Lookout®

ホワイトペーパー

ポストペリメターの世界を保護する方法

Lookout

ポストペリメターの世界とは

クラウドやモバイルが中心となっていく世界では、企業リソースを情報漏えいや攻撃から守るため、企業は重要な次の 3 つの現実について考える必要があります。

1. 境界はもはや存在しない。
2. 従来のセキュリティ技術では十分ではない。
3. 端末は信頼できない。

従業員が企業のリソースにアクセスするために使用する端末に、管理されているものと管理されていないものが混在しているため、新たなセキュリティ アーキテクチャのニーズが高まっています。それは
ポストペリメター セキュリティです。

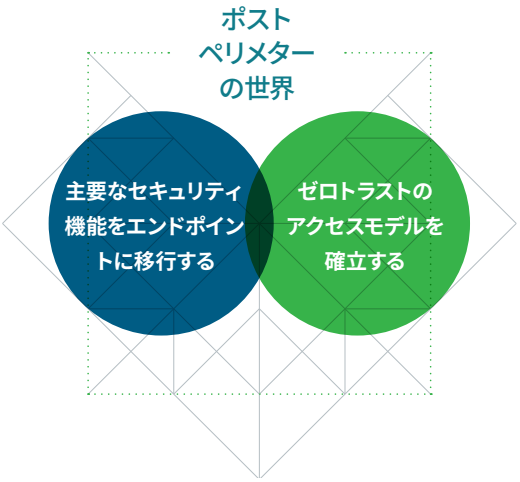
問題:
境界はもはや存在しない

働き方は根本から変化しています。重要なデータがクラウドに移行し、従業員は世界中のどこにいても、あらゆるネットワークからアクセスできます。たとえば、従業員が仕事のメールを確認したり、外出先から機密文書を閲覧/ダウンロードするために、わざわざ VPN に接続する必要はないのです。

また、フィッシングなどの攻撃も進化し、もはや既存の境界保護ではユーザー トラフィックへの可視性が保てないという点が悪用されてます。さらに、現在では企業の端末も個人的なものになっています。ソーシャル メディアやメッセージング アプリでの従業員が個人的な活動を通じて、フィッシング被害に遭ったり、企業の認証情報が盗まれたりしやすい環境が生まれています。

モバイル活用や企業データへのシームレスなアクセスは、企業の生産性にとっては大きな発展です。その一方で、ファイアウォールやセキュア Web ゲートウェイなどのペリメター セキュリティに依存するセキュリティ チームにとっては深刻な課題が生じています。

実際、もはや従来通りの場所に企業データは保管されていません。データの保管場所は柔軟に変化して、アクセスしやすくなっています。このようなエコシステムの変化により、次の 2 つの新たなセキュリティ ニーズが生じています。



主要なセキュリティ機能をエンドポイントに移行

第一に、エンドポイントを従来のペリメター セキュリティの影に隠したり、VPN でトラフィックを境界内に入れたりするのではなく、セキュリティ自体をエンドポイントに移行しなければなりません。セキュリティは、データがアクセスされるあらゆる場所に配備し、かつエンド ユーザーのプライバシーに影響を与えないようにする必要があります。

ゼロトラストのアクセスモデルを確立する

エンドポイントにセキュリティが装備されていていても、有害性が実証されるまで企業端末が無害であると思い込んではなりません。この新たな世界では、エンド ユーザーのプライバシーに影響を及ぼさずに企業データへのアクセスを許可するには、すべての端末の正常性を継続的にチェックする必要があります。

新たなセキュリティ アーキテクチャ: ポストペリメター セキュリティ

この、新しいセキュリティ アーキテクチャが必要であるという概念を、Lookout では「ポストペリメター セキュリティ」と呼んでいます。[1]ポストペリメター セキュリティは、それぞれがパズルのようにつながった、次の 3 つの機能で構成されています。

- エンドポイント保護
- クラウドへのアクセス
- ID とアクセスの管理

エンドポイント保護ソリューションを使用して端末のリスクを評価することは、ポストペリメター セキュリティ アーキテクチャの極めて重要な側面です。この保護により、端末上のあらゆる脅威やリスクを絶えず可視化することができます。こうすることで初めて、従業員の端末が認証を受けて企業のリソースにアクセスするのに相応しい正常性を保持しているかどうかを判断できるのです。この保護を通じて、企業固有のリスク許容度に応じて、リアルタイムでポリシーを施行できます。

