CrowdStrike 導入事例

マクセル株式会社

自社を主軸とした運用体制で、マクセルグループは4,400台のエンドポイントをCrowdStrike Falconで保護

コロナ禍で一変したエンドポイント保護委託先でのインシデントも発生

マクセル株式会社は、1961年、日東電工株式会社の乾電池、磁気テープ事業部門が独立して誕生した製造事業社だ。これらの製品でマクセルブランドは一世を風靡した。

祖業で築き上げた“技”は、今もアナログコア技術として活きる。これは、アナログとデジタルをつなぎ、さらにデジタル技術だけでは到達しえない、複雑で繊細な領域のモノづくりを意味する。特に、素材を均一に混ぜ合わせる技術、粘着剤や塗料を均一に塗る技術、超精密な金型づくりや精密成形といった固める技術は、他の追随を許さない。これらが、エネルギー、機能性部材料、光学・システム、ライフソリューションとさらに広がった同社の事業セグメントの中で脈々と受け継がれ、社会の課題解決に貢献している。

同社の情報システム部では、グループ会社であるマクセルフロンティア株式会社、マクセルクレハ株式会社と合わせ、オフィス環境に配置された約4,000台のエンドポイント端末をサポートしている。

これまで防御策としては、アンチウイルスソフトを主な施策としてきた。過去にはEDRの紹介を受けたこともあったが、その時はEDRの必要性を認識できていなかった。

しかし、ワークライフバランス重視で働き方が変わり始めていたところへ新型コロナウイルスの感染が拡大。一斉テレワークシフトで多くの社員がオフィスの外で働くようになった。会社のエンドポイント端末を自宅で利用できるよう特別許可を出し、新たに整備しなおしたVPNでオフィス内システムへアクセスできるようにした。

さらに2020年のEmotetの被害拡大のニュースから社内の認識が変わっていった。そして実際にヒヤリハット事件も起きた。2021年に、業務委託先に貸与していたエンドポイント端末が、ランサムウェアに感染してしまった事件だ。この端末は、グローバルIPアドレスが外部から閲覧できる状態だった。アンチウイルスソフトはマルウェアの侵入を検知して止めたのだが、攻撃者が残っていたのだろう、その後アンチウイルスソフトがアンインストールされ、それ以降の侵入状況が分からなかったのだ。幸い削除されたことにいち早く気づけたため実害はなかったが、サイバー攻撃が凶悪化していることを実感した一件だった。

マクセル株式会社　情報システム部　情報セキュリティ課 課長 古原健二氏は、次のように語る。

「2020年当時、『次はゼロトラストアーキテクチャ』という方向性が見えてきました。その中で思い至ったのが、まっさきに強化すべきポイントはエンドポイント端末だということです。実際にインシデントも起こっていたため、水際対策だけではなく、もう侵入される前提で、検知して被害を最小限に食い止める施策への転換が必要でした。」

既存のアンチウイルスソフトにも課題を感じていた。スキャンが走ると端末リソースを消費し、常々エンドユーザーからは不満の声がもれていた。また、これはオンプレミスシステムであり、シグネチャアップデートが必要、バージョンアップ時には社内ネットワークの帯域を占領した。そして何より、社内ネットワークでの利用を前提としていたため、テレワークなどの利用では端末がリアルタイムに保護されない。これを同社は問題視した。

運用体制を重視しCrowdStrike Falconを選択

エンドポイント端末で行われているふるまいを検知し、何か異常があればただちに対処する。この機能を有したEDR製品の必要性を感じた古原氏は、選定に当たっていくつかの要件を掲げた。

1. 動作が軽量であること：エンドユーザーに不満を抱かれないよう、動作は軽量であるほど好ましい。
2. クラウドベースであること：エンドユーザーが

業種
電気機器

所在地
京都府乙訓郡大山崎町大山崎小泉1

マクセル株式会社

1961年の創業以来、独自のアナログコア技術である「混合分散」「精密塗布」「高精度成形」をベースに、画期的で高付加価値の製品を世に提供し、人びとの暮らしにさまざまな感動を生み出してきた。ミッションは「独創技術のイノベーション追求を通じて持続可能な社会に貢献する」。今、2030年に向けて「ヘルスケア」「5G/IoT」「モビリティ」分野で技術革新を担うべく、さまざまな社会課題と向き合うことで、より大きな社会的貢献を果たしていくことをめざしている。

URL：https://www.maxell.co.jp/

導入製品

- CrowdStrike Falcon Prevent™ NGAV（次世代アンチウイルス）
- CrowdStrike Falcon Insight™ EDR
- CrowdStrike Falcon OverWatch™ プロアクティブな脅威ハンティング

