Lookout

LOOKOUT MOBILE ENDPOINT SECURITY

場所に依存せず、あなたのデバイスを保護します

最も活用している端末を見過ごさない

従来型のサイバーセキュリティ戦略では、サーバー、ラップトップ、デスクトップなど、固定エンドポイントをサーバー脅威から保護することに焦点を当ててきました。しかし、セキュリティで求められていることは、時の経過とともに実質的に増えてきています。

モバイル端末のセキュリティの問題はしばしば見過ごされ、それがセキュリティ アーキテクチャーにギャップを生じさせる原因となっています。モバイル オペレーティング システムは回復力が比較的高いと考えられてはいるものの、サイバー攻撃の標的にされることが増えています。モバイル端末は個人でも仕事でも使われているからです。このような端末はデータの宝庫であり、攻撃者はこれを組織への侵入の入り口として利用します。

モバイルセキュリティソリューションを導入する際に、包括的なプラットフォームにするか、最善のソリューションの組み合わせにするか、という選択を迫られます。モバイル端末の増加は接続先となるクラウドの成長に従い起きているため、エンドポイントからクラウドまでをカバーする1つのセキュリティソリューションを利用したほうが、スタンドアロンのソリューションを集めた場合に比べ、ユーザの自由度を犠牲にせずに使い勝手と利便性を高め、運用コストの低減にもつながります。

メリット

- クラウド提供のモバイル セキュリティ
- iOS、Android、Chrome OS を保護
- 脅威研究者により構築されたエンドポイントの検出と応答
- プロセッサー パフォーマンスとバッテリー寿命を延ばすために最適化された軽量アプリ
- 企業所有端末と従業員所有端末を保護
- ユーザーのプライバシーを保護しながらコンプライアンス要件を満たす
- すべての従業員の端末にスムーズに展開
- 数十万のエンドポイントを擁するモバイル フリートにスケーリング可能

今日、従業員が組織のデータへのアクセスに使用する端末の半数以上が iOS、Android、Chrome OS で稼働しています。

モバイルによって開かれた新たなサイバー犯罪の機会

モバイル端末を保護することは、デスクトップやラップトップの保護とは全く異なります。モバイル端末における脅威はデスクトップでの脅威とよく似ていますが、保護のためのアプローチは異なります。その結果、モバイル フリートにより生じた新しいセキュリティ要件に対応する必要があります。

モバイルのリスクには最新のエンドポイント保護が必要

モバイル オペレーティング システムは回復力が高いものの、サイバー攻撃の標的にされることが増えています。個人生活でも仕事でも使われているからです。iOS、Android、Chrome OS の端末はデータの宝庫であり、攻撃者はこれを組織への侵入の入り口として標的にします。

一般的な攻撃ベクトルでは、スパイウェア、バンキング トロイの木馬、ルートキットなどのモバイル マルウェアが利用されています。マルウェアは、モバイル端末の通信回線、WiFi、Bluetooth のいずれの接続でも配信可能です。一旦マルウェアが実行されると、モバイル端末の全体的な安全性がむしばまれます。

最新のエンドポイント保護では、アプリ、端末、ネットワーク接続の脅威を検出しなければなりません。ユーザー、端末、そして会社を、プライバシーに配慮しながら保護する必要があります。そして、従業員所有の端末にも企業所有の端末にも同様に機能する必要があります。

> 「モバイル セキュリティは規制の厳しい業界や官庁組織のためのツールから、すべての組織の基本的なセキュリティ ソリューションへと発展してきました。」
>
> - **Phil Hochmuth** 氏、IDC 社、
> エンタープライズ モビリティ部門、
> プログラム担当副社長。

モバイル フィッシングを攻撃者のエントリ ポイントにさせない

モバイル端末での従来型のアンチフィッシング アプローチでは、すぐにプライバシーが問題になります。攻撃をブロックするためにメール メッセージを調べるからです。すべてのモバイル端末は、企業が支給したものであっても、個人端末と見なされます。メール コンテンツを調べるだけでは、モバイル ユーザーにフィッシング リンクを送信するために使用されるその他の方法を見過ごしてしまいます。

