WHITE PAPER

ハイブリッドワークにおける クラウドの保護

重要資産の保護で求められる エンドポイントセキュリティへの新たなアプローチ

概要

クラウドベースのサービスにアクセスするリモートワーカーは、今後もますます一般化が進むでしょう。リモートワークでの通信を保護するには、エンドポイントセキュリティへの新たなアプローチが求められます。パターンファイルと一致するマルウェアシグネチャがネットワークに侵入するのを受動的に待つよりも、最新の EDR（エンドポイントの脅威検知とレスポンス）ツールを使用する方が、組織はセキュリティに対してより積極的なアプローチを展開できます。EDR ツールを大規模なサイバーセキュリティメッシュアーキテクチャ（CSMA）に統合すれば、そのメリットはさらに増大します。

EDR ソリューションを検討する際に、外してはならない重要な機能がいくつかあります。まず、EDR ソリューションには攻撃対象領域を評価する機能が必要です。これはギャップの解消を可能にするためです。次に、シグネチャベースと振る舞いベースの両方のアプローチを用いて、プロアクティブなマルウェア対策を実施する必要があります。さらには、甚大な損害が生じる前に、攻撃を検知し無効化できなければなりません。将来の攻撃を防止するには、脅威のレスポンスと修復を自動化すると共に、広範囲にわたるフォレンジックと脅威ハンティングを実行する機能も必要です。

クラウドにおけるエンドポイントの課題

産業界があらゆる業種で Work-From-Anywhere（場所に縛られない働き方）を取り入れているように、リモートワークやハイブリッドワークの勤務体制が定着しつつあることは明らかです [1]。ある調査によると、94% の組織が何らかの形でハイブリッドワークを導入しています。また、69% の組織は、こうした新しい働き方がオフィスのスペースや IT 人材の確保など、あらゆる面に影響していると答えています [2]。

もちろん、このような傾向はサイバーセキュリティにも大きく関係します。さまざまな場所で業務ができる体制を整えることで、攻撃対象領域は拡大します。さらには、内外の脅威からの保護を必要とするエンドポイントが増加する可能性もあります。こうした状況は、ますます巧妙化する脅威によって深刻化しているため、組織は増え続ける感染経路からのエンドポイント攻撃に備えておく必要があります。

リモートワーカーとクラウド

組織がクラウドベースのサービスへと急速に移行することで、従業員が遠隔地からアクセスする企業資産を保護するための対策はさらに複雑化します。誰の目にも明らかなように、新型コロナウイルスのパンデミックは、すでに急ピッチで進んでいたクラウド導入をさらに加速させました。これは、組織が在宅勤務の基盤を確立または拡充し、顧客がサービスのさらなるデジタル化を求めた結果です。

最近のある調査によると、IT 担当者の約 3 分の 2 が現時点で、自社が 2 年以内に IT サービスの 60% をクラウドに移行すると予測しています [3]。しかし、多くの場合、自宅やコーヒーショップで仕事をする従業員は、主に SaaS（Software-as-a-Service）アプリケーションやクラウドベースのインフラストラクチャから提供されるサービスを以前から利用しており、そもそも企業のデータセンターにアクセスする必要がほとんどありません。

現代のデジタル環境における組織の成長と発展を促進するうえで、クラウドテクノロジーが重要な要素となっていることは明白です。パンデミックの発生直後には、完全なリモートワークへの急な移行を実現し、サプライチェーン、コストの増加、顧客の好みや期待の急激な変化といった目下の問題への対応も可能にするなど、企業にとってクラウドテクノロジーの重要性は計り知れません。

しかしながら、組織が近年行ってきた変更の慌ただしさは、多くの面でセキュリティが疎かになっていたことを意味します。マルウェアなどのサイバーセキュリティ攻撃に対する不安の声はよく聞かれますが、エンドポイント保護に対する取り組みの強化については、特にクラウドベースのリソースとなると、あまり進展が見られません。残念ながら、攻撃者はほんの数秒もあれば、侵害されたクラウド接続のエンドポイントに対して高度な攻撃を仕掛けることができるのです。

クラウド固有の課題

サイバーセキュリティチームは、たとえクラウドベースのサービスが存在しなかったとしても、多くの課題を抱えていたことでしょう。ただし、クラウドプラットフォームは、オンプレミスインフラストラクチャとは多くの点で異なります。クラウドプラットフォームを保護するには、クラウドに固有のセキュリティに関する課題を理解する必要があります。課題には以下のようなものがあります。

