ゼロトラスト＋ AI

組織の保護と最適化

ホワイトペーパー

ゼロトラストと AI が必要な理由

人々の働き方は数年前とは大きく変わりました。かつて、従業員は仕事をするために毎日オフィスに足を運び、組織のオンプレミス データ センターでホストされているアプリケーションやリソースにアクセスしていました。つまり、ユーザー、アプリ、データはすべてオフィスに存在し、組織は基本的にオンプレミスのみで運営されていたのです。しかし、2 つの現象の相乗効果によって、こうした体制は一変することになります。

1 つ目は、クラウドや SaaS アプリケーション (Salesforce や Microsoft 365 など) の普及です。これにより、組織はオンプレミスで IT リソースを構築したり管理したりする必要がなくなりました。代わりに、ベンダーのクラウドからサービスとして提供される専用のアプリやツールを使用できるようになりました。この柔軟性によって、組織は活力を飛躍的に高めるとともに、大幅なコスト削減を実現しました。

2 つ目は、リモート ワークの普及です。主にクラウド アプリの採用がこれを後押ししました。IT リソースがオフプレミスに置かれるようになれば、それにアクセスするためにオフィスに出向く必要はありません。2020 年の世界的なパンデミックで外出が制限されるなか、組織が生産性の維持に努めた結果、当然ながらリモート ワーク (およびクラウド アプリ) の採用が加速することとなりました。ここでも、柔軟性の向上が組織の活力向上とコスト削減につながりました。

こうした変革は大きな価値をもたらしている一方、サイバー リスクや競争圧力に関する重大な課題も生んでいます。

- サイバー リスクの増大：従来の「城と堀」のセキュリティ モデルはクラウドやリモート ワーク向けに設計されておらず、現代の脅威の高度化に対応できません。
- 競争圧力の増大：こうした変革によって生産性や活力が向上した状態が一般化したことで、組織は可能な限り効率的に業務を遂行するとともに、高まる顧客の期待に迅速に対応する必要に迫られています。

今日、組織が成功するためには、この 2 つの課題に対処する必要があります。これを踏まえ、この話に関連する現象としてもう一つ非常に重要なのが人工知能と機械学習 (AI/ML) の出現です。AI は、ビジネス ソリューションやサイバーセキュリティ ソリューションなども含め、現在の業務環境全体にごく短期間で広く普及しました。AI を最新のマーケティングのバズワードとして片付けるのは簡単に思えるかもしれません。しかし、実は、少なくともゼロトラストと組み合わせることで、AI は上記 2 つの課題に対処するうえで重要な役割を果たします。世界中の無数の組織が Zscaler に目を向けている理由はそこにあります。