ほとんどのアンチフィッシング ソリューションは、悪意のあるドメインと Web アドレスのリストに依存しています。ところが、毎月 150 万を超えるモバイル フィッシング サイトが作られています。そのほとんどは、ほんの数時間あるいは数日のうちに構築されては破棄されています。モバイル フィッシング攻撃の検出をレピュテーションベースの方法だけに頼っているのでは不十分です。

> 50 人の企業ユーザーのうち 1 人が毎日モバイルでフィッシングに遭遇しており、モバイル攻撃の 87% はメール以外で発生しています。

適切なアプリと OS バージョンを把握し、確実にパッチを適用することが必要

これまでの脆弱性とパッチ管理は、エンドポイントではなくサーバーに焦点を当てていました。デスクトップとラップトップは管理され、共通のイメージが利用され、定期的にパッチが適用されていたからです。それで、主な脆弱性リスクはパッチが適用されていないサーバーにありました。

現在、モバイル端末管理 (MDM) を使用しても、モバイル端末で最低バージョンのオペレーティング システムが稼働していることを確認することしかできません。しかし、従業員は管理されていない個人のスマートフォンやタブレットをますます仕事に使用するようになり、MDM では完全にはカバーできないのです。従来型の脆弱性管理は、端末が自宅の WiFi や通信回線ではなくオフィスのネットワークに接続されていることを前提としているので、このギャップを埋められません。

> フィナンシャル タイムズ誌はある WhatsApp の脆弱性について報告しました。ユーザーの介入なしに iOS と Android の端末にスパイウェアを配信できるというものです。ユーザーが反応しなくても、端末は侵害される可能性があります。[1]

1. Srivastava, Mehul, Financial Times, 'WhatsApp voice calls used to inject Israeli spyware on phones', May 13, 2019

モバイルをゼロ トラスト ネットワーク アーキテクチャーに組み込むことが必要

スマートフォンとタブレットによる自由は、リスクももたらします。今や私たち一人ひとりが、セキュリティ保護が必要なリモート オフィス ネットワークとなっているのです。従来の境界セキュリティの外側で仕事を続ければ、誰をそしてどの端末を信頼できるかに関して何の保証もありません。

モバイル ユーザーは VPN を使用せずにクラウド内の組織のデータに接続しています。これらのユーザーはその場所からアクセスする必要があり、あなたは彼らが機密データをリスクにさらさないことを保証する必要があります。リスクの低い端末だけに、組織のリソースへのアクセスを許可してください。アクセス権が付与された後もリスク評価を継続的に行うことにより、データを保護するためアクセス権を動的に変更できます。

「個人端末のユーザー認証 — ZTNA [Zero Trust network access] は、セキュリティを向上させ、フルマネジメントの要件を少なくし、よりセキュアな直接アプリケーション アクセスが可能にすることで、BYOD プログラムをシンプルにすることができる。」[2]

アプリに対する可視性を高めてリスクを減らす

多くの組織ではデスクトップとラップトップのアプリケーションがデータを扱う方法に対する可視性は得られていますが、モバイル端末に関してはそうではありません。iOS、Android、Chrome OS ではそれぞれアプリの実行方法が異なり、それらを調べるのは難題になります。そのようなインサイトがなければ、これらのアプリが組織のデータをどのように扱っているかをセキュリティ チームが把握することはないでしょう。

マネージド デバイスでは、モバイル端末管理 (MDM) やモバイルアプリ管理 (MAM) を通して、従業員が使用しているアプリに対する可視性と制御は得られます。しかし、リアルタイムのアプリ アクセス許可とデータ アクセス制御に対するインサイトは提供されません。個人の管理されていない端末では、MDM と MAM から得られる限定された可視性さえ得られません。