- **不適切なクラウドセキュリティプロトコル**：クラウドのセキュリティ保護が不十分な企業では、高度なツールを使用する攻撃者の標的になるリスクが増大します。強力なクラウドセキュリティ対策を講じていない企業は、これまでの不審なネットワークアクティビティや、更新されていないセキュリティパッチ、クラウドエンドポイントの脆弱性などの問題に気づくことができません。
- **低速のレスポンス**：攻撃者は偵察ツールを使用して、企業が反応する前にセキュリティの弱点を攻撃する方法を探します。このような攻撃は多大な損害を与えます。なぜなら、攻撃者には企業のセキュリティ対策を回避する時間が与えられるからです。攻撃組織の中には、侵入ツール（Cobalt Strike Beacons など）の開発と販売だけを行うものもあります。そのため、より有能な攻撃グループは、損害を与えて被害者から金銭を搾り取ることのみに集中できます。
- **クラウドの構成ミス**：クラウドエンドポイントが適切に保護されていなければ、サイバー攻撃者は自らの目的のためにデータを窃取することができます。クラウドセキュリティポリシーの知識が不足していると、クラウドインフラストラクチャの実装で間違いが起こる可能性があります。

組織はリスクを理解し、適切な制御機能を導入し、分散した従業員を管理する必要があります。なぜなら、リモートで業務を機能させることが最重要課題だからです[4]。

強力な EDR ツールの重要性

複雑化する攻撃者の手法や、ハイブリッドクラウドアーキテクチャを使用するリモートワーカーがもたらす個々の課題は、エンドポイントセキュリティへの新たなアプローチが必要であることを明確に示しています。EDR ソリューションは、シグネチャベースのアンチウイルスや侵入防止だけでなく、事後対応型の脅威レスポンスからプロアクティブなリスク減災への移行を支援します。

ただし、少し前に EDR を導入した組織では、現在、管理上の問題が生じています。その理由の一つは、第1世代の EDR ツールは多くの手動操作を必要とし、セキュリティインシデント発生時のレスポンスが遅いことにあります。プロアクティブな脅威レスポンスが遅れると、エンドユーザーの本番環境やシステムが停止するリスクが生じます。新しい EDR ソリューションは、インシデントレスポンス（IR）を自動化し、侵入口で脅威をすばやく無効化して損害を最小限に抑えると共に、クラウドクラスタや接続先ネットワークでの水平移動を阻止します。

EDR ソリューションに求められるもの

優れた EDR ソリューションは、エンドポイントへの攻撃前と攻撃後に、未来志向でリアルタイムの脅威保護を実施することで、エンドポイントセキュリティの欠点に対処します。これにより、組織は事前に攻撃対象領域を縮小できます。さらに、次世代のエンドポイント保護ソリューションは、軽量のフレームワークで広範囲な検知、防止、およびレスポンス機能を提供するため、システムリソースがそれほど多くないデバイスにも導入できます。

EDR ソリューションに必要な機能は次のとおりです。

攻撃対象領域の発見と縮小

優れた EDR ソリューションは、自動化された攻撃対象領域ポリシーによる高度な制御を行います。これには、脆弱性を自動的に管理するための脆弱性評価やポリシー作成などの機能が含まれます。組織はこの技術を使用して、セキュリティ保護におけるギャップや弱点を見つけることもできます。EDR ツールでは以下を実行できる必要があります。

- 保護または管理されていないデバイスを特定し制御する。
- 脆弱性に関する総合的かつ実用的なインテリジェンスを、判定や評価と共に提供する。
- 脆弱性に仮想パッチを適用して攻撃を減災する。

EDR ソリューションのプロアクティブなリスク減災機能を使用すると、組織内の保護されていないエンドポイントを削減し、攻撃者が利用可能な攻撃対象領域を効率的に縮小することができます。

マルウェアの防止

サイバー犯罪者は新しく高度なツールを使用することで、より簡単に脆弱なクラウドエンドポイントへのマルウェア攻撃を実行できるようになりました。特徴的な事例を紹介しましょう。RaaS（Ransomware-as-a-Service）プロバイダーは、専門知識がなくてもあらゆる業種と規模の組織に破壊的ランサムウェア攻撃を実行することを可能にしました。これは、近年このような攻撃が急増している要因の一つです。

今日では、既存マルウェアのシグネチャに加えて、振る舞いベースのアンチマルウェア、すなわち次世代アンチウイルス（NGAV）とも呼ばれるテクノロジーの利用が必要不可欠です。NGAV は、オンプレミスやクラウドベースのネットワークで水平に拡散される前に新型マルウェアを阻止します。