ペリメター セキュリティの防御に頼らずに、企業のクラウドへのアクセス、ひいてはインターネットへのアクセスを保護することは、このアーキテクチャのもう 1 つの重要な側面です。これを可能にするため、重要なセキュリティ機能の一部をエンドポイントに移行する必要があります。悪意のあるリンクや Web サイトを監視し、従業員の危険なコンテンツへのアクセスを阻止する機能は、必ず移行すべき重要な機能です。

これら 2 つの側面がシングルサインオン (SSO) プロバイダーなどの ID 管理ソリューションと連携し、従業員に認証と企業リソースへのアクセスを許可したり、認証さえも拒否したりします。認証後も引き続きエンドポイント リスクが評価され、新たなリスクが検知されると、その都度アクセスが取り消されます。特定のシナリオでは、アクセスは、管理対象端末などを対象としたエンタープライズ モビリティ管理 (EMM) や、管理対象アプリケーションなどを対象としたモバイル アプリケーション管理 (MAM) で管理されます。

世界がポストペリメター セキュリティへ移行している理由

企業データはますますクラウドでホストされるようになり、同時に IT 部門の管轄下にないネットワークとつながっているエンドポイントからアクセスされるようになってきています。たとえば、広域携帯通信網や公共 Wi-Fi などです。企業データは IT 部門が管理するサーバーやネットワーク上のエンドポイント間で移動するものではなくなりました。企業データの大部分が、物理的に企業に出入りすることすらないのです。今日の企業データは、あらゆるネットワークを移動し、どの端末からでもアクセス可能なのです。

「ガートナー社は 2020 年までに、従業員の業務の 80% がモバイル端末で行われると予想しています。」

– ガートナー社「Prepare for Unified Endpoint Management to Displace MDM and CMT」2018 年 6 月

クラウドベースの生産性向上ツールの登場

現在、ID とアクセス管理ソリューションを活用した上で、サービスとしてのソフトウェア (SaaS) 提供モデルを通して、オフィスで中心となる生産性向上アプリケーションが利用されています。SaaS アプリのライセンス モデルは単一の端末に制限されることなく、ユーザー ID に割り当てられます。つまり、ユーザーは PC かモバイル端末かを問わず、どこにいても、どの端末からでも必要に応じてこれらのアプリケーションにアクセスできるのです。その反面、組織は従来のセキュリティで企業データへのアクセスや移動を制御する方法に頼ることはできなくなりました。

高度な管理と制御のニーズ

ポストペリメターの世界では、従業員が仕事に使用するツールを制御できる自由裁量の幅が大きくなっています。IT 部門から提供される企業アプリやサービスではなく、生産性や使いやすさの面から一般のツールを活用することも増えてきました。IT 部門には、ユーザーの業務を阻むことなく、企業データへの安全なアクセスを提供するという課題があります。これには BYOD の普及も伴っています。BYOD ではたいていの場合、IT 部門が端末自体を制御する機能が制限されます。モバイル端末管理やモバイル アプリケーション管理ソリューションなどによって可能な限り端末とアプリケーションを管理することに加え、ID と SaaS アプリケーションの制御によって企業データを保護することも大切な要素です。

既存の戦略に基づく
ポストペリメター セキュリティ

ユーザーやエンドポイントが企業ネットワークにアクセスしたときに、データへのアクセス権を自動的に付与することは、モバイルやクラウドの世界ではもはや通用しません。これが、Forrester Research 社のアナリスト Jon Kindervag 氏が 2009 年に策定したゼロトラストのセキュリティ フレームワーク[2]につながりました。ゼロトラストは、企業データに接続しているすべてのエンドポイントを信頼できないものとして扱い、ユーザーの正しい使用を検証するためにすべてのトラフィックを調査し、記録することを目標としています。

2011 年、Google 社は BeyondCorp という企業セキュリティ モデルを確立しました[3]。BeyondCorp は Google 社内の一施策としてスタートし、すべての社員が VPN を使用せずに、信頼できないネットワークからでも仕事できるようにしました。アクセス要件は、機密性のレベルに合わせた信頼の層にまとめられています。BeyondCorp では、モバイル端末は第一のプラットフォームとして扱われます。つまり、タスクを遂行するアクセスと機能が同じレベルでなければなりません。

