ーお客様導入事例ー

NETWORLD

株式会社グラファー

Graffer

所在地：東京都渋谷区千駄ヶ谷1-5-8
ＵＲＬ：https://graffer.jp/

全社員のエンドポイント保護に CrowdStrike Falcon プラットフォーム を活用 リモートでも安全に働ける環境を実現

[BEFORE]
◆内部への侵入を前提としたエンドポイント対策を行いたい
◆検知したアラートへの対応に掛かる運用管理負荷を軽減したい

[AFTER]
◆脅威の防御から侵入後の検知・対応まで網羅的にカバーできる環境を実現
◆MDRサービスの導入により、効率的なセキュリティ運用を実現

持ち前の知見と技術力で行政DXや生成AI活用を支援

業種・業態の別を問わず、今やあらゆる組織で進められているデジタル変革。持ち前の技術力や知見を活かし、こうした取り組みを支援する新たな企業も次々と登場している。

「プロダクトの力で 行動を変え 社会を変える」をミッションとして掲げるグラファーも、そうした企業の一社だ。同社では、行政のデジタル変革を実現する行政DXソリューション「Graffer Platform」と、企業のビジネス変革を実現する生成AIソリューション「Graffer AI Solution」の二本柱で事業を展開している。

まず前者では、市民や行政職員の利便性を高める「Graffer スマート申請」や「Graffer 手続きガイド」、「Graffer 窓口予約」など、多彩なサービスを提供。既に全国約190団体に導入されており、約3,900万人の市民の生活を支えている。

また後者では、生成AIを自社のビジネスに取り入れたいと考える企業を強力に後押し。生成AI活用をトータルで支援する「生成AI活用伴走支援」や、生成AIの業務活用を推進するプロダクト「Graffer AI Studio」、AI人材育成を支援する「生成AI研修・人材育成サービス」などのソリューションを展開している。

エンドポイント対策のさらなる強化が課題に

このように躍進を続ける同社だが、事業活動における最重要課題の一つとして取り組んでいるのが、情報セキュリティの確保である。同社のセキュリティエンジニアを務める森田 浩平氏は「当社では、行政や市民の方々に関わるサービスを展開していますので、強固なセキュリティ体制があることは大前提です。プロダクトそのものの安全性はもちろんのこと、標的型サイバー攻撃のような人を狙う攻撃に対しても、細心の注意を払って対応しています」と語る。


株式会社グラファー
エンジニア
森田 浩平 氏

そうした取り組みの一環として今回実施されたのが、社員向けエンドポイント端末のセキュリティ強化である。森田氏はその背景を「アンチウイルスソフトの導入などはもちろん実施していますが、昨今では侵入を前提とした対策も強く求められるようになっています。従来型のパターンマッチングの仕組みでは、社員を守り切れないおそれもありますので、エンドポイント対策のさらなる高度化を図りたいと考えました」と説明する。

新たなエンドポイント対策製品に求められた要件としては、振る舞い検知や機械学習などの高度な検知ロジックを備えていること、CPUやメモリなどのリソース消費量が少なく業務に影響を与えないこと、Windows/Mac/Linuxの各OSに対応していることなどが挙げられる。

さらにもう一つ重視したのが、オフィスだけでなくリモートワーク環境の安全も守れるという点だ。森田氏は「基本的に当社はリモートワークが主体なので、端末も社員の自宅にあるケースが少なくありません。これらに対しても、日常的な防御やインシデント発生時の対応が行えることが必須でした」と語る。

こうした点を満たせるソリューションとして採用されたのが、ネットワールドが提供するクラウドストライク社のセキュリティプラットフォーム「CrowdStrike Falcon」である。

CrowdStrike Falconで脅威への網羅的な対策を実施

CrowdStrike Falconには様々なコンポーネントが用意されているが、今回同社では次世代アンチウイルス「Falcon Prevent」、EDR「Falcon Insight XDR」、脅威ハンティング「Falcon OverWatch」、IT資産管理「Falcon Discover」などを導入している。

