未来を拓くチカラと技術。

NTT AT

News Release

2021年1月13日
NTTアドバンステクノロジ株式会社

FortiGate SOCサービスに「Microsoft Defender for Endpoint」の監視を追加
～エンドポイントセキュリティを強化し、コロナ禍でのリモート勤務を安心・安全に～

NTT アドバンステクノロジ株式会社（以下：NTT-AT、本社：神奈川県川崎市、代表取締役社長：木村丈治）は、高度化・巧妙化する攻撃に対応するためのエンドポイントセキュリティ対策の強化を狙い、NTT-AT が提供している FortiGate SOC（Security Operation Center）サービスの監視対象に「Microsoft Defender for Endpoint*1」（以下：本製品）を追加した監視トータルソリューションの提供を1月13日から開始します。

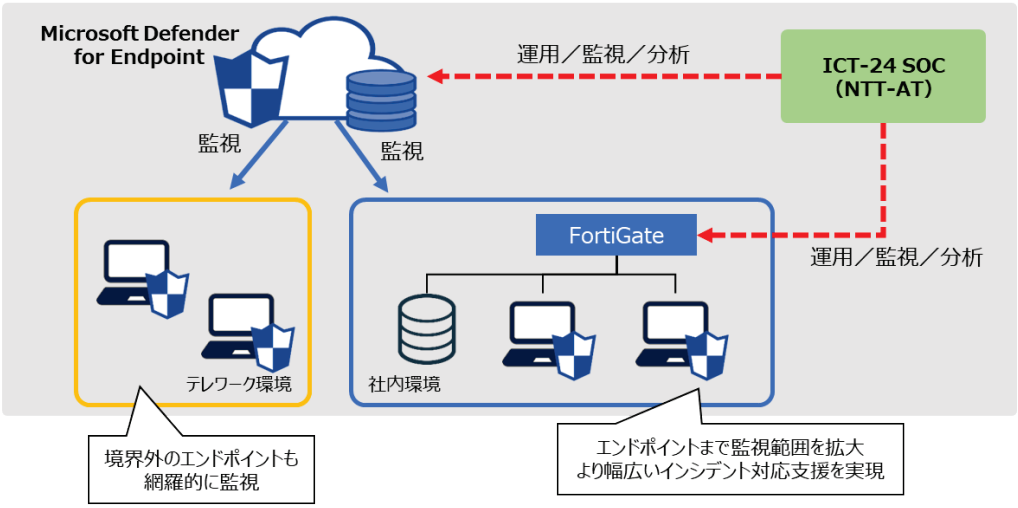
従来、NTT-AT では、FortiGate SOC サービスによる運用・監視ノウハウを使い、ネットワーク通信の観点でセキュリティ監視を実施してきました。しかし、近年の標的型メール攻撃などが高度化・巧妙化してきていること、またモバイル環境での端末のセキュリティを確保する必要があることから、エンドポイントのセキュリティ強化が一層重要になっています。

このような中、NTT-AT は本製品を使用することにより、社内ネットワークに接続していないリモート環境の端末を含めたセキュリティ監視を ICT-24 セキュリティオペレーションセンター（ICT-24SOC）にて提供します。またインシデント発生時には、端末で発生した事象のリモート分析も可能です。さらに、インシデント発生予防のため、各端末におけるセキュリティパッチの状況把握を可能とする監視ソリューションを提供いたします。

■背景および提供開始に至った経緯

近年マルウェアを用いた標的型攻撃は多様化しており、従来のファイアウォールなどのネットワーク通信向けの防御をすり抜ける攻撃が増加しています。あわせて、コロナ禍でのリモート環境の普及により、社内ネットワークに接続していない端末から、社内のリモートアクセス環境を経由した攻撃の可能性がでてきました。その一方で、個々の端末を管理することによるセキュリティ対策へのコスト増および運用業務の負担増などが課題となっています。

このような中、端末に着目したエンドポイントのセキュリティ強化の必要性が増しており、NTT-AT は、より高度な分析に対応するため、現在サービス提供中の FortiGate SOC サービスにエンドポイントの監視を追加し、ICT-24SOC にて提供することといたしました。



【提供するソリューションのポイント】

■本ソリューションの概要

本ソリューションは、NTT-AT が提供する FortiGate SOC サービスに、EDR（Endpoint Detection and Response：エンドポイントでの検出と対応）によるエンドポイントの監視を加えることにより、お客様環境に導入されている端末やサーバーをトータルで監視するものです。以下の特長があります。

① 本製品を使い、リモート端末を含め、端末が危険な状態にないかを監視します。端末が危険な状態にある場合、リモートで隔離し、復旧後はリモートで接続し再開が可能です。

② お客様の社内環境は、統合脅威管理 UTM（Unified Threat Management）製品（FortiGate）により監視することができます。これにより、本製品を搭載していない端末やサーバーについて、外部からの攻撃がないかどうかも監視します。また、端末間での感染拡大の監視も可能です。

③ ICT24-SOC サービスにて、24 時間 365 日の監視が可能です。

④ インシデント発生時には、リモートから端末の状況を分析します。オプションサービスとして、問題となったファイル（検体）をリモートで取得後、ふるまい解析し、専門知識をもったアナリストがリスク分析と、推奨する対応をお客様に提示します。

なお、EDR 製品として、FireEyeHX シリーズ*2 などへの対応も可能です。

■提供開始

2021 年 1 月 13 日

■提供価格

ご利用や価格などに関する詳細につきましては下記「お問い合わせ先」までご連絡ください。

■今後の予定

コロナ禍でテレワークが進む中、これまでのファイアウォールなどでオフィスの入り口を守るセキュリティから、リモートワーク環境も守り、そしてクラウドで守る時代への移行が進んでまいります。このような中、NTT-AT はゼロトラストの実現に向け、クラウド PROXY、CASB*3 等も拡大サポートしていく予定です。また、SASE*4 を指向したクラウド型 UTM のご提供をはじめとし、他の UTM、EDR のサポート製品を広げつつ、さまざまなソリューションを組み合わせたセキュリティサービスを展開してまいります。

*1：Microsoft Defender for Endpoint（旧称：Microsoft Defender Advanced Threat Protection（ATP））
⇒ Microsoft 社が提供する EDR 製品です。

*2：FireEyeHX シリーズ
⇒ FireEye, Inc.社が提供する EDR 製品です。

*3：CASB（Cloud Access Security Broker：キャスビー）
⇒ ガートナー社が提唱した用語で、企業が利用するクラウド・アプリケーションについて可視化、データ・プロテクション、ガバナンスを実現するサービス／製品を指します。

*4：SASE（Secure Access Service Edge：サシー）
⇒ ガートナー社が提唱している、 ネットワークとセキュリティの新しいアーキテクチャです。

【一般の方のお問い合わせ先】
NTTアドバンステクノロジ株式会社
セキュリティ事業本部
セキュリティサービス&ソリューションビジネスユニット
SOC担当
https://www.ntt-at.co.jp/product/fortigate-soc/edr

【報道関係のお問い合わせ先】
NTTアドバンステクノロジ株式会社
経営企画部
コーポレート・コミュニケーション部門
担当：加藤・増田
E-Mail：inquiry@ml.ntt-at.co.jp