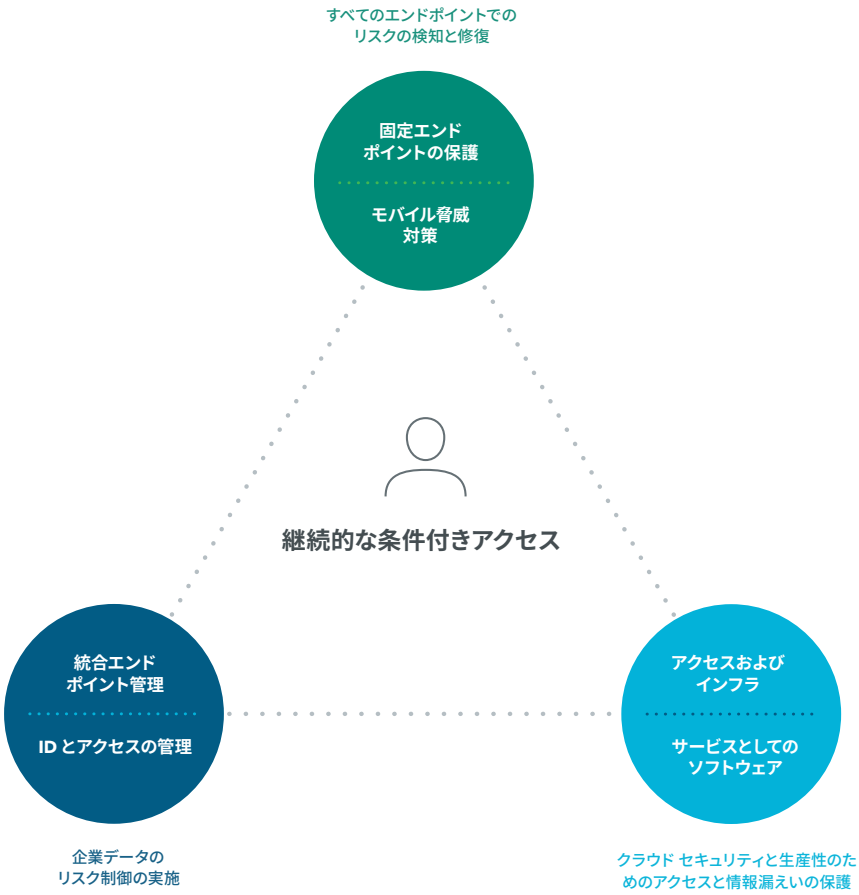
2017 年、ガートナー社の CARTA (Continuous Adaptive Risk and Trust Assessment) フレームワークは、ゼロトラストと BeyondCorp でさらに広がりました。ガートナー社によると、アクセスと保護のための最初のワンタイム ブロック/許可セキュリティ評価 (ログイン時など) には欠陥があり、企業がゼロデイ攻撃や標的型攻撃、資格情報の盗用、内部関係者による脅威に晒されています[4]。CARTA フレームワークの鍵となるものは、デジタル ビジネス エンティティとそのアクションの信頼性 (と危険性) は、静的なものではなく、動的なものであることであるという点です。インタラクションが発生し、さらにコンテキストを得る中で、信頼性は常に評価されます。

このようなモバイルとクラウド第一主義の世界における最新セキュリティの主な指針を基盤として、ポストペリメター セキュリティは、信頼できないエンドポイントが引き起こす動的なリスクに基づき、企業リソースに対する条件付きアクセスを継続的に確立し、しばしばサイバー攻撃の開始点となる、ユーザーに対して重要な保護を追加できるようなアーキテクチャを企業に提供しています。

ポストペリメター セキュリティの実現方法

ペリメター ベースのセキュリティ制御が及ばないアプリ、端末、ネットワークがある多くの IT 企業にとって、ゼロトラスト、BeyondCorp、CARTA を採用することは企業目標となっています。多くの企業にとって、ポストペリメター セキュリティを実現することは、既に配備されている既存のサービスを拡張し、統合することなのです。

