FortiNAC：MSSP が提供するセキュリティサービス拡充を支援

要約

急速に進化するネットワーク、高度化し続ける脅威、IT リソースの不足などのプレッシャーが重なったことで、自社のセキュリティニーズを MSSP（マネージドセキュリティサービスプロバイダー）へとオフロードする動きが活発化しています。最上位の攻撃ベクトルであるエンドポイントは、多くの組織が最優先で保護しなければならない対象である状況が続いています。FortiNAC は、フォーティネット セキュリティ ファブリックの重要な構成要素であるネットワークアクセス制御（NAC）製品で、MSSP 固有のニーズに対応し、顧客への付加価値サービスの提供を通じたサービスポートフォリオの拡充を計りたいと考える MSSP を支援します。FortiNAC は、可視化、動的な制御、自動化された脅威へのレスポンスの優れた機能を備えているため、標的にされやすいエンドポイントベースの脅威に晒されるリスクが大幅に低下し、機密性の高いネットワーク資産が確実にセグメント化され、不正アクセスから保護されるようになります。

主なメリット

- あらゆるデバイスとユーザーの完全な可視化を実現
- 動的なセグメンテーション制御により、重要なデータや知的財産を保護
- 脅威へのレスポンス自動化により、封じ込めに要する時間を数日から数秒へと短縮
- 厳格化が進むコンプライアンス要件への対応を支援
- 容易な導入、拡張、管理

顧客を脆弱性のリスクに晒し続けるレガシーのアクセス制御

自社のセキュリティの一部を機能と予算の両方の理由からアウトソースしたいと考える企業が増えており、このような現状が MSSP のビジネス拡大を後押ししています。IDC は、セキュリティ関連サービスの規模が 2018 年には 914 億ドルに達し、2017 年と比べて 10.2% 増となる見通しだと予測しています。[1] Allied Market Research が発表した最近のレポートによれば、2016 年から 2022 年にかけて、マネージドサービスは CAGR（年平均成長率）20.3% で成長すると予測されており、最も成長著しい分野とされています。[2]

急速な変化と上昇するリスクの 2 つの要因が重なることで、この需要の高まりをさらに加速させています。デジタルトランスフォーメーション、すなわちクラウドサービスの採用、IoT（モノのインターネット）デバイス、モバイル製品の多様化によって、ネットワークのセキュリティ確保が限りなく困難になりました。標的型攻撃の脅威が高度化し続けていることで、たった 1 台のエンドポイントデバイスに起因するブリーチの平均被害額は 500 万ドルまで膨らんでいます。[3] このように極めて深刻な脆弱性の問題への対応が求められるなか、ほとんどの企業で高度なスキルを持つサイバーセキュリティのプロフェッショナルを確保できない状態が続いており、2021 年までに 350 万人もの人材が不足すると予測されています。[4]

エンドポイントは、攻撃の標的として常に最上位になっています。そのような状況で、古いアクセス制御によってマルウェアに感染したデバイスや、盗難されたエンドポイントの認証情報を使った不正アクセスが発生し、ネットワークが危険な状態になる可能性があることが、大きな問題となっています。第 1 世代のネットワークアクセス制御製品は、「スキャンしてブロック」する単純なテクノロジーを使ってエンドポイント（主に管理対象である PC）を認証し、アクセスを許可する機能を備えるものでした。第 2 世代の NAC ソリューションへの進化によって、企業ネットワークへのゲストアクセスの管理に伴う新たな課題が解決されています。

しかしながら、ネットワークやエンドポイントの脆弱性の現状が発端で第 3 世代の NAC ソリューションのニーズが生まれ、セキュリティギャップを解消して顧客の重要なデータや知的財産を保護することが期待されるようになりました。

FortiNAC が MSSP のお客様に提供するメリット

フォーティネットの第 3 世代 FortiNAC ソリューションによって、エンドポイントを標的にする脅威からの保護が実現するとともに、セグメント化の制御がサードパーティ製デバイスまで拡大し、さまざまなネットワーキングデバイスへの自動レスポンスのオーケストレーションが可能になります。

MSSP の顧客は、包括的な NAC によるセキュリティの次の 3 つの柱に対応し、その効果が実証済であらゆる機能を備えた、PAYG（Pay-As-You-Go）方式の統合エンドポイントアクセスソリューションを必要としています。

- **ネットワーク全体の可視化**：あらゆるユーザーとデバイス（BYOD や IoT を含む）の可視化
- **動的なアクセス制御**：ポリシーベースのネットワークセグメンテーションによるアクセス制御
- **瞬時の自動レスポンス**：潜在的な脅威を数秒で阻止

同様に重要なのは、クライアント向けの分析とレポート、特にコンプライアンス要件としてこれらの機能を求められることです。FortiNAC によって、MSSP は新規および既存のクライアントに対して柔軟で経済的なサブスクリプションベースのライセンス体系、トレーニング、サポートを通じてネットワークセキュリティサービスを提供できるため、新たな収入源が創出され、競争力の向上にもつながります。

