eBook

SSEデータ保護のトップユースケース

現代のビジネス環境におけるデータ侵害を
Zscaler SSEで阻止

コンテンツ

SSEの普及

組織のユーザとアプリはかつてすべてオンプレミスであったため、コストのかかるアプライアンスを介して「城と堀」のセキュリティが構築され、ネットワーク境界を作成してその中のデータを保護していました。

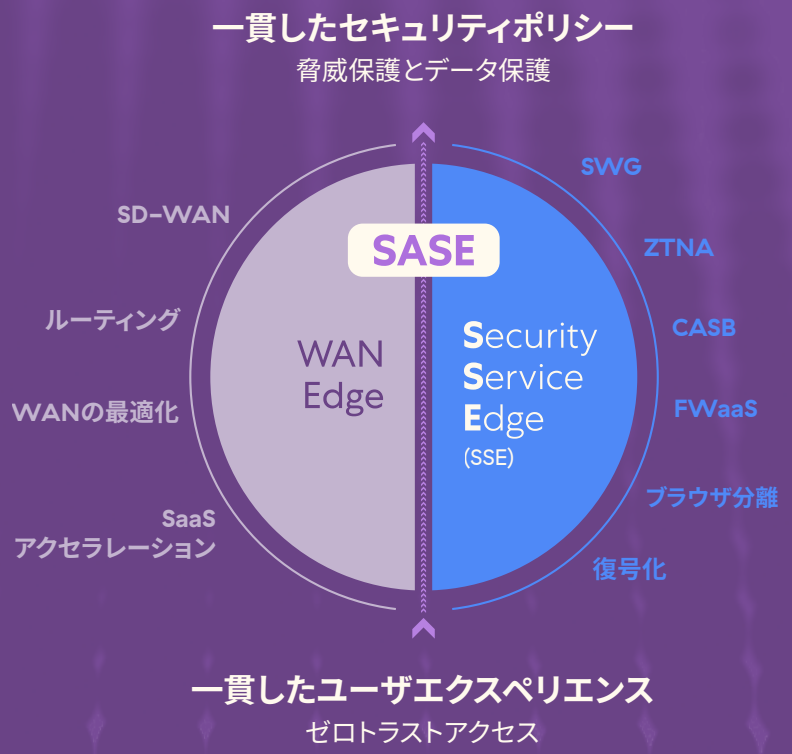
クラウド、Web、リモートワークの普及で「城」は姿を消しましたが、多くの組織は依然として「城と堀」のシステムに頼っています。残念ながら、アプライアンスの複雑なスタックは、最新のデータ保護ニーズに対応できません。また、バックホールトラフィックは、パフォーマンスの低下、スケーラビリティの制限、ユーザの生産性の妨げの原因となっています。

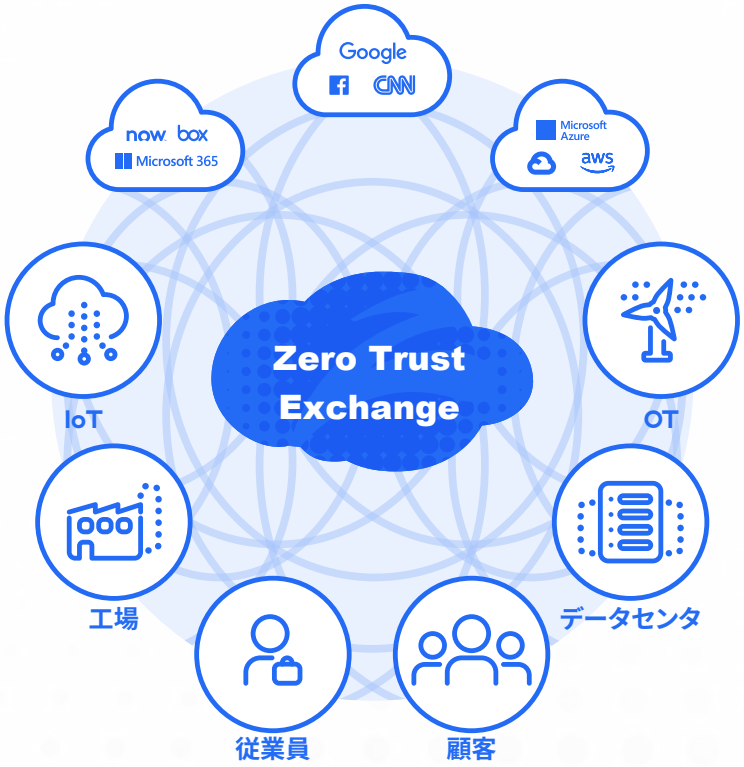
最新のデータ保護ツールの多くも十分ではありません。とくに、インサイダー脅威に焦点を当て、データに対する外部の脅威を無視している場合はなおさらです。つまり、適切なデータ保護には強力なセキュリティが必要なのです。