組織は、多数の OT（オペレーショナルテクノロジー）システムをはじめとする、インターネットに接続されていないエンドポイントへのマルウェア攻撃も防止しなければなりません。これらのエンドポイントの多くは、重大な脆弱性を抱えつつも更新ができない旧式のオペレーティングシステムで動作しています。このようなシステムには、本番環境への導入前にシミュレーションモードでの実行が可能なエンドポイントセキュリティソリューションが適しています。

EDR ツールに必要とされる重要なマルウェア防止機能は次のとおりです。

- 攻撃を阻止できる振る舞い / カーネルベースの NGAV
- 継続的アップデートを受信するリアルタイムの脅威インテリジェンスフィードとの統合
- 機密度の高いシステムのロックダウンに役立つアプリケーション制御
- 修復ツール
- オプションがカスタマイズ可能で、きめ細かいポリシーを作成できる自動 IR
- 脅威ハンティング機能

攻撃の検知と無効化

最良のマルウェア対策を講じていても、クラウドシステムへの攻撃は避けられません。EDR ソリューションは、攻撃が発生した場合にリアルタイムでそれを無効化できる必要があります。損害が生じる前に、実行中の攻撃を停止させることが、侵害を防止し、データ喪失のリスクやその修復作業を軽減するための重要なポイントとなります。

EDR ソリューションの AI（人工知能）が、異常なフローやプロセスの振る舞いなど不審なアクティビティを検知した場合は、アウトバウンド通信の送信をブロックし、ただちに攻撃を無効化しなければなりません。さらに、その攻撃が他のクラウドシステム、接続デバイス、またはネットワークにアクセスできないようにしておく必要があります。EDR が防止すべき不正ソフトウェアの活動には次のようなものがあります。

- データの不正入手
- C2（コマンド & コントロール）通信の有効化
- ファイルやレジストリの改ざん
- ファイルの暗号化
- バックドアの設置

セキュリティ侵害の影響をさらに抑制するには、以下の関連機能が必要です。

- メモリベースおよび「環境規制型」を含む攻撃の検知
- ログ履歴全体を分析する機能
- 脅威の分類を継続的に検証

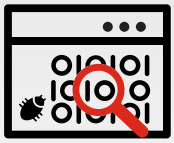
レスポンスおよび修復

組織が迅速にポリシー違反に対応し修復を行う主な方法は、IR 操作のオーケストレーションです。オーケストレーションには、ユーザー、デバイスタイプ（サーバーなど）、およびクラウド別の各グループ向けに設計された、カスタマイズ可能なプレイブックを使用します。攻撃を仕掛けられた組織は、クラウドなどの環境で 1 台または複数のデバイスに対して行われたシステム変更を手動または自動でロールバックします。これにより、セキュリティ担当者は以下の処理が可能になります。

- セキュリティインシデントの自動分類
- プレイブックの自動化によって実行される標準 IR 手順の作成

組織は以下の処理を自動化することで、セキュリティリソースを最適化できます。

- ファイルの削除
- 不正なプロセスの終了
- 永続的変更の取り消し
- アプリケーションおよびデバイスの隔離
- チケットの作成



攻撃のさらなる巧妙化が続く中、エンドポイントを狙った高度な攻撃やサイバースキル不足に対処するには、リアルタイムのアプローチが不可欠です [5]。

調査および追跡

EDR ツールには、感染前および感染後のマルウェアの動作について収集した情報を自動的に使用して、感染したエンドポイントのフォレンジックを実行する機能も必要です。セキュリティアナリストは、ガイド付きインタフェースを利用できる必要があります。ここには、セキュリティに関するベストプラクティスや、潜在的脅威の評価で次に実施すべき論理的手順が表示されます。

最も優れたソリューションは、インメモリ攻撃のメモリスナップショットを保存する機能を使用して、攻撃チェーン全体を可視化します。ガイド付きインタフェースには、イベントに「不審」のフラグが付けられた明確な理由と共に、MITRE ATT&CK マトリクスの中の該当する TTP（戦術、手法、手順）が表示されます。

EDR ソリューションの構築方法

EDR ソリューションを選択する場合は、そのツールの各種機能のほか、自社のインフラストラクチャやサイバーセキュリティワークフローの中でツールがどのように動作するかを検討する必要があります。

セキュリティインフラストラクチャとの統合

EDR ツールは、セキュリティインフラストラクチャの他のコンポーネントと共に、Gartner がサイバーセキュリティメッシュアーキテクチャ（CSMA）と呼ぶ仕組みに組み込まれている必要があります。広範かつ統合的で自動化されたアプローチをセキュリティアーキテクチャに用いることで、以下のように EDR の有効性を高める多くの利点が得られます。

