



LOOKOUT SASE ソリューション

エンドポイントからクラウドまでカバーするセキュリティにより、
安全なリモートワークを実現する

ユーザー、アプリ、データはもうオフィスビルにはいない

以前は、アプリとデータはデータセンターに置かれていて、皆オフィスで働いていました。アクセスするため、全従業員は企業が支給したラップトップかデスクトップを使用して社内ネットワークに接続しました。セキュリティ境界で困うことにより、データフローを制御し、組織のデータを保護できていました。エンドポイントは管理されていたので、そこに格納されているものも把握していました。

このすべてはクラウドテクノロジーとリモートワークで変化しました。今日、データは必要な場所であれば、どこにでも移動します。従業員は、どこからでも、どの端末でも、なんであれ必要なものに簡単にアクセスできることを期待しています。飛躍的に増えているコラボレーションを活用するには、組織はクラウドを受け入れるときにセキュリティ態勢を緩めなければならないと感じました。しかし、アプリとデータはオフィスから離れたからといって、監視を緩めていいわけではありません。

5か所の企業拠点から5,000か所のリモートオフィスへ

多くの組織は仮想プライベートネットワーク (VPN) に投資して、リモートワーカーをサポートしています。そうすればどこからでもオンプレミスのアプリにアクセスできますが、これはすべてのユーザーと端末が信頼できるものとみなしています。さらに、VPNは接続する誰に対しても内部ネットワークへの無制限アクセスを提供するので、インフラストラクチャー全体がリスクにさらされます。

データの安全を保持しながらコラボレーションを促進するには、完全な可視性と動的アクセス制御が必要です。ここで、Secure Access Service Edge (SASE) と呼ばれる新しいフレームワークが必要になります。これにより、境界で困っていたときと同様の保護がクラウドで実現します。

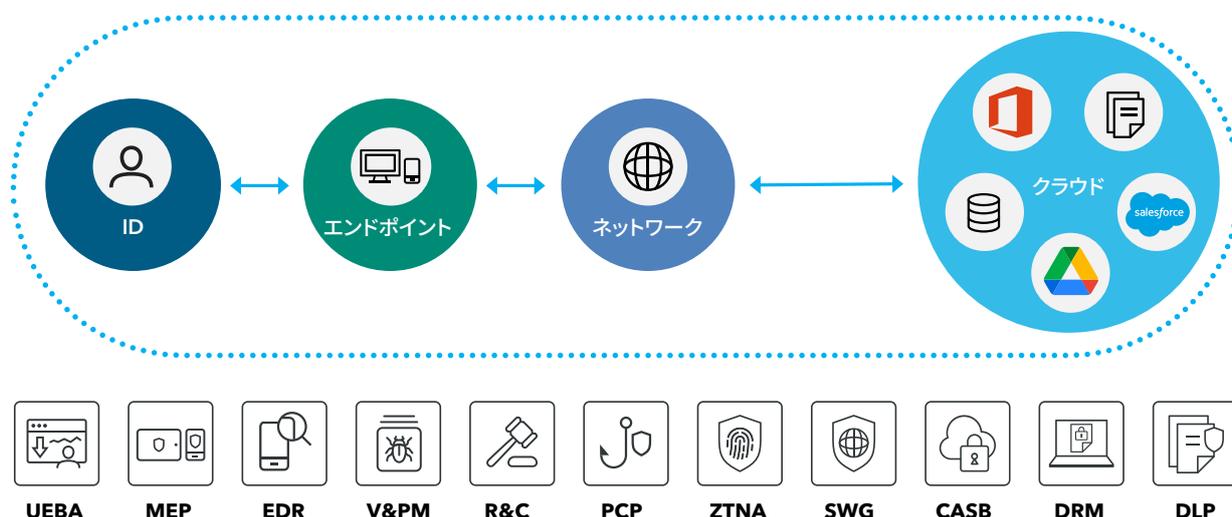
専用 SASE ベンダーは脅威に対するネットワークベースのインサイトのみを提供し、エンドポイントのセキュリティ体制に対して得られる可視性は限定的なものです。つまり、エンドポイント機能が欠けており、エンドポイントからクラウドまで組織を効果的に保護するために必要なもののごく一部しか備えていないのです。既存の SASE テクノロジーは侵襲的でもあり、とりわけ個人の端末での作業時に、ユーザーが望んでいるプライバシーと競合してしまいます。

エンドポイントからクラウドまでカバーする統合型のソリューションが必要

現状では、エンドポイントからクラウドまでカバーするセキュリティを求めるなら、特定の問題を解決するスタンドアロン ツールを複数購入する必要があります。でも、それでは複雑で非効率です。全体的なデータ セキュリティにも対応しません。

Lookout は 1 つのセキュリティ プラットフォームを提供し、個人のプライバシーに配慮した方法でエンドポイントからクラウドまでデータを保護します。当社の統合型ソリューションは次のようなものです。

1. 完全なインサイトに基づいて動的アクセスを提供する精確な制御
2. ユーザー、エンドポイント、アプリ、データへの完全な可視性
3. データがどこに移動し、どのように扱われているかに関わらず保護する
4. 1 か所で緻密なポリシーを施行して、脅威を検出し、調査を実施
5. 個人のプライバシーに配慮



境界で困っているときと同様の可視性

データ保護の第 1 ステップは何が起きているかを把握することです。ユーザーが散らばっていて、制御されていないネットワークを使用してクラウドのアプリやデータにアクセスしているなら、直面しているリスクを理解するのは難しくなります。管理対象のエンドポイントと管理されていないエンドポイントで、クラウドで、そしてその間のどこでも、何が起きているかを理解できる可視性を与えることにより、推量を排除します。