セキュリティサービスエッジ (SSE)は、これらの課題に対応するソリューションです。複雑さを軽減し、CASB、SWG、ZTNAなどを統合することで最新のデータ保護ギャップを埋める完全なプラットフォームです。エッジでのクラウド配信型セキュリティを通じて、SSEは最大のパフォーマンス、スケーラビリティ、ユーザエクスペリエンスを提供します。

Zscaler Zero Trust Exchange™は世界最大のセキュリティクラウドで、SSEが登場する前からあらゆるトランザクションを保護するように設計されており、データに対するすべての内部および外部リスクを阻止します。

データ保護にSSEを活用するユースケースについては、以下をお読みください。





ゼロトラストセキュリティの実現

従来型のセキュリティツールは、ネットワーク全体　(内部のすべてのデータとアプリ)への自由なアクセスを許しています。このため、リソース間の脅威の水平移動が可能になり、データ侵害の影響が拡大する可能性があります。これは承認されたユーザが必要なときに必要な場所にだけアクセスできるという、ゼロトラストの「最小特権」の原則に反しています。

Zero Trust Exchange

Zero Trust Exchangeは、それとは根本的に異なるアプローチを採用し、ゼロトラストに基づく最新のデータ保護を提供します。Zscalerは、ユーザ、SaaSアプリ、プライベートアプリ、IoT/OTなどの間のインテリジェントな交換機として機能することで、必要に応じて個々のリソースへの安全なアクセスのみを提供し、さらに細分性を高めるための情報漏洩防止 (DLP) を実施します。

Zscalerの利点

- すべてのITリソースをZero Trust Exchangeの背後に隠し、攻撃対象領域を排除
- ユーザをネットワークではなくアプリに直接接続させることで、脅威の水平移動を防止
- ユーザからアプリ、アプリからアプリ、デバイスからデバイスのトランザクションを保護することで、侵害を阻止

暗号化トラフィックによるデータ損失の防止

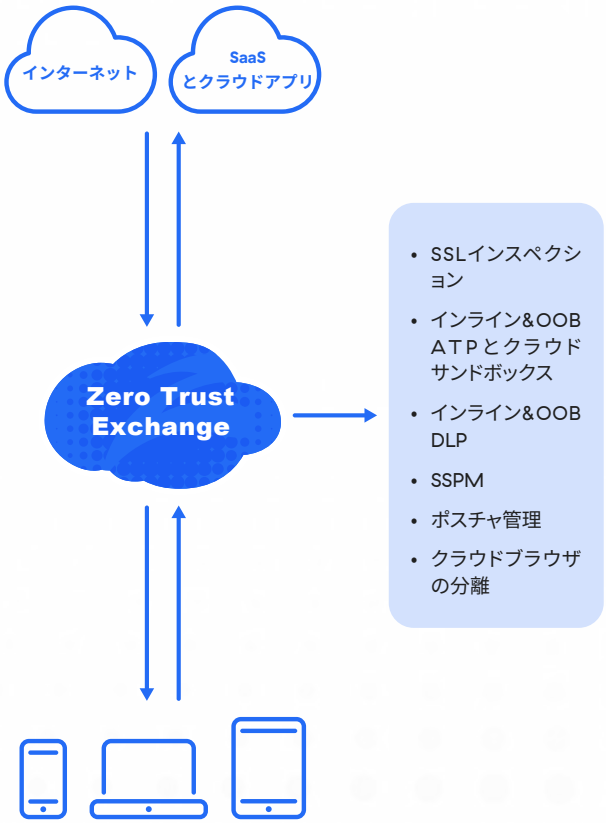
従来型のセキュリティアプライアンス　(ハードウェアまたは仮想)　は、Webトラフィックによるデータ損失を検査するために用いられています。しかし、これらのアプライアンスはユーザにサービスを提供する際に固定容量を持ち、大規模な暗号化トラフィックを処理できず、その結果SSLインスペクションをほとんどまたはまったく提供できていません。Webトラフィックの95%以上が暗号化されている今日、これは危険な弱点です。