ポストペリメター セキュリティを実現するために必要なもの



すべてのエンドポイントでのエンドポイント保護

エンドポイント保護の役割は、ユーザーの操作と端末が引き起こすリスクを判別し、確定することです。この新しいアーキテクチャでは、そのすべてが信頼できないものと見なされます。ユーザーはどの端末からでも企業アプリケーションにシームレスにアクセスできるため、このような保護を固定端末とモバイル端末の両方に広げる必要があります。また、エンドポイント保護は、ID とアクセス管理ソリューションなどのアクセス アービター、もしくはクラウドベース アプリケーション自体と統合し、許容できないリスクが生じた場合には修復措置を取るようにする必要があります。特定のシナリオでは、統合によってエンタープライズ モビリティ管理が提供する制御と連動して、修復措置を実施することができます。

クラウド セキュリティと生産性

クラウドサービスとインフラへの依存がさらに高まるにつれ、ホストされているアプリケーションとデータへの安全なアクセスを提供するニーズは頂点に達しています。クラウド セキュリティ ソリューションはホストされているデータとサービスに対して個別にアクセスと情報漏えいの保護を提供します。その他にも、クラウド サービス プロバイダーは ID およびアクセスの管理とエンドポイント保護と統合し、アクセス要求に関連する潜在的なリスクを具体化する必要があります。企業を装う悪意のあるサイトへのアクセスからユーザーを保護するには、適切なプロビジョニングをエンドポイント自体に組み込む必要があります。

ID とアクセスの管理

ID は「新しいペリメター」と見なされ、企業データへのアクセス権を付与する基盤となっています。ID プラットフォームは、シングル サインオンなどの機能によりアクセスを円滑化し、ユーザーが複数のアプリやサービスで仕事しやすくします。ID とアクセス管理のベンダーは、多要素認証などの重要なセキュリティ機能を活用してクラウドやオンプレミスのデータへのアクセスを保護するのと同時に、エンドポイント保護と統合し、信頼できない端末が引き起こすリスクを継続的に判別する必要があります。ID をエンドポイント保護と組み合わせることで、企業はユーザーと端末の両方の信頼性を継続的に評価することができます。

POST-PERIMETER SECURITY ALLIANCE

Post-Perimeter Security Alliance は、現代における境界のない、クラウド提供型の、プライバシー重視の世界に対応したセキュリティと生産性を提供するという共通のビジョンを持った大手のエンタープライズ ベンダーが参加しています。現在、エンドツーエンドのポストペリメター セキュリティを 1 つの企業で実現することは難しくなっています。代わりに、Alliance がエンドポイント、クラウド、ID の統合されたセキュリティ機能を提供することによって、望ましい生産性を実現し、企業データへのアクセスを保護します。Post-Perimeter Security Alliance が提供するソリューションが合わさって、社内データに対するリスクを継続的に評価し、そうしたリスクは発生した場合の修復と制御も行います。

Post-Perimeter Security Alliance のメンバーには、モバイル脅威検知、エンドポイント保護、ID とアクセスの管理、エンタープライズ モビリティ管理、クラウドベースの生産性向上のベンダーがいます。これらのベンダーはそれぞれの市場をリードする存在であることから、企業では既に自社の環境でこうしたベンダーのソリューションを 1 つ以上導入している可能性があります。いずれにせよ、多くの企業はポストペリメター セキュリティ戦略の道を歩み始めているのです。

「Post-Perimeter Security Alliance などの企業を超えた取り組みは、現在、大きな意味があります。ポストペリメター アーキテクチャを実装したくても、その全体的な仕組みがよくわからない企業に必要なガイドを提供できるからです 。」

– Phil Hochmuth 氏、プログラム ディレクター、
IDC 社、エンタープライズ モビリティ部門

[1] Putting the trust in zero trust:Post-perimeter security for a new age of work (2018 年 11 月 1 日)
出典元: https://www.lookout.com/info/lookout-post-perimeter-lp

[2] Getting Started with Zero Trust:Never trust, always verify
出典元: https://drive.google.com/file/d/1y_bexOdulUAr8M9wZxTqAGv21T3Vchor/view?ts=5c361c31

[3] Barclay Osborn、Justin McWilliams、Betsy Beyer、Max Saltonstall(2016 年春) BeyondCorp、Design to Deployment at Google
出典元: https://storage.googleapis.com/pub-tools-public-publication-data/pdf/44860.pdf

[4] ガートナー社、Seven Imperatives to Adopt a CARTA Strategic Approach (2018 年 4 月 10 日)
出典元 [要サブスクリプション]: https://www.gartner.com/doc/3871363/seven-imperatives-adopt-carta-strategic