端末、アプリ、データを深く調査するよりも、挙動を分析することによりインサイダーの脅威とファイルレス サイバー攻撃を検出します。

インフラストラクチャー内のユーザーの異常な動作（データの共有、ダウンロード、削除など）を理解することにより、悪意のあるインサイダーによる疑わしいアクティビティを簡単に突き止めることができます。データがデータセンター、パブリック クラウド、マルチクラウド環境のいずれに格納されているかに関わらず、当社はデータへの深い知識を有しています。エンドポイントのリスク レベルも継続的にモニタリングするので、アクセスを動的に変更してデータを保護することができます。このデータをアプリ、端末、ネットワークの脅威検出と組み合わせて、すべてのエンドポイントにわたる最も包括的なセキュリティ態勢を実現することができます。

統一されたインサイトですべてを解明する

スタンドアロン ツールはサイバーセキュリティを不必要に複雑で非効率的なものにします。複数のソリューションを管理すると、チームがミスをして、セキュリティ ポリシーの不整合も見逃してしまうかもしれません。当社の統合型プラットフォームでは、ユーザー、エンドポイント、アプリ、データ全体にわたる実用的なインサイトを提供します。

あらゆる組織で、Microsoft 365 や Google Workspace などの生産性スイート、Salesforce のような顧客関係管理、Workday のような人事関連のアプリなど、数え切れないアプリとクラウド プラットフォームを利用して従業員をサポートするようになっています。すべてを 1 か所にまとめて、一貫性のあるセキュリティ ポリシーを施行すれば、トータル コントロールを確実に保持できます。すべてのクラウド アプリとプラットフォームで生じていることに対して可視性を得られるので、異常、悪意のある動作、脆弱性を特定できます。これには、悪意のあるサードパーティ統合や、アプリのコードに深く埋め込まれたライブラリが含まれます。データが扱われる方法、格納される方法、転送される方法も把握しているので、データを動的に保護できます。

脅威を突き止め、高度なサイバー攻撃に対する科学調査を実施するために必要なすべてのテレメトリ データも提供します。注目する問題に注意を促すためのアラートを即時で受け取ります。管理者は異常なイベントや疑わしいアクティビティに対する通知をカスタマイズできます。集計レポートにより、すべての端末、ネットワーク接続、クラウド サービスにまたがる広範な監査証跡を確認できるので、インシデントがどこでどのように起きたのか正確に突き止めるのが容易になります。

動的なセキュア アクセスとコラボレーションのための精確な制御

従業員はいつでもどこからでも仕事をしたいと思っているので、クラウドやオンプレミスにある企業データへのアクセスをオール オア ナッシング方式にすると、不必要なリスクが生じます。データを保護するには、ユーザー、エンドポイント、アプリとのすべてのインタラクションをセキュリティ保護する必要があります。すべてのものへの完全な可視性、統一されたインサイト、そして統合型の制御があれば、精確なアクセスを細かく調整して、シームレスで効率的な接続とコラボレーションを提供することができます。

端末にマルウェアがインストールされたかどうか、ユーザーが職務に関係のない機密データにアクセスしているかどうかなど、各ユーザーのリスク態勢にマッチする、きめ細やかで動的なアクセスを実現します。当社の製品は、お客様の従業員が仕事に必要なアプリとデータを把握しています。結果として、境界内のエンタープライズ アプリケーション、プライベート クラウド、クラウド アプリケーションのいずれに格納されていても、従業員は必要とするデータに、安全かつ動的にアクセスすることができます。

セキュリティのために生産性が妨げられたり、ユーザーのエクスペリエンスが損なわれたりするべきでもありません。当社の製品にはお客様のデータに対する深い知識があるので、お客様の組織全体にシームレスなデータ保護を拡張することができます。ワークフローが妨げられないようにします。保存中、転送中、使用中のデータを暗号化するので、お客様は最も強力なセキュリティ要件に対応しつつ、ユーザーのオンラインとオフラインのアクセスも同時に提供することができますようになります。ダウンロード中の機密データも暗号化できるので、不正アクセスを防止するデジタル著作権管理を実施することもできます。

エンドポイントからクラウドまでカバーするセキュリティで、どこにいても仕事ができる

デジタル コラボレーションが飛躍的に増加し、データは必要とされればどこにでも移動するようになりました。データをリスクにさらさずにこの強化された生産性を活用するには、どのネットワークを使用し、どのアプリケーションに接続していても、あらゆるエンドポイントを保護することが必要です。Lookout はエンドポイント セキュリティと SASE を統合しているので、個人のプライバシーに配慮した方法でエンドポイントからクラウドまでデータを保護します。

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

© 2021 Lookout, Inc. LOOKOUT®, the Lookout Shield Design®, LOOKOUT with Shield Design®, SCREAM®, SIGNAL FLARE® は、Lookout, Inc. の米国およびその他の国における登録商標です。EVERYTHING IS OK®, LOOKOUT MOBILE SECURITY®, POWERED BY LOOKOUT®, PROTECTED BY LOOKOUT®, は、Lookout Inc. の米国における登録商標です。POST PERIMETER SECURITY ALLIANCE™, DAY OF SHECURITY™ は Lookout, Inc. の商標です。その他すべてのブランドおよび製品名は、それぞれの所有者の商標または登録商標です。20210415-Lookout-JPv1.0