Bromium　ユーザ事例　I

Mosaic 会社の概要

業界
世界的に有名な穀物用濃縮肥料の生産メーカー

環境
全世界の従業員数は 9,000 人
Microsoft Windows のエンドポイントは 6,000 か所

解決策
Bromium® Advanced Endpoint Security

課題
現在使っている従来のセキュリティ技術よりも更に効果的なソリューションを使って、エンドポイントのリスクを軽減し、全体的なセキュリティ体制を向上させる。

利点
- CPU レベルでの仮想化によって、システムのセキュリティが保たれ、企業ネットワークへのマルウェア拡散が防げる
- 導入や構成が簡単なので、セキュリティギャップがなくなる
- ランサムウェアを駆逐し、問題がないものにできる

Mosaic：Bromium の完璧なエンドポイントセキュリティによってリスクへの対策が向上

Mosaic は、 6か国におよそ 9,000 人の社員を抱える濃縮リン酸塩と炭酸カリウムの大手生産会社であり、販売会社でもあります。同社はフロリダ州中部にある自社所有の約 200,000 エーカーの土地にあるリン酸塩鉱山からリン酸塩を採掘し、北米、主にサスカチュワンにある 4 つの鉱山から炭酸カリウムを採掘しています。Mosaic の生産物は作物用肥料に加工され、全世界の主要な農業地帯にいる顧客へと出荷されます。

課題：従来のセキュリティでは、昨今のゼロディ攻撃や標的型攻撃に対抗するにはあまり効果がない

Mosaic 社のセキュリティ、リスクおよびコンプライアンス担当責任者である Paul Hershberger 氏の業務は、コンピュータ環境を最新のものにし、エンドポイントセキュリティを最適化することで、同社の全体的なリスク対策を向上させることです。彼の部署は定期的に、同様の業界にある会社ならどこでも直面するような、進化した攻撃と戦っています。すなわち、国家の支援を受けた攻撃者、ハッキング行為者、外部のサイバー犯罪者、社内の攻撃者など、4 種類の悪意ある行為者によって行われる攻撃です。Hershberger 氏は、Mosaic の既存のセキュリティインフラストラクチャに対して徹底的なリスク評価を敢行し、エンドポイントセキュリティから着手しました。当時、Mosaic は既に伝統的と言える多層に渡る脅威軽減技術から構成される複数のベンダーの製品で構成されていました。すなわち侵入検知システム（IDS）、侵入防止システム（IPS）、ウェブと電子メールのフィルタ、デスクトップのファイアウォール、アンチウィルス、アンチマルウェア、アンチスパムなどです。評価後、Hershberger 氏は、もっと効果的なエンドポイントセキュリティを探し始め、チャネルパートナーから、Bromium の独自の手法を紹介されたのです。

Hershberger 氏のチームは、保護されたラップトップやデスクトップ、携帯デバイス上の「残存リスク」（リスクを特定して排除するように設計されたセキュリティ制御が導入された後も残っている脅威）を特定することによって、そのようなリスクを統制するために現在持っているすべてのソリューションを考慮して評価を開始しました。「そこで達した結論は、私たちが長い時間と労力と費用をかけてきたエンドポイントソリューションは、リスクに対してほんの些細で取るに足りない効果しか与えていなかったということでした。自分たちのソリューションや制御をすべて評価した後でわかったことは、残存リスクがもともとのリスクよりほんのわずか減っただけだということなのです」と Hershberger 氏は説明しています。「私たちが行ってきたことは、基本的には無駄でした。そこで、リスクを真の意味で大幅に減らしてくれる道を探し始め、そんなときに Bromium に出会ったのです」

Bromium の CPU 機能のセキュリティが侵害をなくす

Bromium を選ぶ前に、Hershberger 氏とそのチームは、幅広いエンドポイントソリューションを多数評価しましたが、最終的には簡単で完璧な Bromium のソリューションが勝利を収めたのでした。