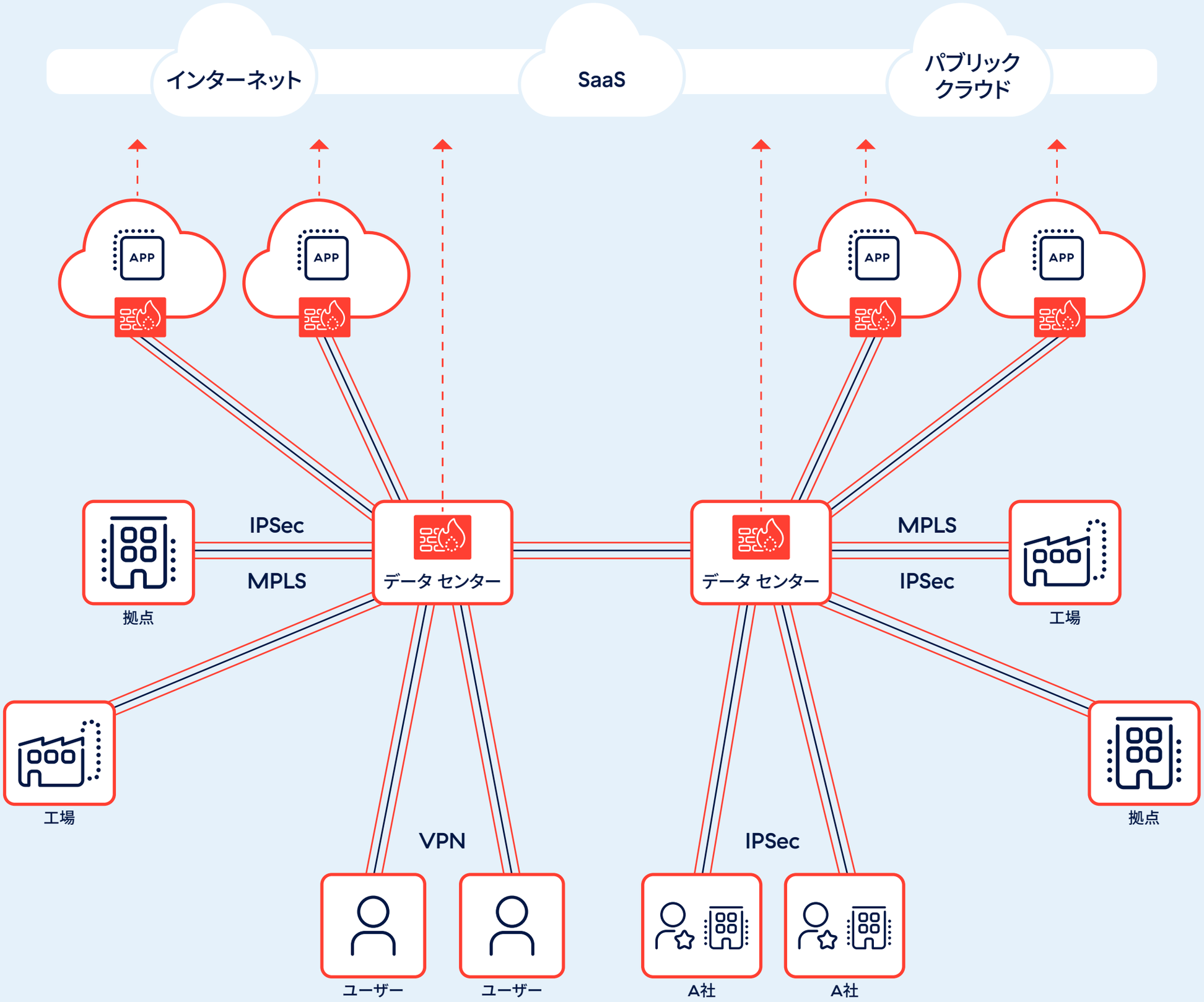
Zscaler のゼロトラスト＋ AI

クラウド ネイティブな Zscaler Zero Trust Exchange プラットフォームは、ゼロトラスト アーキテクチャーを実現するとともに、AI/ML を取り入れてその機能を強化しています。ゼロトラスト アーキテクチャーと AI という強力な組み合わせにより、リスクの増大と、少ないリソースでの生産性向上を迫る圧力の高まりに対応し、前述の問題を解決することが可能です。その理由を理解するために、これらの各要素について見ていきましょう。

ゼロトラスト アーキテクチャー

ゼロトラストは、従来のような単なる現状維持の手段でも、セキュリティのポイント製品でもありません。標準的な境界ベースのセキュリティ アーキテクチャーとは一線を画した、根本的に異なるアプローチであり、従来の手法の欠点からの解放を実現します。したがって、セキュリティに AI を実装するにあたっては、その基盤としてゼロトラストを使用することが非常に重要です。ゼロトラストなしで AI を活用して境界ベースのセキュリティ アーキテクチャーを改善しようとすることは、割れた鏡を磨くようなもので、輝きを増したとしても本質的な欠陥を残すことになるためです。