真のクラウドアーキテクチャ

世界最大のセキュリティクラウドで構築されるZscalerのセキュリティサービスエッジは、数十万人のユーザを抱えるグローバル企業向けに大規模な暗号化トラフィックを検査するために必要なパフォーマンスを提供します。これにより、SSLによって隠された潜在的なデータ損失を効果的に検出し、リアルタイムでの修復が可能になります。

Zscalerの利点

- 1日2,000億件以上のトランザクションを処理する拡張性とパフォーマンスを備えたセキュリティサービスエッジ
- Forbes Global 2000企業の25%以上が使用するインラインアーキテクチャ上に構築されたプラットフォーム
- エッジのセキュリティを確保し、高水準のユーザエクスペリエンスを実現する世界各地に配置された150以上のデータセンタ



二重脅迫型ランサムウェアの阻止

二重脅迫型ランサムウェアは、デバイスの暗号化やデータの窃盗に加えて、情報の公開を止める代わりに身代金の支払いを要求します。これらの脅威は、ソフトターゲット(セキュリティで保護されていない保存データや構成ミスのあるアプリなど) を利用してデータを急増および流出させます。残念ながら、従来のセキュリティアプライアンスではクラウドファーストの環境でこれらを防ぐことはできません。

完全な脅威保護とデータ保護

Zscalerは、アップロード時およびITエコシステム全体の保存時にランサムウェアを阻止するための完全な脅威保護を提供します。さらに、DLPやCASBはすべてのクラウドデータチャネルを精査して流出を阻止し、ポスチャ管理やSSPMはデータを公開するクラウドアプリの構成ミスを検出します。

Zscalerの利点

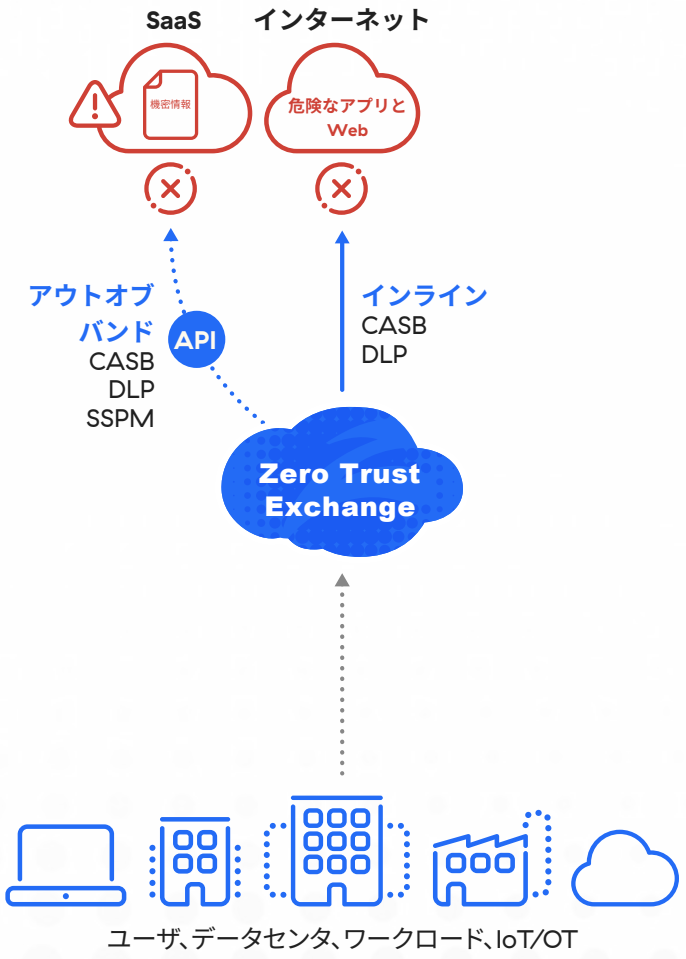
- データの流出や送信中のランサムウェアをリアルタイムで識別する完全かつスケーラブルなSSLインスペクション
- ゼロデイランサムウェアをインラインとアウトオブバンドの両方で阻止するためのクラウドサンドボックス技術
- 検知した脅威をすべてブロックする世界最大のセキュリティクラウド

