Lookout®

ホワイトペーパー

ゼロトラスト環境で **信頼性**を確保する: 働き方新時代の ポストペリメター セキュリティ

企業をデータ漏洩や攻撃から守るための 3 つの懸案事項

1. 企業の境界は消えつつある。
2. 従来のセキュリティ技術が通用しない。
3. デバイスは信頼できない。

従業員が会社に管理されているデバイスも管理されていないデバイスも併用しているため、新たなセキュリティ アーキテクチャとして**ポストペリメター セキュリティ**へのニーズが高まっています。

問題:
企業の境界は消えつつある

仕事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それらのデータにアクセスできます。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参照やダウンロードするために、 VPN に接続する必要がない場合もあります。

「ガートナー社は 2020 年までに、労働者の業務の 80% がモバイル デバイスで行われると予想しています」

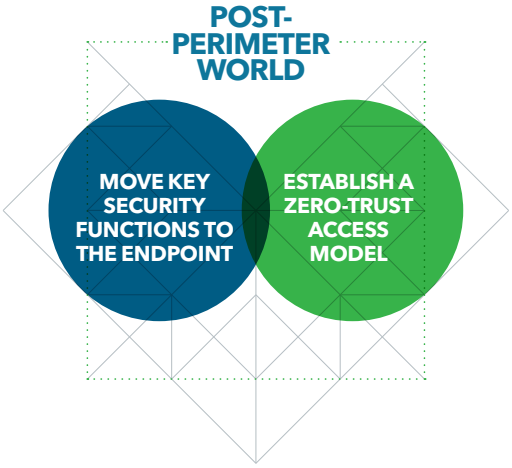
– ガートナー社「Prepare for Unified Endpoint Management to Displace MDM and CMT (MDM と CMT に置き換わる統一エンドポイント管理への準備)」 2018 年 6 月

また、フィッシングなどの攻撃も進化し、もはやペリメター セキュリティが通用しないという点に付け込むようになっています。さらに、現在では企業のデバイスも個人的なものになっています。ソーシャル メディア アプリやメッセージング アプリなどにより、従業員が個人的な活動を通じてフィッシング被害に遭い、企業の認証情報が盗まれやすい環境が生じています。2018 年の一定期間中に、セーフ ブラウジングを有効にしている Lookout ユーザーの 50.8% がフィッシング リンクに遭遇しています。

50.8% Safe Browsing 機能を有効にしている Lookout ユーザーがフィッシングリンクに直面した率（2018年現在）

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、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、もはやそうした場所に企業データは保管されていません。データは流動的に移動しており、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する

第一に、エンドポイントを従来のペリメター セキュリティの背後に隠す代わりに、セキュリティ自体をエンドポイントに移行する必要があります。城壁自体がすでに存在しない場合、城塞の前で防御を固めても意味はありません。セキュリティは、データが存在するあらゆる場所に配備すべきです。

ゼロトラストのアクセスモデルを確立する

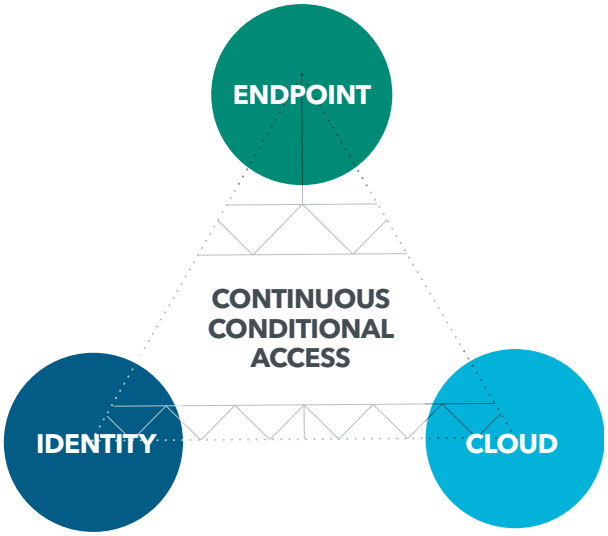
エンドポイントにセキュリティが装備されていていても、企業は有害性を実証しない限り、デバイスが無害であることを確認できません。この新たな世界では、企業データへのアクセスを許可するには、すべてのデバイスの健全性を定期的にチェックする必要があります。