チームのメンバーは、他のエンドポイントセキュリティソリューションの動作方法を見たときに、手順がたくさんありすぎて、間違ってしまう可能性が高いと感じたそうです。「こうしたソリューションはたいてい、構成の選択肢をたくさん提示しているので、その構成のしかたによって、効果と、セキュリティに対する誤った認識との間に差ができてしまいかねません」Hershberger 氏は言います。「異なるツールセットの中で食い違いが発生する可能性を調べている際に、Bromium が単純でありながら完全な手法を編み出していて、セキュリティに関する誤った安心感、食い違いを生じさせないような保護の方法を幅広いレベルで提供してくれることがわかったのです。他のソリューションは、保護/検出時に何も応答しないことがあまりに頻繁に起こるのに対し、Bromium ではそれが当てはまりません」

Hershberger 氏と彼が率いるチームは、デバイス上の CPU による強化された安全なマイクロ仮想マシン（Micro-VM）でユーザのタスクを切り離す Bromium のやり方が効率向上に貢献しているとしています。彼が指摘する通り、セキュリティ製品の中にはある程度仮想化技術を組み込んでいるものがあり、例えばその場で分析を行う仮想マシン（VM）を起動する、サンドボックスでマルウェアを実際に実行する、などして分析システムを通じてそれを送付するというようになっています。ところが、Bromium はそれ以上の技術を駆使しています。「Bromium の技術は実に健全です。私が気に入っているのは、これが CPU とハードウェアレイヤでのテクノロジー・スタックを介して仮想化を利用している唯一のソリューションであるということです」Hershberger 氏はこのように言い切っています。

初期展開の成功

2015 年初めに最初に導入されたとき、Bromium の展開は 2000 ものエンドポイントに及びました。Hershberger 氏は、この技術導入について次のように述べています。「単純でわかりやすい。そして、Bromium のコンサルタントとの共同作業は、素晴らしいの一言でした」

Bromium をシステムにインストールしている Mosaic のユーザは、生産性を落とさずに新たな保護が加えられることが気に入っています。ユーザたちは、「何の制限もなく、何も気にせずにあらゆるものをクリックできる自由」を謳歌していると Hershberger 氏は言うのです。
Bromium Advanced Endpoint Security を単なる保護ツールとして使うほかに、Mosaic のセキュリティ担当チームは、Bromium Threat Analysis モジュールと合わせて、調査と分析のツールとしてすぐにこれを使い始めました。「私たちの環境には、多くの疑わしいコードやファイルが入ってくる上に、それが実際にどのようなものか普通はわかりません。以前はこうした疑わしいものを隔離された診断環境に注意深く移動しなければなりませんでした。Bromium があれば、すぐさまデスクトップ上でその処理を開始することができるのです」Hershberger 氏は言います。「チームの人間が、安全に、かつ自信を持って自分のデスクトップですぐに疑わしいコードを見つけ、どのようにそれを処理するかその場で判断できるというのは、開放的な気分ですね」

Bromium はランサムウェアを駆逐する

コンピュータやそのファイルをロックダウンし、お金を払わなければアクセスできないようにするのがランサムウェアですが、Hershberger 氏は、Mosaic ではこの脅威が増えてきていることに気づきました。彼のチームは数か月間連続で、ランサムウェアの事象をいくつか検出しており、それは非常にとらえにくく、しかも破壊力が強いうえに、アンチウィルスソリューションやその他の防御手段による検知をすり抜けるものであることがわかっています。Hershberger 氏は、ランサムウェアの根源は通常、一般にアクセスされる人気の高いウェブサイトであることを突き止めました。
Bromium を Mosaic 環境でしばらく実行した後、Hershberger 氏とそのチームは、自社に従来あった予防手段に比べて、Bromium がどれほどランサムウェアに対して高い防御能力を発揮するかということがわかりました。ユーザと IT サポートスタッフに対して実験を行い、生産性、ファイルの消失、ホストの再イメージ化などの点について、保護されていないホストとされているホストとの間で違いを比べてみました。その結果は？ 「Bromium が有効でした」と、Hershberger 氏は言っています。

Bromium の実績を広げる

人目につかない高度な脅威と、ユーザの中にそれが広まりつつある問題に直面した際の Bromium の効用について全幅の信頼を置いた Hershberger 氏は今年、全世界規模ですべての PC に Bromium を導入する計画を立てています。Bromium を採用することによって、Mosaic は古いシステムを必要に応じて最新の安全な、ハイブリッドのエンドポイント環境の仮想デスクトップや物理システムへ交換する作業に踏み切るきっかけができました。「Bromium は、セキュリティを本当に劇的に変化させる能力を持っています」と Hershberger 氏は言っています。

以上