SaaSアプリケーションの保護

SaaSアプリはこれまでにない生産性と柔軟性を提供しますが、適切に保護されていない場合はデータ損失につながる可能性があります。これは、ユーザが未承認アプリに定期的にデータをアップロードし、保存されているファイルを未承認のユーザと簡単に共有でき、構成を誤るとアプリのセキュリティ体制が損なわれ、データが公開される可能性があるためです。

CASBとDLPの組み合わせ

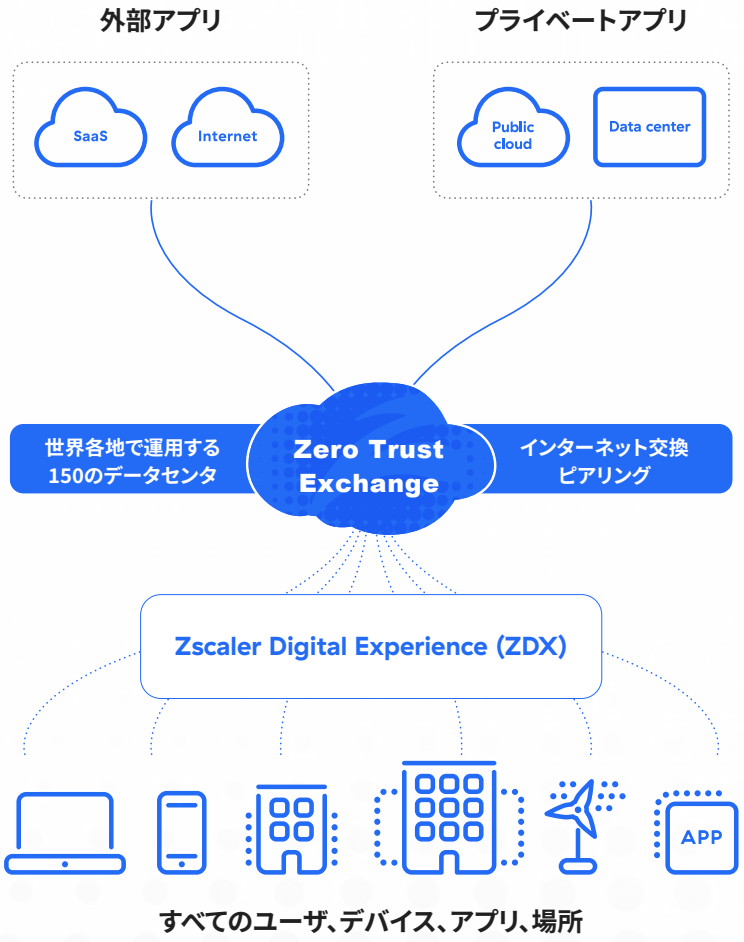
Zscalerは、シャドーITの自動検出、未承認のクラウドアプリへのデータアップロードの制御、認可されたクラウドアプリに保存されているデータの保護により、SaaSアプリの使用を保護します。さらに、SaaSセキュリティポスチャ管理は、アプリをスキャンすることでデータを公開したり、コンプライアンスを侵害したりする恐れのある構成ミスを検出します。



Zscalerの利点

- 統一したポリシーですべてのSaaSおよびクラウドデータチャネルに一貫性のある統合データ保護
- 最も実績のある統合セキュリティサービスエッジの一環としての高性能CASB機能
- 特定の値や画像データを保護するためのEDMやOCRなどの高機能を備えたクラウドDLP

