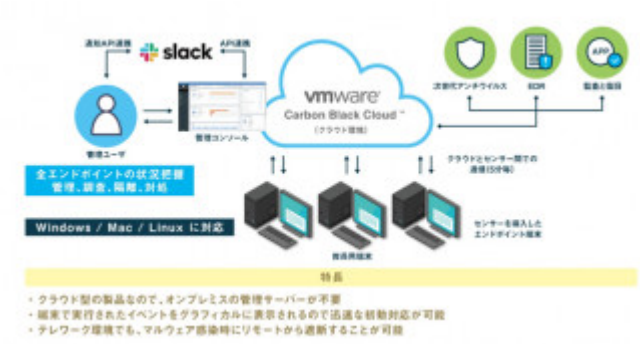
成城大学、次世代アンチウイルスとEDR機能を備えた「VMware Carbon Black Cloud」を採用



端末の挙動や操作をすべて可視化して、的確な状況把握と脅威対応を実現
調査・検索やマルウェア感染端末の遮断をリモートから実施可能に

ITインフラのソリューション･ディストリビューターである株式会社ネットワールド（本社：東京都千代田区、代表取締役社長 森田 晶一）は、成城大学（所在地：東京都世田谷区、学長 戸部 順一）のセキュリティ対策強化プロジェクトにおいて、ネットワールドが提供する「VMware Carbon Black Cloud」が採用され、2021年4月 より本番稼働を開始したことを発表します。

サイバー攻撃が巧妙化、複雑化の一途をたどる昨今、ウイルスの侵入を100%防御するのは不可能であることから、成城大学では、エンドポイントセキュリティ対策に早くから注目し、EDR（Endpoint Detection &
Response）製品を導入していましたが、データの収集や分析に時間がかかり、使い勝手が悪いなどの問題が多く、期待する成果が得られていませんでした。

今回、新たに導入したVMware Carbon Black
Cloudは、端末の操作や挙動を記録・可視化して、過去に遡って調査することが可能です。独自のストリーミング分析機能が搭載されており、Webアクセス、ファイルアップロードなどエンドポイントで実行される一連のイベントをリアルタイム解析してタグ付けし、相関分析できます。これにより、インシデントの原因となったアクションを的確に突き止めることが可能となりました。
学外でテレワークする職員には、VMware Carbon Black
Cloudエージェントを導入した端末を貸し出すことで、各端末の状況把握はもちろん、マルウェア感染時の遮断などもリモートから実行可能となりました。また、クラウド型のため、エージェントだけで物理／仮想の両方を監視できる点も評価されました。

PoCの段階では、低レベルの脅威もすべて通知する設定で運用開始したため、軽微なアラートが大量に発生してしまいましたが、これらにどう対処するべきかなどのアドバイスをはじめ、ネットワールドから提供した様々な運用ノウハウが高く評価されました。

◆ 導入の背景と選定ポイント

成城大学は、セキュリティには細心の注意を払っており、様々な製品を導入して対策を行ってい

ますが、情報漏えいなどの被害が「本当に無かった」と実証できることが非常に重要であると考えていました。内部に侵入した脅威の検知と、その後の対処を目的とするエンドポイント対策の有用性に着目し、早くから、EDR製品を導入していましたが、データの収集や分析に時間がかかる、使い勝手が良くないなどの問題が多く、なかなか思うような成果を上げられませんでした。

そこで、今回、新たなEDR製品を検討した結果、NGAV（次世代アンチウイルス）とEDRの両方の機能を備えたVMware Carbon Black Cloudを採用しました。VMware Carbon Black Cloudは、クラウド型の製品であるためオンプレミスの管理サーバーを自前で運用する必要がなく、大量ログの保管場所にも悩まされずに済みます。また、物理／仮想両方の環境を監視できる点や、エージェントだけで使える手軽さなどが評価されました。

◆ 導入の経緯と成果

具体的な監視対象として、大学の事務業務で利用されるPC約160台を選定しました。今回のような取り組みでは、複数のセキュリティ製品同士が競合してうまく動作しないことも多くありますが、VMware Carbon Black Cloudはスムーズに既存の環境に導入できました。また、端末へのエージェント配布は、資産管理ソフトを利用して20～30分程度で完了しました。

VMware Carbon Black Cloudの導入により、課題であった端末の操作や挙動を可視化することができ、独自のストリーミング分析機能により、PCで実行されるイベントをすべて記録／タグ付けして相関分析できるため、いつ、どのように実行されたアクションがインシデントの原因なのかを突き止めることが可能となりました。さらに、それぞれのイベントのつながりがグラフィカルに表示されるため、高度な専門知識を持たないメンバーでも、素早く正確な判断を下せることができ、このことは初動対応のスピードを上げることにつながり、非常に大きなメリットとなります。
また、一般的に、ファイルサーバーからのデータ持ち出しは、端末側からメディアにコピーされてしまうとゲートウェイでは検知できませんが、VMware Carbon Black Cloudは、このような行為もエージェントで確実にキャッチできます。

成城大学はテレワークを推進しており、自宅などで働く職員向けに、VMware Carbon Black Cloudのエージェントを導入した貸出端末を用意しました。これにより、各端末の状況把握はもちろん、マルウェア感染時の遮断などもリモートから行えますので、学外でも安心して働くことができます。
成城大学は、「ゼロトラスト」の実現に向けて、今後も環境改善を続けていく計画で、ネットワールドの提案に期待が寄せられています。

◆ 学校法人成城学園 成城大学について

https://www.seijo.ac.jp/
所在地：東京都世田谷区成城6-1-20
1950年に開設され、4学部11学科から構成される人文社会科学系の総合大学。

■ 株式会社ネットワールドについて

https://www.networld.co.jp/
株式会社ネットワールドは、ITインフラストラクチャーのソリューション
ディストリビューターとして、クラウド
コンピューティング時代の企業IT基盤を変革する技術製品と関連サービスを提供しています。サーバー、ストレージやネットワーク、そしてアプリケーションやデスクトップの仮想化に早期から取り組み、次世代のITインフラストラクチャーのあるべき姿をリードしています。
