Lookout

エンドポイントから クラウドまで、企業の アプリとデータを保護する

LOOKOUT CLOUD ACCESS SECURE BROKER は 完全な可視化と制御によりあなたのデータを保護します

クラウド フットプリントの拡大によってもたらされたセキュリティ上の課題

新しい働き方の発展により、同僚、契約社員、パートナーとのコラボレーションはクラウドサービスに依存しています。クリエイティブな仕事をするのに必要なデータへのアクセスができるようになり、自分が作業をしている場所や、どんなデバイスを使って作業をしているかはもはや問題ではありません。

飛躍的にコラボレーションが拡大していく中で、必要に応じ企業のデータは次々と姿を変えて移動していきます。従業員はあらゆる場所から作業を行い、時には企業の管理ができない社外のネットワークとデバイスを利用してコラボレーションが行われることもあります。さらに、生活する上で必要となる雑事をこなすために企業用のクラウドアプリだけでなく、個人用のアプリも同じ環境では利用されています。

クラウドに移行しても可視性と制御を維持する

会社がクラウドでコラボレーションしているなら、データを保護しながら、コンプライアンスが取れていることを確かめる必要があります。適切な人物だけがアクセス権を持つようにするには、データとユーザーがどのように行動するかに対する複雑な知識が必要です。

使われている端末やクラウドに関わらず、過剰なログイン試行や大量のダウンロードなどの疑わしいアクティビティーを指摘できる必要があります。同様に、複数のクラウドにまたがってデータを見つけ、分類し、漏えいを防げるようにすることも必要です。このように、境界の無いクラウド環境でも、境界型防御で行っていたようなセキュリティの可視化と制御を実現する必要があります。

メリット

- クラウドとプライベートのすべてのアプリに対するセキュリティ ガバナンスの簡素化
- Google Workspace や Microsoft 365 などのコラボレーションツールとの統合
- マルチクラウド環境での広範囲に及びデータ検出機能
- 高度な分類およびデータ損失防止 (DLP) を利用したデータの保護
- 暗号化と権利管理による、社外共有したデータの保護と制御
- UEBA(User and Entity Behavior Analytics)による内部脅威の検出
- クラウドのインフラストラクチャーとアプリケーションのセキュリティ体制の管理

データ保存クラウドに依存しないアクセス制御

データを誰がどのように利用し、どのクラウドサービスを通って流れているかに関わりなく、データを継続して追跡可能なセキュリティが必要です。Lookout CASB により、シングルコンソールでクラウド上のデータとアプリの状況を把握することができ、これにより状況を的確に把握することができます。

ユーザーの行動とユーザーがアクセスしたり共有したりするデータのタイプを深く理解することにより、精確なアクセスを動的に微調整できるようになります。フォワードプロキシとリバースプロキシの最適な組み合わせにより、エンドポイントとアプリ インスタンスを自社で管理してるかどうかに関わらず、すべてを制御できるようにします。さらに、Lookout CASB は Enterprise Mobility Management (EMM) ソリューションと統合して、エンドポイントでのアクセス ポリシーを施行します。さらに、マルチクラウド環境にまたがって制御を維持することを保証します。こうして、データを扱う方法を制限することにより、コンプライアンス条件を満たし、機密性の高い知的財産を保護します。

コンテキスト認識属性のセレクション		
• ユーザー • ユーザー グループ • IP アドレス	• 場所 • 端末タイプ • オペレーティング システム	• ユーザーの動作 • 端末コンプライアンス • IP リスク

所有データ、保存場所、保護状況の把握

クラウド サービスとデータへのアクセスを制御することは第一段階です。所有しているデータと、その位置、保護方法を把握することも必要です。Lookout CASB により、クラウドサービス、ユーザー、端末のすべてにわたってデータの場所を識別することができます。リアルタイムでデータを分類し、最高レベルの暗号化を使用して保護します。

