します。デバイス、アプリケーション、ネットワークに関する情報をクラウドで相関分析し、リアルタイムの脅威情報を配信。データのないモバイル・アプリについては、サンドボックス環境で実行して不審な活動の有無を確認します。データを実際に検査することなく、ネットワークの通信リンクで高度なコード解析を実施することが可能です。アプリケーションの振る舞いのヒューリスティック分析により、root化やJailbreakにも対応。ユーザがダウンロードしたファイルが、Check Point Mobile Threat Preventionによってマルウェアと判断された場合には、MDMシステムに通知して、デバイスの隔離、セキュリティ・プロファイルの削除、社内ネットワークへのアクセス禁止などの措置を実行させることができます。

短時間で容易に導入

Check Point Mobile Threat Preventionは、容易に導入することができます。「わずか3週間で完了しました。Check Point Mobile Threat Preventionをネットワークに展開し、既存のMDMを使用して各デバイスで有効化するだけです。日常的な運用管理も簡単です」とレンツ氏は述べています。

「Check Point Mobile Threat Preventionの貢献度は、優に正社員1人分に匹敵します。その分、他の作業に人員を振り分けられるようになりました」

スティーブン・レンツ氏
（CISSP、CIPP/US）

ビジネスにもたらすメリット

導入直後から効果を発揮

Check Point Mobile Threat Preventionは、導入初日から社員の私物デバイスに3個のマルウェアを発見し、その後さらに20種類以上のマルウェアを検出しました。Check Point Mobile Threat Preventionは、新たなマルウェアが見つかると、すぐさま管理者に通知し、MDMと連携して問題のデバイスを社内ネットワークから隔離します。マルウェアが駆除されるまで、社内ネットワークや社内資産へのアクセスは許可されません。

本格運用の開始後には、業務に利用しているデバイスの5%に何らかのマルウェアが見つかりました。認証情報を窃取するマルウェア、キー入力内容を記録するキーロガー、前述のmRAT、無許可のroot化ツールなどです。デバイスでマルウェアが検出された場合、そのユーザに通知が行われ、マルウェアが駆除されるまで、デバイスはネットワークや資産から隔離されます。

「Check Point Mobile Threat Preventionは、iOSとAndroidに両対応しており、現在のところすべてのデバイスの保護が実現しています。それも自動的に保護される点が重要です。モバイル・ユーザを常時監視して、問題発生時に手作業でデバイスを復旧するのは現実的ではありませんからね。マルウェアに感染したデバイスが即座に隔離されるCheck Point Mobile Threat Preventionなら、被害の拡大を効果的に防止できます」（レンツ氏）

高いユーザ利用率

新しいソフトウェアの導入は社員に告知されましたが、社員は何か特別な操作を要請されたわけではありません。Check Point Mobile Threat Preventionは、AirWatch by VMwareのMDMによって分離されたモバイル・デバイス上の業務データと個人データの両方を保護します。わずかなシステム・リソースのみを使用してバックグラウンドで動作するため、ユーザが新しい操作を習得する必要は一切ありません。デバイスが隔離された場合にメッセージが表示されるだけです。

「透過的に動作するCheck Point Mobile Threat Preventionは、社員の負担が最小限で済みます。ソフトウェアは簡単に登録可能で、プライバシーも守られます。そのうえ作業の邪魔をせずバックグラウンドで動作するため、多くの社員に好意的に受け入れられています」（レンツ氏）

モバイル脅威を可視化

脅威情報をSplunkのSIEMと統合できるCheck Point Mobile Threat Preventionでは、モバイル・デバイスのセキュリティ・ポリシーの遵守状況を正確に把握できます。このため、セキュリティ管理を効率化しつつ、セキュリティ脅威への予防的な対処を実現できます。さらに、クラウド型のダッシュボードでリアルタイムの脅威情報を参照し、ネットワークへの侵入を試みるモバイル脅威の数や種別を確認できます。

「AirWatch by VMwareのMDMやSplunkのSIEMとも統合され、リアルタイムで自動的にセキュリティ脅威に対処できます。隔離機能によって、セキュリティ脅威がネットワークにアクセスできなくなるので、機密情報の保護も一層強固になります」（レンツ氏）

Check Point Mobile Threat Preventionは、メンテナンスの手間が最小限に抑えられる点も評価されています。必要な作業は週あたり1時間程度で済みます。モバイル・デバイスでマルウェアが検出された場合に、ユーザからの応答を待機してマルウェアを駆除するのが主な作業です。それ以外の時間、Check Point Mobile Threat Preventionはバックグラウンドで動作し続け、モバイル・デバイスを静かに保護します。

「Check Point Mobile Threat Preventionの貢献度は、優に正社員1人分に匹敵します。その分、他の作業に人員を振り分けられるようになりました」（レンツ氏）

強固なセキュリティの下でモバイル・デバイスを有効活用

Check Point Mobile Threat Preventionは、数多くのマルウェアを確実に（誤検出なしで）検出できることが実証されています。この結果、Samsung Research Americaでは、セキュリティ問題を懸念することなく、私物デバイスによる社内ネットワークへのアクセスを社員に許可できるようになりました。社員が私物のモバイル・デバイスを業務に使い始める際は、Check Point Mobile Threat Preventionをインストールして、マルウェアや不正なアプリの有無を確認していますが、デバイスではその後も、毎日のように、不正なリンクやダウンロード、アプリケーション経由で侵入を試みるマルウェアが検出されています。

不安を払拭するCheck Point Mobile Threat Prevention

業務データや知的財産を保護する多層防御のプロアクティブなセキュリティを実現したレンツ氏は、同業他社にもCheck Point Mobile Threat Preventionの導入を勧めています。

「Check Point Mobile Threat Preventionは、モバイル・デバイス向けのゼロデイ・マルウェア対策として最良の選択肢です」とレンツ氏は話します。「未知のマルウェア対策には、多層防御のセキュリティが最も大きな効果を発揮します。Check Point Mobile Threat Preventionに任せれば、知的財産の保護は万全です」

詳細については、次のWebサイトをご覧ください。
http://www.checkpoint.co.jp/products/mobile-threat-prevention/

製品に関するお問い合わせ

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社

〒160-0022　東京都新宿区新宿5-5-3　建成新宿ビル6F　Tel：03（5367）2500　E-mail：info_jp@checkpoint.com　http://www.checkpoint.co.jp

P/N EOB46E0 2016.7