「ゼロトラスト:この用語の出典は、2013 年のフォレスター社の NIST に関する調査文書 Developing a Framework to Improve Critical Infrastructure Cybersecurity (重要なインフラストラクチャのサイバー セキュリティを改善するためのフレームワークの開発) です。この調査自体は、Jerricho Forum 社が 2004 年から開始したペリメターレス化に関する初期の調査に基づいています。」

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。ポストペリメター セキュリティの中心となるのは、それぞれがパズルのようにつながった、次の 3 つの機能です。

- エンドポイント保護
- クラウドへのアクセス
- ID 管理



エンドポイント保護ソリューションを使用してデバイス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、デバイス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。次にこのソリューションは、従業員のデバイスが、認証を受け、企業のリソースにアクセスするのに相応しい健全性を保持しているかどうかを判断します。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、企業のクラウドやインターネットへのアクセスを総合的に保護することは、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、最初に移行する必要があります。

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、新たなリスクが検出されると、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 ID に代わり、管理対象デバイスなどを対象とした Enterprise Mobility Management (EMM) や、Mobile Application Management (MAM) で管理されます。

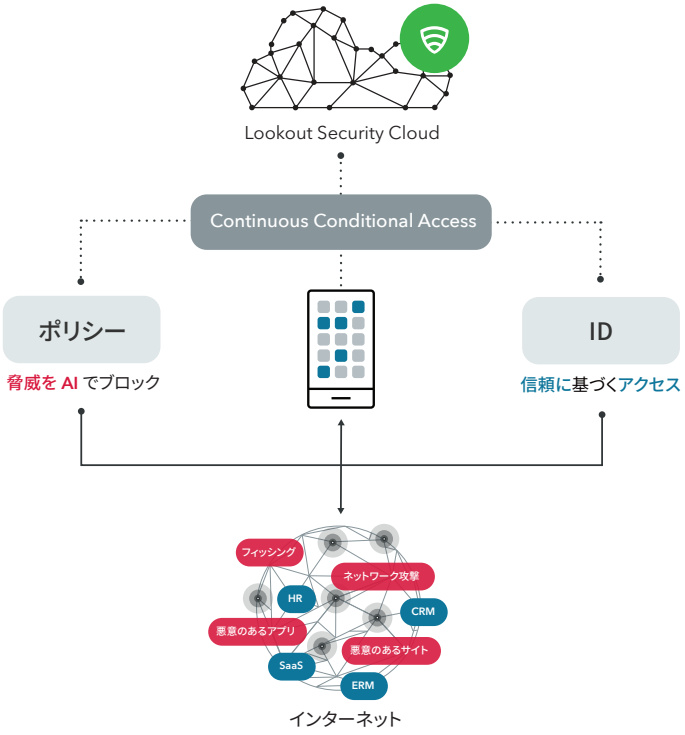
Continuous Conditional Access

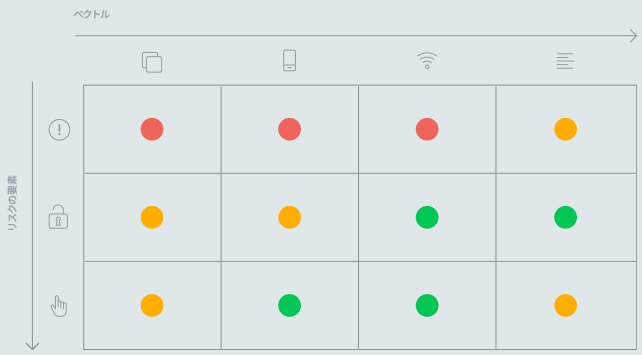
継続的なリスクの評価と、その評価を利用したリソースへのアクセス制御を、「Continuous Conditional Access(CCA: 継続した条件付きアクセス)」と呼びます。つまり、ポストペリメター セキュリティの 3 つの柱は、企業のリスク レベルを超えないように、常に監視しています。リスク レベルを超えた場合、アクセスが拒否されることによって、企業リソースが保護されます。