リモートユーザのデータ防御



リモートワークは今後さらに定着すると予想されますが、従来のセキュリティはこの新しいビジネススタイル向けには設計されていません。VPN利用でユーザトラフィックをセキュリティアプライアンスにバックホールすると、スケーラビリティが不十分になり、ユーザの生産性が低下し、クラウドファーストの企業が必要とする最新のデータ保護ニーズに対応できません。

エッジのクラウド配信型セキュリティ

Zscalerは、世界最大かつ実績のあるセキュリティクラウドにより、世界中でリモートワークをサポートしながら、データ保護に必要な規模と専門知識を提供します。アプライアンスへのトラフィックをバックホールすることなく、SaaS、IaaS、PaaS、Web、プライベートアプリなどの使用を対象に、最大のパフォーマンスでデータ全体を保護します。

Zscalerの利点

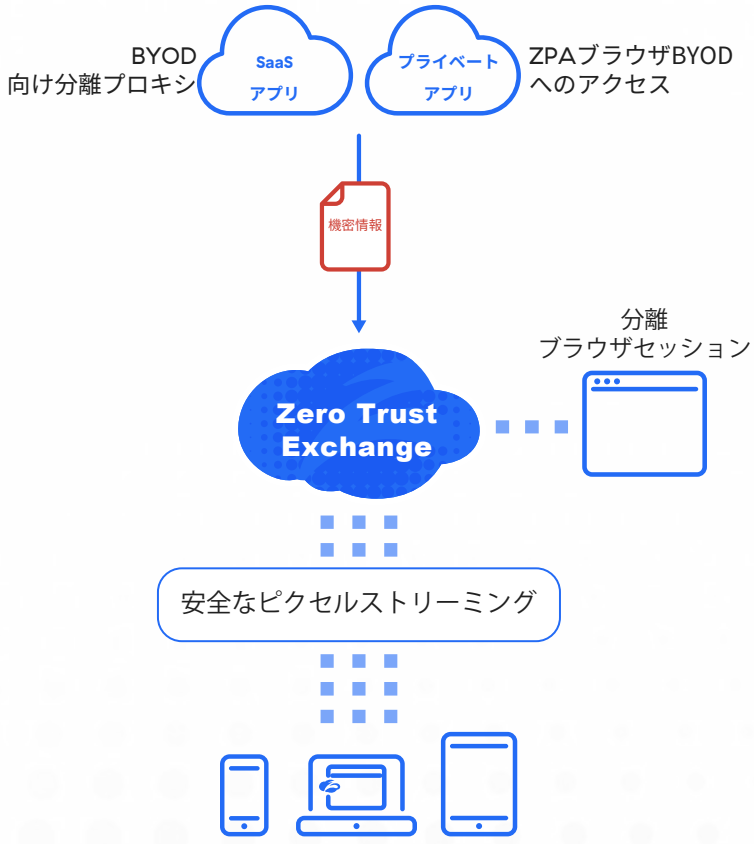
- 150以上のデータセンタを備えたグローバルセキュリティクラウドが提供するエッジの高性能なデータセキュリティ
- ハードウェアや仮想アプライアンスへのバックホールの必要性を排除するSecurity-as-a-Service型のソリューション
- あらゆる場所で効率的かつ完全な保護を実現するCASB、SWG、ZTNAなどを備えたシングルパスアーキテクチャ

BYODなどの管理対象外デバイスの保護

BYODやB2Bデバイスなどの個人用または管理対象外エンドポイントから、正当な目的で企業アプリにアクセスするケースも多くあります。しかし、一旦データをダウンロードしてしまうと、それ以降はIT部門がコントロールする余地がありません。残念ながら、これらのデバイスをブロックすると、ソフトウェアエージェントのインストールは通常実行不可能になり、リバースプロキシは頻繁に中断されるため、生産性が低下します。では、IT部門はどう対処すべきでしょうか？