- ネットワークアクセス制御（NAC）ツールを使用して、デバイスをネットワークから修正用 VLAN に隔離する。
- 次世代ファイアウォール（NGFW）を使用して不正な IP アドレスをブロックし、後続の攻撃を防止する。
- SIEM（セキュリティ情報 / イベント管理）ツールと SOAR（セキュリティオーケストレーション、自動化、レスポンス）ツールの統合を通じて、攻撃のフォレンジックへの理解を深める。

多くのベンダーが自社のセキュリティ製品を統合していますが、自動的に起動する定義済みアクションにおいて、ベンダーがどのようなサードパーティソリューションをサポートしているかを知ることも有益です。ベンダーがセキュリティアーキテクチャのコンポーネントをサポートしていない場合は、内部の統合に API（アプリケーションプログラミングインタフェース）を利用できるかどうかを確認する必要があります。

マネージドオプション

EDR ツールの利用経験がない、あるいは専任の SOC（セキュリティオペレーションセンター）チームがない組織にとって、旧式のアンチマルウェア技術から振る舞いベースのエンドポイントソリューションへの移行は、重大な方針転換になり得ます。このような組織は多くの場合、マネージドオプションを提供するベンダーを希望します。これは、自社の EDR ソリューションのアラート、調査、例外作成、レポート作成などの管理に利用するためです。

マネージドオプションを導入する組織にとっては、以下が判断の基準となります。

- スタッフ全員がベンダーの正規従業員であり、請負業者ではない。
- ベンダーのマネージド EDR スタッフは、現地チームと同じ地域に配属されている。
- マネージド製品のスタッフは、EDR ソリューションに組み込まれている他のセキュリティ技術（ファイアウォール、チケット発行システム、NAC、SIEM など）についても訓練を受けている。

サイバーセキュリティメッシュアーキテクチャ（CSMA）は、共通かつ統合されたセキュリティ構造とセキュリティ態勢を提供し、オンプレミス、データセンター、クラウドなどの場所を問わず、すべての資産を保護することができます[6]。

終わりに

リモートおよびハイブリッドワークの勤務体制は、クラウドベースのサービスと共に定着しつつあります。この組み合わせはリスクを伴う可能性があり、エンドポイントセキュリティへの新たなアプローチを必要とします。EDR ソリューションは、組織の内外で発生するサイバー攻撃から、社内およびクラウドベースのサービスを保護します。EDR ソリューションの必須機能は次のとおりです。

- 振る舞いベースのマルウェア検知
- 不正なデバイスの発見
- 脅威ハンティング
- 仮想パッチ
- フォレンジック調査
- リアルタイムの攻撃ブロック
- 自動 IR

最も優れたソリューションは、他のセキュリティコンポーネントとシームレスに一体化する統合型 CSMA アーキテクチャを採用することで、セキュリティアーキテクチャ全体が連携して攻撃を防ぎ、攻撃があった場合は即座に対応します。攻撃後には徹底したフォレンジックを実施し、同じ攻撃の再発を防止します。

FortiEDR を Google Cloud マーケットプレイスで確認する

Google Cloud

1 「Hybrid Work Is here to Stay, So Companies Are Spending More on Security」、Liam Tung 著、ZDNet、2022 年 6 月 28 日（英語）：https://www.zdnet.com/article/hybrid-work-is-here-to-stay-so-companies-are-spending-more-on-security/

2 同上

3 「Rush to Cloud Computing Is Outpacing Organizations' Ability to Adapt」、Joe McKendrick 著、ZDNet、2022 年 3 月 5 日（英語）：https://www.zdnet.com/article/rush-to-cloud-computing-is-outpacing-organizations-ability-to-adapt/

4 「The Security Challenges of Hybrid Working」、Verizon、2022 年 8 月 16 日時点の情報（英語）https://www.ft.com/partnercontent/verizon/the-security-challenges-of-hybrid-working.html

5 「Endpoint Detection and Response is a Key Weapon in the Battle Against Ransomware」、David Finger 著、CSO、2021 年 5 月 24 日（英語）：https://www.csoonline.com/article/570767/endpoint-detection-and-response-is-a-key-weapon-in-the-battle-against-ransomware.html

6 「サイバーセキュリティメッシュアーキテクチャ構築の進め方：Gartner® リサーチレポート」、Gartner®、Felix Gaehtgens、James Hoover、Henrique Teixeira、Claudio Neiva、Michael Kelley、Mary Buddy、Patrick Havesi 共著、2021 年 10 月 18 日：https://www.fortinet.com/jp/solutions/gartner-cybersecurity-mesh

FORTINET

フォーティネットジャパン合同会社

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

お問い合わせ

WP-Cloud-Hybrid-Protection-202310-R1