Lookout は履歴データをスキャンすることで、保護されていない情報や意図せず公開されているファイル共有を検出し、潜在的なデータ漏洩を防止します。一元的なデータ損失防止 (DLP) ポリシーを利用して、クラウド展開、メール、アプリケーション全体にわたって一貫性のある方法で、機密性の高いデータを検出し、分類し、保護できます。これにより、Personally identifiable information (PII)、Protected Health Information (PHI)、および Payment Card Industry (PCI) として分類された情報などの規制データの整合性を維持しながら、シームレスなコラボレーションが可能になります。

組織ではエンタープライズ デジタル著作権管理 (E-DRM) を施行して、オフラインでの情報交換とファイル共有をセキュリティ保護できます。機密性レベルに基づいて、Lookout E-DRM では機密性の高いファイルをダウンロード中に自動的に暗号化し、承認されたユーザーのみにそれらのファイルにアクセスするための有効な暗号解除キーの利用を許可します。

サイバー脅威の検出と修復

クラウドには価値の高いデータがあるので、サーバー攻撃のターゲットになる可能性が高くなっています。さらに、API により、従来型のネットワーク アンチウイルス システムをバイパスして隣接クラウド サービスへの水平移動が可能です。Lookout CASB は、すべてのインバウンドとアウトバウンドのコンテンツをスキャンし、ウイルス、マルウェア、ランサムウェアを検出して停止します。Lookout は、認識可能な遅延を加えずに、感染したコンテンツをその場で隔離します。

Lookout UEBA (User and Entity Behavior Analytics) は、ユーザー、端末、アクティビティーを継続的に評価し、異常な動作を検出して潜在的な脅威を修復します。例としては、過剰なファイルのダウンロード、ユーザーからのログイン試行、承認されていないアカウントによる持続的なログイン試行などがあります。