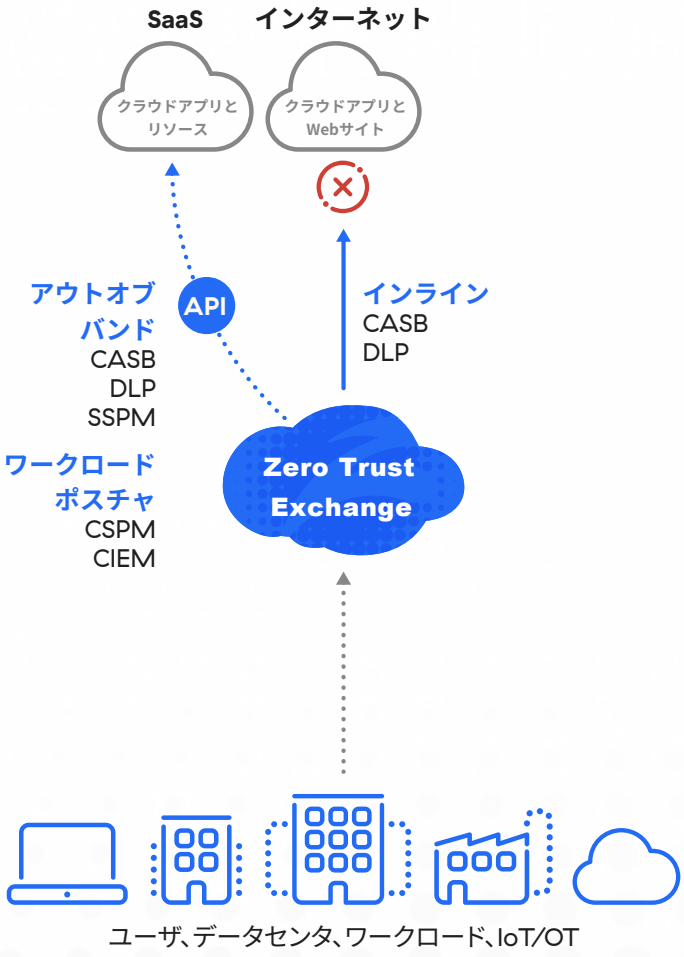
クラウドブラウザ分離

エージェントレスブラウザ分離により、Zscalerは隔離された環境でユーザのアプリセッションを仮想化し、ピクセルのみをエンドポイントにストリーミングすることで、ダウンロード、コピー、ペースト、印刷を防止します。つまり、IT部門はデータを安全に保ちながら、エージェントやリバースプロキシに伴う問題を回避しつつ、管理対象外デバイスからのアクセスを有効にすることができます。また、危険なエンドポイントからの感染ファイルのアップロードも防止します。



Zscalerの利点

- 世界最大かつ高性能のセキュリティクラウド上に構築されたクラウドブラウザ分離
- SaaSアプリケーションにアクセスするあらゆるデバイスでエージェントレスセキュリティを実現する分離プロキシ
- ZPAブラウザアクセスにより、クライアント側のソフトウェアをインストールすることなくプライベートアプリへの安全なアクセスを実現



規制コンプライアンスの徹底

GDPR、HIPAAなどの規制対象データは、企業のその他の機密情報とともにプレミス外に移動していますが、従来のツールではクラウド上でのデータ保護コンプライアンスを維持できません。CCPAをはじめとするプライバシー法やPCI DSSなどのフレームワークを遵守しないと、罰金や消費者からの信頼の喪失、または収益減少につながる可能性があるため、非常に重要な課題になります。

徹底したコンプライアンスの保証

Zscalerのセキュリティサービスエッジは、規制遵守を念頭に構築されたものです。このソリューションは、ITエコシステム全体にわたって完全な可視性とコントロールを提供し、規制対象データの安全性を維持し、ゼロトラストの原則をあらゆる所で適用させアプリケーションにコンプライアンスに影響する脆弱性がないことを保証します。