「2022 年までに企業で利用されているスマートフォンの 75% は個人所有の機器の持ち込み (BYOD) になり、端末中心の管理からアプリとデータ中心の管理に移行せざるを得なくなるでしょう。」[3]

ツールを使って侵害を防止し、インシデントを検出して対応する

多くの組織ではサーバー、デスクトップ、ラップトップ コンピューターに対する包括的アクティビティー モニタリングを行っていますが、iOS、Android、Chrome OS の端末に対して同じテレメトリを持つことはできていません。従業員が仕事でモバイル端末を使用することが増えるにつれ、それらの端末への攻撃も増加してきています。

データ侵害を効果的に食い止めるために、セキュリティ チームはサーバー、デスクトップ、ラップトップに関して持っているデータと同じような包括的なデータをモバイル端末に関して必要とします。モバイル オペレーティング システムでは、決してカーネル アクセスは許可されず、アプリは独立した状態で動作しなければなりません。このことから、包括的テレメトリの収集は不可能だと誤って認識されてきました。

2023 年の終わりまでに 50% を超える企業で、古いアンチウイルス製品が、検出と応答の機能を備えた防止機能を補う EPP と EDR ソリューションに置き換わるでしょう。[4]

モバイル セキュリティにはより広範なセキュリティ アーキテクチャーとの統合が必要

従業員のモバイル端末をモバイル端末管理 (MDM) や統合エンドポイント管理 (UEM) などのツールで管理している組織もあります。セキュリティ情報とイベント管理 (SIEM) も活用して脅威インテリジェンスを収集しています。MDM/UEM と SIEM にあらかじめ統合されていれば、モバイル セキュリティ ソリューションからすぐに価値を最大限に引き出せます。

2. Gartner “Market Guide for Zero Trust Network Access,” Steve Riley, Neil MacDonald, Lawrence Orans, June 2020
3. Gartner “Define BYOD Ownership and Support Expectations in Contracts to Ensure Successful Implementation,” DD Mishra, David Ackerman, 3 July 2019
4. Gartner, “Market Guide for Endpoint Detection and Response Solutions,” Paul Webber, Prateek Bhajanka, Mark Harris, Brad LaPorte, December 2019

「モバイル セキュリティ市場は、ベスト・オブ・ブリードの脅威防止や修復ではなく (こうしたコア機能も確かに重要ですが)、パートナーシップ、統合、エコシステムがすべてです。携帯電話会社などの主要チャネルとの強力なパートナーシップや、EMM/SIEM プラットフォームとの強力な統合性を持つベンダーに注目してください」。