導入時期：2021年12月

社内・社外どこで働いていても、クラウドベースなら常時保護が可能。

3.バージョンアップ負荷が低い：バージョンアップのたびに時間や工数がかかるようでは運用負担が大きすぎる。

4.過検知が少ない：異常へのすばやい対処のため、ある程度の自社運用は必要。しかし負担がかかりすぎるなら、他の業務に支障をきたす。

5.高い防御力：実績での判断。たとえば昨年来、活動を再開したEmotetは完全に止めることができたか。

6.Windows、Mac、Linuxの3OS対応：台数は少ないがデザイン部門でMacが使われており、Linuxはサーバで40台以上存在。

こうした観点で検討を進め、3つのサービスを候補に上げた。それぞれ同じだけ時間をかけてPoCを行ったところ、3サービスとも上記の要件を満たしたという。それでは最終的にどれを選ぶか。ここで定期的にEメール訓練を依頼し、2021年のインシデント調査にも携わったセキュリティパートナーの存在が重要な決め手となった。

焦点を当てたのは運用体制である。本番導入後、同社で運用をリードするのは古原氏だった。ただ、昨今のサイバー攻撃は凶悪化している。背後でサポートするセキュリティ専門家の目も必要で、そのサポート役をセキュリティパートナーに託した。外部に“丸投げ”にもならず、マクセルに運用負担がかかりすぎない、同社を主とし、セキュリティパートナーを従とする理想な形での体制構築。それを実現できるのがCrowdStrike Falconだった。

「自社の環境を守ろうというのですから、ここは人に任せるわけにはいきません。自社運用は絶対に必要だと考えていました。自分達も使いやすい、またセキュリティパートナーもCrowdStrike Falconに精通していることから安心して選択することができました。またパートナー側より、運用のベースとしてどの製品を選択するかは、現在の脅威だけではなく将来にも関わるとクラウドストライクを推薦されました。」

そう古原氏は語る。導入製品として選んだのは、EDR機能であるCrowdStrike Falcon Insight、次世代アンチウイルス CrowdStrike Falcon Prevent、プロアクティブな脅威ハンティングをセキュリティ専門家が提供するCrowdStrike Falcon OverWatchという3モジュール。Falcon OverWatchを含めたのは、専門家中の専門家といえるクラウドストライクの脅威ハンターから、“マクセルにこういう攻撃が来ている”といった情報をいち早く得られることを期待したからだ。

異常なふるまいを見せていた仮想通貨マイニングツール

導入を正式に決定したのは2021年8月末。翌9月より、まずPC3,000台をターゲットにエージェントインストールを開始した。

現在はさらに導入が進み、マクセル、マクセルフロンティア、マクセルクレハ合わせて、PC4,100台、サーバ250台でCrowdStrike Falconが稼働する。古原氏は日々、一時間ほどかけてダッシュボードを精査する。気にかかる事象があればセキュリティパートナーに調査を依頼、必要があればエンドユーザーへの問い合わせを行う。

CrowdStrike Falconの導入によって、エンドユーザーがどこで働いていようとも、途切れることなくエンドポイント端末をモニタリングできる体制が整った。報道で幾度となく取り上げられたEmotetも、マクセルにおいてはインシデントとして上がったことはない。

また、想定していなかった事象も見つかった。あるPCにふるまい異常が検知されたため、パートナーに調査を依頼。その結果、返ってきたのは、仮想通貨のマイニングツールが動いているという報告だった。そのPCのユーザーに問い合わせてみると、Webブラウザのアドインツールは入れたが、それが仮想通貨のマイニングに使われているとは認識していなかった。悪事を働くウイルスではないが、今が油断もすきもない時代であることを物語る一件だ。

2022年5月、香港のグループ会社がエンドポイント端末強化を望み、60台のPCにCrowdStrike Falconを導入した。今後の計画として、マクセルイズミ株式会社への導入も決定している。

今後同社では、日常運用の簡素化、そしてさらなるゼロトラストアーキテクチャの推進に向けて動きを速める。前者では、ダッシュボードを見る時間をもう少し軽減したいそうだ。High、Medium、Lowという三段階のリスクレベルをどう扱うか、セキュリティパートナーとあらためて精査する時期に来ている、と古原氏は語る。

ゼロトラストアーキテクチャという観点では、クラウドの広がりが予想される中、“なりすまし”を防ぐために認証基盤の強化をすべく、近々具体的な実現方法の検討に入るとのこと。マクセルグループは次の段階を迎えた企業情報セキュリティに、どこまでもキャッチアップを続けていく。

マクセル株式会社
情報システム部 情報セキュリティ課 課長
古原 健二 氏

POINT

- 過去に見送ったEDR導入だが、状況の変化から施策を転換
- AVソフトをアンインストールする攻撃に遭い、侵入前提の施策の必要性を実感
- どの製品を選択するかは、現在の脅威だけではなく将来にも関わるとクラウドストライクを推薦したパートナーの存在
- CrowdStrike Falconがこっそりインストールされた仮想通貨マイニングツールも発見

CROWDSTRIKE

we stop breaches

クラウドストライク 株式会社
お問い合わせ: crowdstrike.jp/request-information/