Bromium　ユーザ事例　Ⅱ

ADP 会社の概要

業界
世界的規模の給与支払い名簿、税金、人事サービスのプロバイダ

環境
全世界の従業員は 55,000 人

解決策
Bromium® Advanced Endpoint Security

課題
セキュリティの体制を「受け身的な対応」から「予防」に変え、エンドポイント攻撃にさらされる全体的な面を減らす。

利点
- 独自の CPU 機能を使った隔離によって、攻撃面の全体が劇的に減り、OS から独立した高度な防御が実現した
- 詳細な脅威分析ができるため、攻撃を詳しく見ることができ、それを使ってよりタイミングよく環境を保護することができるようになった
- インシデント対応のコストが削減でき、セキュリティ工程が簡略化され、予算を他の投資に向けることができる
- ユーザにとって完全に切れ目のない迅速かつ効率の良い企業規模への展開

ADP：防御から防止へ
1949 年に設立された ADP は、世界有数の人材管理サービス会社の 1 つです。ADP の核となるソリューションには、給与支払い名簿、人事および福祉に加え、人材管理や報酬、データ分析のための高度なツールなどがあります。
2015 年には、ADP は米国内だけでも 2,400 万人の労働者の給与支払い名簿を管理しました。クライアントの税金、自動振り込み、関連の資金など、1 兆 7,000 億ドルを電子的に動かし、およそ 5,600 万もの源泉徴収票書類を処理しました。ADP は、フォーチュン誌の「世界で最も称賛される企業 2015」でトップクラスに入る金融データサービスの会社です。

課題：複雑で高度な攻撃から顧客の資産を守る
ADP のセキュリティ最高責任者（CSO）である Roland Cloutier 氏は、セキュリティマガジン誌で、「セキュリティ部門で最も影響のある人物」と認定されていますが、モバイルやクラウド、高度なサイバー攻撃が盛んなこの時代において企業のセキュリティ担当部門が直面している課題を明確に理解しています。Cloutier 氏の主な使命は、ADP の社内インフラストラクチャと複雑な世界規模のクラウドポータルを防御することであり、8,000 万人、700,000 社によってアクセスを受けています。

ADP における自分の第一の責務は、顧客に安全なサービスを提供することで、結果的にはそれがすべての人にとってビジネスを成功に導くことになると彼は思っています。昨今のように急速に変化する複雑な脅威が多い環境に照らしてみて、Cloutier 氏は 2 つの事を考えると夜も眠れなくなるといいます。大きな関心事の 1 つが、「企業全体と私どものお客様のプラットフォームを通して、真の可視化と透明性を実現し、正しい防御法を手に入れることです」さらに Cloutier 氏は、実際に間違いが起きたときには、セキュリティ事象に対応できる能力を備えておきたいとも思っています。彼の関心事の 2 つ目は、セキュリティの保証を真の意味で提供するということです。「私は、自分たちの制御の効果と、自分たちが環境全体を通じて安定した防御を行える範囲について、自信を持たねばなりません」とセキュリティ最高責任者である彼は言いました。

こうした問題を考えて Cloutier 氏は、対処ではなく予防に焦点を移した「まず防御を」という方策を採り入れることにしました。Cloutier 氏の目標の 1 つは、自社が攻撃にさらされる面を少なくすることで、そのために彼はエンドポイントに注意を向けました。「問題はもはやウェブ上のやり取りやブラウザだけの事ではありません。毎日届く大量の電子メールに加え、流れてくる決まった形のないデータにも対応する必要がありました」Cloutier 氏は、オペレーティングシステム（OS）独立型で使いやすさの度合いが高いエンドポイントのセキュリティソリューションを必要としていました。

ADP は、Bromium のマイクロ仮想化技術と分析を利用

Cloutier 氏は、管理上の必要性や定期的なセキュリティソフトウェアの更新に伴う費用、ADP がサポートするインフラストラクチャなどのために、エージェントベースのセキュリティソフトウェアでユーザのエンドポイント使用の邪魔をすることはよくないと強く感じていました。彼が Bromium の Advanced Endpoint Security を選んだのは、その独自のマイクロ仮想化の技術のためでした。これは、マイクロ仮想マシン（Micro-VM）でタスクをオペレーティングシステムから切り離し、操作が完了するとそのタスクを破棄するようになっています。