クラウドのセキュリティ構成を理解する

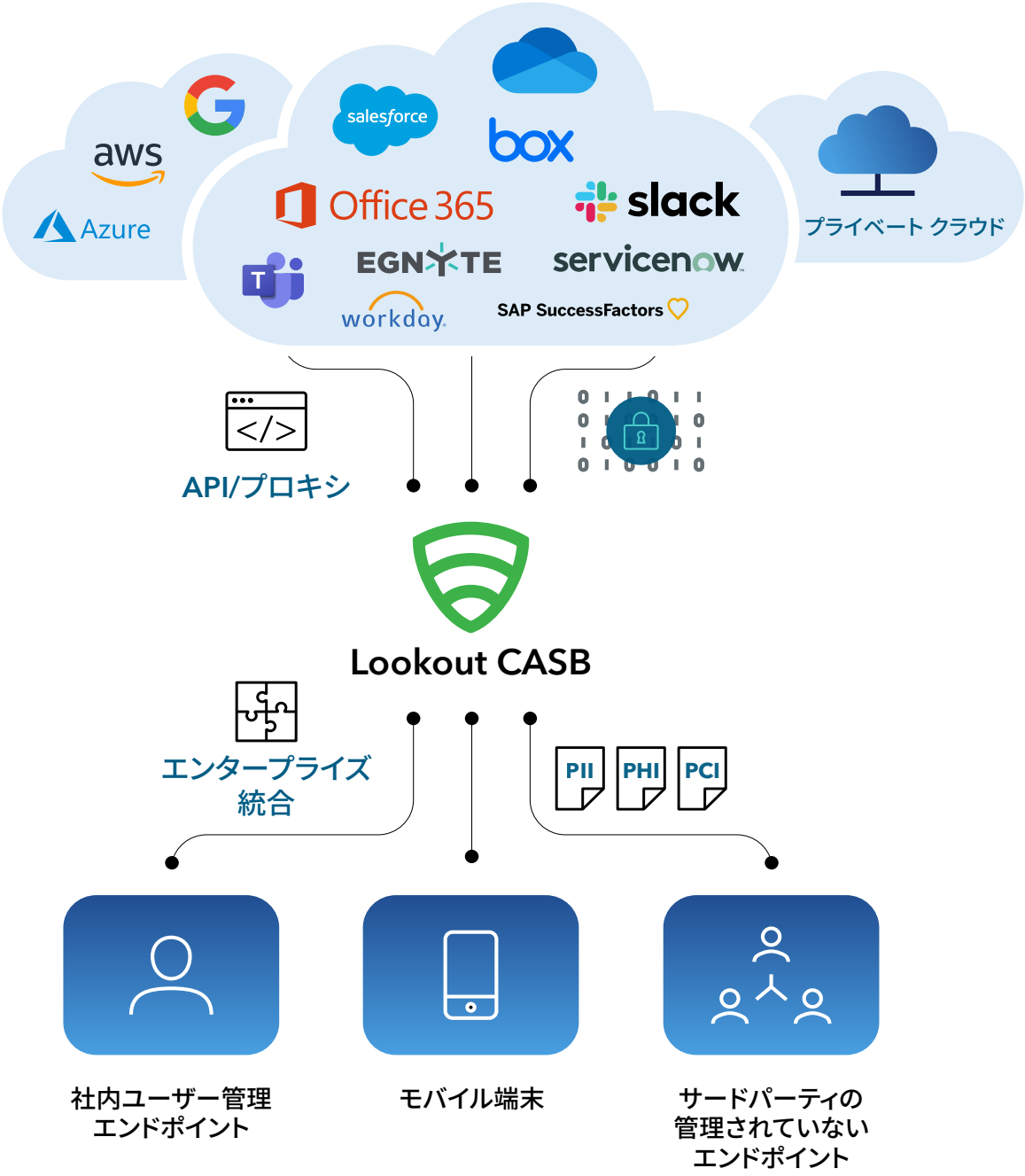
クラウドのインフラストラクチャーとアプリケーションのセキュリティ態勢に対する可視性があれば、データ保護ポリシー制御を施行できます。Lookout CSPM/SSPM (Cloud / SaaS Security Posture Management) は、Software as a Service および Infrastructure as a Service 環境に自動評価と修復を実行し、構成ミスを検出し、アカウント侵害を防止するためのセキュリティ ガードレールを敷きます。

シャドー IT に対する保護

Lookout CASB は、組織がシャドー IT のリスク暴露を制限するためにも役立ちます。既存のネットワーク端末、ファイアーウォール、プロキシ サービスと統合することにより、Lookout はクラウド サービスの使用を評価し、組織で使用しているクラウド サービスへの完全な可視性を実現します。この情報は直感的で詳細なダッシュボード、リアルタイムのアラート、および監査レポートを通して配信されます。

Lookout CASB の差異化要因	

• クラウド アプリのスムーズな展開
• エージェント不要の設計で迅速な展開を可能に
• ゼロ トラスト適応可能アクセス制御
• クラウドおよび SaaS のセキュリティ態勢管理
• クラウド メールのセキュリティとガバナンス
• 高度なポリシー エンジンとコンプライアンス管理
• 次を含む高度なデータ保護:
  • データ検出
  • データ損失防止
  • エンタープライズ デジタル著作権管理
  • 暗号化
	• 以下を対象とするエンタープライズ統合
	  • アイデンティティ アクセス管理
	  • データ損失防止
	  • データ分類
	  • セキュリティ情報とイベント管理
	  • セキュリティ オーケストレーションの自動化と応答
	  • モバイル端末管理



「インターフェースは整然としていて、新しいポリシーを作成するためのワークフローは理解しやすく管理が容易です。管理者はすぐに行動して、効果的なポリシーを迅速に作成できます。」[1]

- ガートナー

[1] Lawson.Craig and Riley.Steve, Gartner, Magic Quadrant for Cloud Access Security Brokers, p. 5. 28 October 2020 - ID G00464465.5

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®