CROWDSTRIKE

全社員のエンドポイント保護にCrowdStrike Falconを導入

導入メリット

- 脅威の防御から侵入後の検知・対応まで、網羅的な対策が行える環境を構築
- CrowdStrike FalconのAPIを利用し、アラートの情報共有を自動化
- MDRサービスの導入により、効率的なセキュリティ運用を実現

森田氏はその理由を「前述の通り、侵入を前提とした対策が求められる時代ですので、EDRは絶対に外せないと考えました。その点、CrowdStrike Falconは、EDRを含めた幅広い機能を提供しています。いろいろなセキュリティ製品が乱立すると運用管理も煩雑になりますので、単一のソリューションで幅広い領域をカバーできるのはありがたいです」と語る。

これにより、脅威の防御から侵入後の検知・対応まで、網羅的な対策が行える環境が実現。実際の導入作業に関しても、スムーズに進められたとのことだ。森田氏は「ポリシーやアラートの設定なども、CrowdStrike Falconの推奨設定でほぼ問題ありませんでしたね。おかげで追加のカスタマイズもそれほど行っていません」と語る。

EDRを導入した企業の中には、大量アラートへの対応などで疲弊してしまうようなケースも見受けられる。この点は同社でも認識していたため、今回は製品保守と運用をサポートするマネージドサービスも併せて導入している。

「専任のセキュリティエンジニアは私一人なので、細々とした対応に時間を取られるようだと本業に影響が生じかねません。その点、CrowdStrike Falconについては、様々な企業がマネージドサービスを提供していますので、セキュリティと運用管理負荷軽減を両立できます」と森田氏は語る。

リモートで働く社員が安心して働ける環境を実現

システム構築面での工夫としては、CrowdStrike Falconのアラートを既設のサーバー監視システムと連携させている点が挙げられる。ここには検知した脅威をSlack上で確認できる仕組みを構築しているため、万一インシデントが発生した場合も速やかにメンバー全員に通知することができる。「このようなことが実現できるのも、CrowdStrike Falcon側でAPIを提供してくれているからこそ。様々な作業を自動化できるのは大きなメリットですね」と森田氏は語る。

CrowdStrike Falcon導入後、幸いにして大きなインシデントに見舞われるような事態は起きていないとのこと。しかし、安心感は以前より格段に高まったという。「もし、リモートで働いている社員の端末に異常が発生したとしても、迅速に検知・隔離することができますし、状況によってはリモートワイプなども行えます。社員に安全・快適に働いてもらう上で、こうした環境が整った意義は大変大きい。また管理者の立場としては、過検知／誤検知が非常に少ない点も高く評価しています」と森田氏。今後はペネトレーションテストなども実施し、CrowdStrike Falconの導入効果をさらに高めていきたいとのことだ。

なお、今回の取り組みでは、ネットワールドの支援も大きく貢献。技術支援サービスを活用することで、効率的な製品導入を実現している。「導入時に手間が掛かりそうなところをすべて支援してもらえましたので、大変助かりました。ネットワールドでは他にも様々なセキュリティ製品を取り扱っていますので、今後の提案にも期待しています」と森田氏は述べた。

お問い合わせ

株式会社ネットワールド

https://www.networld.co.jp/

crowdstrike-info@networld.co.jp

本　社　〒101-0051　東京都千代田区神田神保町 2 -11-15
住友商事神保町ビル
TEL：03-5210-5020,5031,5095

関西支店　〒530-0001　大阪市北区梅田 3-3-20
明治安田生命大阪梅田ビル 24F
TEL：06-7777-4174

中部支店　〒450-0003　名古屋市中村区名駅南 1-17-23
ニッタビル 10F
TEL：052-588-7611

九州支店　〒812-0013　福岡市博多区博多駅東 2-6-1
九勧筑紫通ビル 3F
TEL：092-461-7815