ソリューション: LOOKOUT によるポストペリメターセキュリティの実現方法

Lookout のプラットフォームは、企業がポストペリメター セキュリティを実際に全従業員に適用できるよう設計されています。

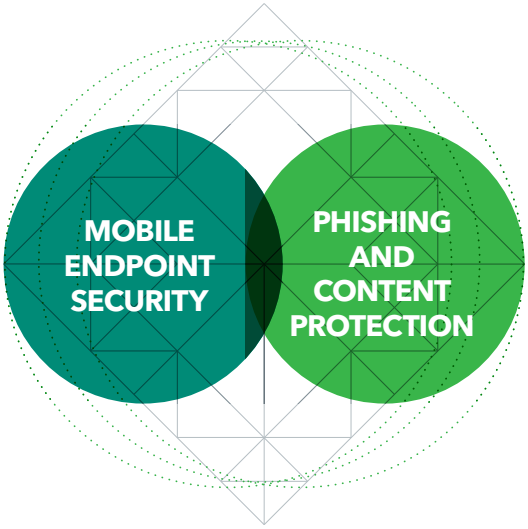
基盤となるのは、世界中の 1 億 7 千万のデバイスと 7 千万のアプリから得られた、Lookout のセキュリティ テレメトリー データセットです。このデータセットに基づき、デバイス、ネットワーク、アプリ、コンテンツに対する脅威やリスクなど、リスクのあらゆる側面を前例のない深さで見極められます。それにより、従業員のデバイスで起きる潜在的に有害なシナリオを、いつ何時でも直ちに企業に提示できるのです。





モバイル リスクはあらゆる企業に影響を及ぼします。「モバイル リスク マトリクス」では、企業のリスク許容度について説明します。

詳細を見る



Mobile Endpoint Security を使用

企業は、Lookout Mobile Endpoint Security を使用して、あらゆるデバイスに対して企業データへの継続的な条件付きアクセスを許可することができます。そうすることで、企業リソースへのアクセスの認証前と、アクセス中のいずれにおいても、ポリシーが常時適用され、デバイスの健全性が検証されることになります。

企業は、デバイスを社内および社外の必須条件に確実に準拠させるポリシーを、そのリスク許容度に応じて選択することができます。企業が定義したリスクの許容レベルをデバイスが超えた場合、Lookout は従業員に修復を促すメッセージを送信し、Lookout Mobile Endpoint Security コンソールで管理者に問題を通知し、企業リソースからその従業員をログアウトします。

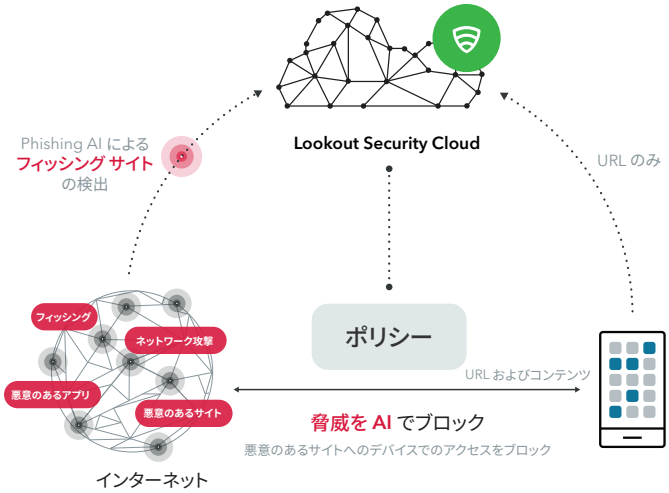
従業員は、デバイスが (通常は従業員自身による修復により) リスクの許容レベルまで戻った場合に限り、企業リソースへの認証を許可されます。