Zscalerの利点

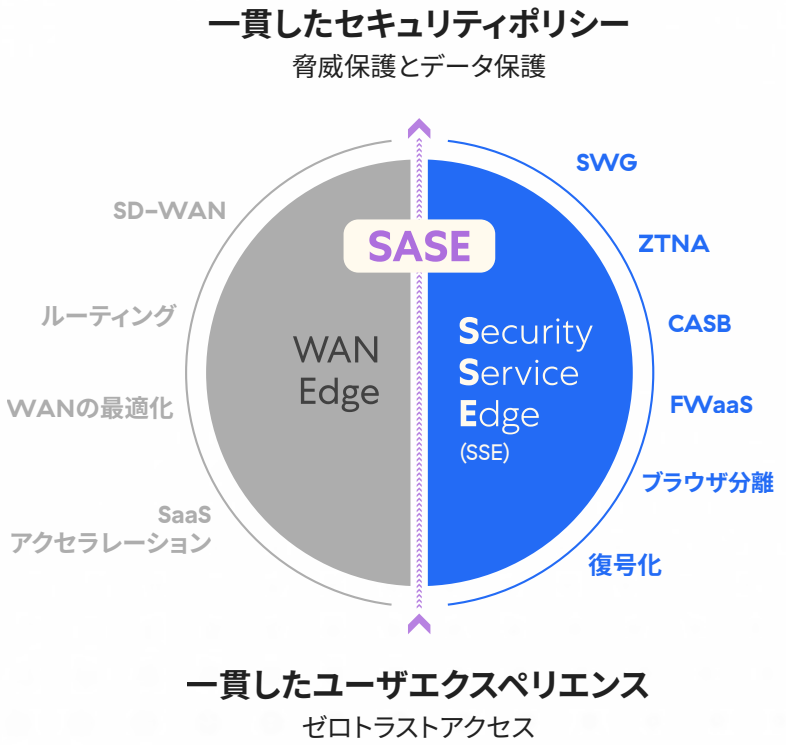
- 移動中および保存中の規制対象データを保護するマルチモードCASB機能を備えたクラウドDLP
- コンプライアンスの維持: 完全データ一致 (EDM) 目的の場合も含めてインスペクションのためにデータをダウンロードしません。
- コンプライアンス違反につながる構成ミスや権利を発見、修正するZscaler SSPMおよびポスチャ管理

一貫性と管理性を備えたデータ保護の実現

機能の異なるポイント製品のまとまりのない組み合わせに依存することは、多くの問題が発生してしまいます。とりわけ、複雑化する一方のITエコシステム全体におけるデータ保護の一貫性が無くなってしまいます。さらに、サイロ化された多数のソリューションの監督は管理者にとって大きな負担となります。

オールインワンプラットフォーム

Zscaler　SSEは、あらゆるトランザクションを保護し、場所を問わずデータを一貫して完全に保護できる最先端のテクノロジーを統合しています。シングルパスアーキテクチャを備えた総合的なクラウドソリューション提供により、企業ITの複雑さを低減しながら、管理者の負担軽減を実現できます。



Zscalerの利点

- すべてのSaaS、クラウド、Web、プライベートアプリケーションに対する一貫したデータ保護
- ポイント製品やアプライアンスを削減するアーキテクチャの簡素化
- ポリシーの重複を排除し、管理者の時間を節約するシンプルな統合管理

クラウドとモビリティは生産性と柔軟性の面で計り知れないメリットを提供しますが、データの安全性を損なうことなくそれらを活用するには、サイバーセキュリティへの新しいアプローチが必要になります。Zscalerのセキュリティサービスエッジにより、企業は場所を問わずにデータを保護しながらデジタルトランスフォーメーションを実現できます。

- **Zscaler SSEについてのお客様の声**
- **セキュリティサービスエッジのMagic Quadrantはこちら**

zscaler™ | Experience your world, secured.™

Zscalerについて
Zscaler (NASDAQ: ZS) は、より効率的で、俊敏性や回復性に優れたセキュアなデジタルトランスフォーメーションを加速しています。Zscaler Zero Trust Exchangeは、ユーザ、デバイス、アプリケーションをどこからでも安全に接続させることで、何千人ものお客様をサイバー攻撃や情報漏洩から保護しています。世界中で運用する150のデータセンタで稼働するSASEベースのZero Trust Exchangeは、世界最大のインライン型クラウドセキュリティプラットフォームです。詳細は、**zscaler.jp**をご覧いただくか、Twitterで**@zscaler**をフォローしてください。

+1 408.533.0288 Zscaler, Inc.(本社) - 120 Holger Way - San Jose, CA 95134 zscaler.jp