「最終的に私たちは、継続的な OS の防御を行うことができる唯一の技術は Micro-VM であるとわかりました。Micro-VM で残りの PC 環境から隔離することができるからです」と Cloutier 氏はきっぱりと言っています。Bromium は ADP がエンドポイントの攻撃を受けやすい面を大幅に減らすことができる OS 独立型のソリューションを提供すると共に、Bromium Threat Analysis を使った分析で Micro-VM の内部に潜んでいるマルウェアも詳細に見ることができるようにしたのです。

トップダウンの導入

Bromium の技術専門家たちは、Cloutier 氏の部下たちとチームを組み、世界的規模で存在する ADP のエンドポイント全体を通して、よく協力し合って導入作業を行いました。Cloutier 氏によれば、「Bromium は、段階を踏んだ導入の計画を私たちに約束してくれ、とてもいい仕事をしてくれました。よく練られた計画で、それで弾みがついたので計画を進めることができたのです」このようなトップダウンの会社主導型業務は、集中的なサービスを生むことになり、そのため ADP は、エンドユーザへの影響を最小限に抑えながら、何千ものエンドポイントすべてに Bromium をすぐに、そして効率よく導入することができたのです。

導入の間に、Bromium の技術は ADP の定評あるプラットフォームセキュリティインフラストラクチャにも直接統合されました。つまり、Bromium の脅威情報をサードパーティーの防御ソフトウェアで使う事ができました。「ADP にあっては、データは代名詞とも言えるのです。脅威情報があれば、判断を下したり戦略のロードマップを作成したりするのに役立ちます。Bromium によって手に入るようになった情報は、当社のインフラストラクチャに取り込まれ、私たちの環境でどのように攻撃が発生するかということを、それが起きた時点で直接見ることができるようにしてくれるのです」
Cloutier 氏は、Bromium Threat Analysis によってもたらされた独自の可視化機能を非常に賞賛しています。これによって、クリックからダイナミックリンクライブラリ（DLL）に至るまでのすべてに関する詳細なデータを見ることができるからです。「Bromium のおかげで、組織全体のリソースを利用するために必要とするものがすべて手に入り、受け身の防御態勢が変わったので、もっと積極的に防御に注力することができるようになりました」と、Cloutier 氏は言っています。

ビジネスマンとして考える

ADP のセキュリティ最高責任者（ＣＳＯ）の Roland Cloutier 氏は、すべてのＣＳＯはビジネスマンの視点でセキュリティを考えるべきだと思っています。「セキュリティに関する全所有経費を目に見えて最も大きく削減できるのは、他の技術に置き換えられ、インシデント対応のコストを減らし、工程を簡略化することができる製品です」ADP にとって、Bromium のソリューションはそういうものでした。Bromium は、同社の「まず防御を」という考え方にぴったり合っています。「まず防御を行えば」、Cloutier 氏は言います。「対処する必要はなくなります。最終的に、組織が脅威を探し出すといったような他のことに注力するための時間を与えることになるのです。調査のスピードも上がり、環境を守るための脅威分析も、さらにタイミングよく実施することができるようになります。これは大きな功績ですよ。」全体的なコストダウンによって、ADP は他の新しい技術にその資金を振り向けることができるようになりました。
「Bromium は、私たちが組織全体でリソースを利用し、もっと積極的で予防に注力できるように受け身的な態度を変えるために必要なすべてのものを与えてくれました」

「まず防御を行えば対処する必要はなくなります。最終的に、組織が脅威を探し出すといったような他のことに注力するための時間を与えることになるのです。Bromium のおかげで調査のスピードも上がり、環境を守るための脅威分析も、さらにタイミングよく実施することができるようになります。これは大きな功績です」

以上