デバイスの健全性が保たれていれば、従業員は企業リソースに自由にアクセスすることができます。

Phishing and Content Protection を使用

これまで、企業はフィッシング リスクの軽減に、電子メール セキュリティと境界のゲートウェイに頼っていました。電子メール セキュリティは現在のセキュリティ アーキテクチャでも引き続き利用されていますが、問題は残っています。従業員が境界外にあるデバイスから電子メール以外のアプリケーションを使用してデータにアクセスするようになり、こうしたテクノロジーでは不十分になっています。

これが、セキュリティをエンドポイントに移行しなければならない主な理由の 1 つです。Lookout Phishing and Content Protection はデバイス上にあり、ソーシャル メディア アプリ、メッセージング アプリ、SMS をはじめとする、ネットワークに接続するすべてのアプリを含む、さまざまなベクトルからのフィッシング攻撃を監視します。



Lookout の人工知能による検出エンジンは、インターネット上のサイトのレピュテーションを積極的に判別します。Lookout Phishing AI は、常時稼働のこの方法によって、ユーザーが標的になり、攻撃が実施される前に、構築段階のフィッシング キットを検出します。検出した主な攻撃については、@PhishingAI で共有します。

「モバイルエンドポイントのセキュリティ保護は、我社にとっての最優先課題です。我社にとって Lookout は、企業データを侵害から守り、かつすべてのプライバシー保護法を遵守するために、絶対に不可欠な保護層です。」

Christian Jösch、Simon Hegle ネットワーク管理者

2018 年のモバイル フィッシング:
現代のあらゆる企業が直面している迷信と事実

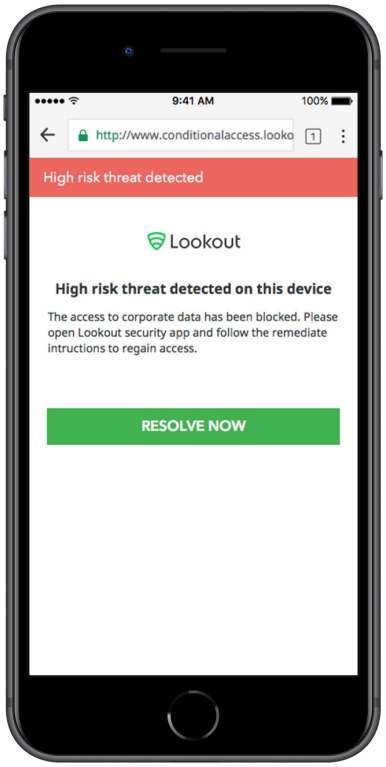
レポートをダウンロード

結果:
管理されていてもいなくても安全な新たな世界

人々の労働は変化しています。IDC (International Data Corporation) によると、「大規模な米国企業の従業員が「モバイル」を検討する割合は、12 から 18 カ月後には、現在の 35% から 43% に増加すると見込まれます」[1]

データを保存する方法、従業員の行動様式、企業のリソースに接続する無数のデバイスは、いずれも急激に変化しているデジタル変革の要因であり、企業はこれに進んで取り組む必要があります。「モバイル エンドポイント」は瞬く間に従業員が作業を行うあらゆるデバイスを指す言葉として認識されるようになりました。

これまでの境界は消えつつあります。従来のセキュリティ技術は通用しなくなりました。こうした新たな時代の渦中で、デバイス自体が信頼できなくても、企業のリソースを保護する方法があります。ポストペリメター セキュリティは、新時代の仕事における重要かつ中心的なアーキテクチャです。



[1]ソース:IDC、The State of Mobile Enterprise Devices in 2018:An IDC Survey of Devices, Decisions, and Deployments, forthcoming October 2018
(2018 年のモバイル エンタープライズ デバイスの状況: 2018 年 10 月に予定されているデバイス、意思決定、および開発に関する IDC の調査)