サードパーティソリューションをサポートする統合セキュリティ

フォーティネット セキュリティ ファブリックの構成要素である FortiNAC は、フォーティネットの他のソリューションだけでなく、MSSP が提供するサードパーティのファブリック・レディ セキュリティ製品とも統合されます。フォーティネット独自のセキュリティアーキテクチャとアプローチでは、MSSP の顧客の既存のネットワークスイッチ、ルーター、アクセスポイントに固有の遠隔制御機能を活用し、あらゆる製造元のネットワーク機器と接続デバイスの包括的なビューが提供され、リスクが持ち込まれる死角が解消されます。この独自のトリアージプロセスによって、セキュリティ、ネットワーク、エンドポイントの情報のサイロが連携可能になり、既存のネットワークインフラストラクチャを活用し、ネットワークトラフィックに影響することなくポリシーベースのアクセス制御によるレスポンスを実装できます。

導入の拡張性と柔軟性：FortiNAC は、高度な拡張性を実現するアーキテクチャの採用によって、サイト毎にサーバーを導入する必要がないため、MSSP は 1 台のサーバーからクライアントの異なる場所でのネットワークアクセスを制御できます。FortiNAC の使いやすい Web インタフェースは、ネットワークとセキュリティの運用を管理する強力なツールを提供します。この優れた柔軟性によって、MSSP は初期段階の試用から試験段階、さらには本番環境への正式導入までのすべて工程でセキュリティサービスを進化させ、有効なセキュリティポリシーを実装することができます。

FortiNAC が MSSP のパートナー各社にもたらすメリット

急成長するこの市場で、MSSP のパートナー各社にできるだけ多くのビジネスチャンスを活かしていただくため、フォーティネットでは、MSSP 専用の FortiNAC ソリューションのライセンスプログラムを提供しています。このプログラムには、次のようなメリットがあります。

成長と利益の最大化：先行投資不要のサブスクリプションベースのモデルの採用によって、設備投資（CAPEX）ではなく運用費（OPEX）ベースでクライアントが FortiNAC セキュリティサービスを利用できるため、MSSP は販売の障壁が低くなります。仮想アプライアンス、セールストレーニング、製品トレーニング、導入支援、導入後の製品アップデートやサポートなど、迅速な運用の開始に必要なサービスは、有償でフォーティネットから MSSP に提供されます。階層型の価格体系で、クライアント向けに柔軟な価格設定が可能なため、MSSP は FortiNAC を活用して自社のビジネスを拡大することができます。

新興市場での新たなサービス機能の提供：FortiNAC は、既存のセキュリティ制御を活用すると同時に、それを補完する機能（可視性、制御、自動レスポンス）を提供することで、万全なセキュリティを実現します。顧客のニーズに合わせて拡張可能な設計の FortiNAC は、要件の厳しい環境でも 24 時間 365 日の監視、自動脅威トリアージ、封じ込めが可能であることが実証されています。また、コンプライアンスや法規制に関連するレポートを容易に作成できるツールも提供されています。

既存のセキュリティサービスの拡張：FortiNAC は、セキュリティ ファブリックの拡張機能として、ファイアウォール、ISP / IDS（不正侵入防止 / 検知）、エンドポイントセキュリティ、SIEM（セキュリティ情報 / イベント管理）、EMM（エンタープライズモビリティ管理）などの既存のセキュリティソリューションと連携して機能します。堅牢な REST API を活用して syslog をネイティブで使用できるため、既存のセキュリティソリューションとシームレスに統合されます。また FortiNAC は、エンドポイントの可視化や脅威へのレスポンスを求める顧客を獲得する際のセールスポイントとしても有効で、追加のマネージドサービスを提案するきっかけにもなります。

見えないものは保護できない

接続されているすべてのエンドポイントをリアルタイムで可視化することは、セキュリティギャップの解消に不可欠な第一歩となります。存在することがわかっていないデバイスを保護することはできません。フォーティネットの第 3 世代 FortiNAC ソリューションは、レガシーのネットワークアクセス制御によって生じるデバイスベースのセキュリティギャップを解消するとともに、MSSP パートナーにとっては、今日の市場で提供されている他のマネージドセキュリティサービスを凌駕する、優れたメリットをもたらすポートフォリオとなります。

[1]「Worldwide Spending on Security Solutions Forecast to Reach $91 Billion in 2018（世界全体のセキュリティソリューションの支出が 2018 年に 910 億ドルに達すると予測）」、IDC、2018 年 3 月 27 日：https://www.idc.com/getdoc.jsp?containerId=prUS43691018

[2]「Cyber Security Market to Reach $198 Billion, Globally, by 2022（世界のセキュリティ市場が 2022 年までに 1 兆 9,800 億ドルに成長）」、Allied Market Research、2018 年 7 月 30 日：https://www.alliedmarketresearch.com/press-release/cyber-security-market.html

[3] Charlie Osborne 著、「Fileless attacks surge in 2017, security solutions are not stopping them」、ZDNet、2017 年 11 月 15 日：https://www.zdnet.com/article/fileless-attacks-surge-in-2017-and-security-solutions-are-not-stopping-them/

[4] Steve Morgan 著、「Top 5 cybersecurity facts, figures and statistics for 2018（2018 年を象徴する 5 つのサイバーセキュリティの事実、数字、統計）」、CSO Online、2018 年 1 月 23 日：https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html

FORTINET
フォーティネットジャパン株式会社

〒106-0032
東京都港区六本木 7-7-7
Tri-Seven Roppongi 9 階
www.fortinet.co.jp/contact

お問い合わせ

SB-FNC-MSSP-201811-R1