- **Phil Hochmuth** 氏、IDC 社、エンタープライズ モビリティ部門、プログラム担当副社長。

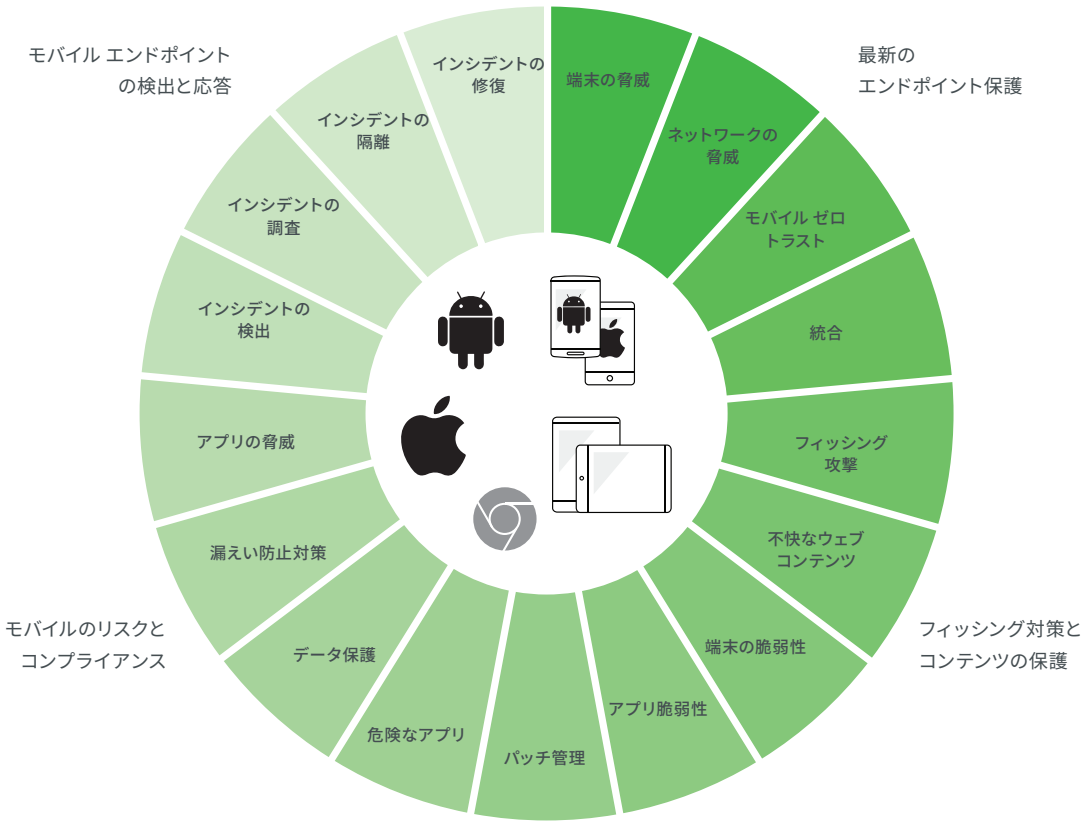
モバイル向けにゼロから構築されたエンドポイント セキュリティ

Lookout Mobile Endpoint Security (MES) は、進化し続けるモバイル セキュリティ要件に対応しています。Lookout MES は Lookout Security Graph を搭載し、数十万のエンドポイントにスケーリングします。そのクラウド モジュールにより、Mobile Endpoint Security をお客様のニーズに合わせてカスタマイズできます。

人工知能を搭載した Security Graph は、既知および未知の脅威からお客様を守ります。Lookout には、2 億台以上の端末と 1 億 3,500 万以上のアプリを分析した最大のモバイル データセットがあります。当社のアルゴリズムは、毎日インターネットを検索して、フィッシングを目的としたウェブサイトを見つけ出し、当社の API を介して無数のカスタム アプリケーションを分析しています。

新しいマルウェアの入ったアプリをダウンロードしたり、最新のランサムウェアやフィッシング詐欺の標的になったりしてしまっても、指一本動かすことなく保護されます。脅威や攻撃が発生した際には、何が起きているのか、どうすれば解決できるのかを調査するための手順をお知らせします。

Lookout Mobile Endpoint Security



Lookout について

Lookout はエンドポイントからクラウドまでカバーする統合型セキュリティを提供する会社です。当社の使命は、仕事と遊びのどちらにおいてもこのような端末が必要不可欠であるプライバシー重視の社会で、デジタルの未来のセキュリティを保護すること、およびより強力なデジタルの未来を実現することです。当社の製品は、消費者と従業員がデータを保護し、プライバシーや信頼を損なわずに安全な接続を維持できるようにします。Lookout は、何百万もの利用者、大企業、公的機関、さらには AT&T、Verizon、Vodafone、Microsoft、Google、Apple などのパートナーからの信頼を得ています。Lookout の本社はサンフランシスコにあり、アムステルダム、ボストン、ロンドン、シドニー、東京、トロント、ワシントン D.C. にもオフィスを構えています。Lookout の詳細は弊社ホームページ (**www.lookout.com/jp**) をご覧ください。また、**ブログ**、**LinkedIn**、**Twitter** で Lookout をフォローすることも可能です。

詳細については、
lookout.com
をご覧ください。

以下からデモのリクエストが可能です:
lookout.com/request-a-demo

エンドポイントからクラウドまでカバーする統合型セキュリティ

lookout.com で詳細をご覧ください

Lookout®