ファイアウォールとVPN中心のアーキテクチャー



信頼されたネットワークがユーザー、サイト、アプリを接続します。
脅威対策とデータ保護はネットワークの保護に重点を置きます。

柔軟性に欠け複雑なうえセキュリティ リスクとなり、トランスフォーメーションの妨げに

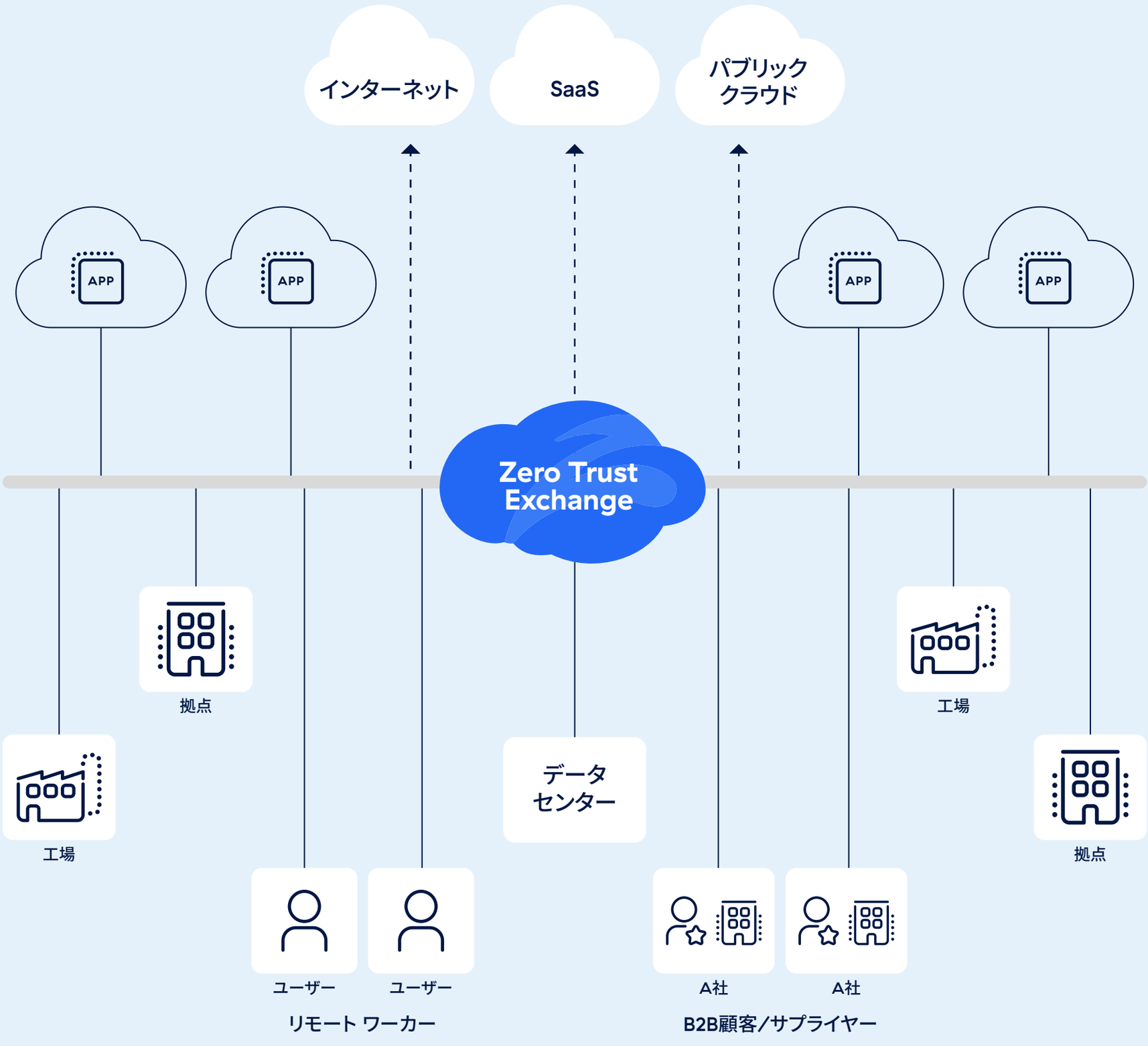
図 1: 境界ベースのアーキテクチャー

ファイアウォールや VPN などのツールに基づいて構築された境界ベースのアーキテクチャーは、組織のハブ&スポーク ネットワークの周囲に安全な境界を確立することに重点を置いています。このアーキテクチャーがよく「城と堀」のセキュリティ モデルと呼ばれるのはそのためです。境界ベースのアーキテクチャーは、クラウド アプリやリモート ワークが普及する前のオンプレミスのみの環境向けに設計されています。したがって、現代の組織がこのアーキテクチャーを使用しようとすると、多くの課題が生まれます。

- 攻撃対象領域の拡大：ネットワークをより多くのユーザー、デバイス、クラウド、場所に拡張し、パブリック IP アドレスを持つファイアウォールと VPN を使用するため、攻撃対象領域が拡大します。
- 侵害を可能にする環境の発生：基盤となるアプライアンス (ハードウェアおよび仮想) は、**脅威の 86% が潜む暗号化されたトラフィック**を大規模に検査するための拡張性に欠けています。
- ラテラル ムーブメントの助長：ユーザーとエンティティーがネットワーク上に置かれ、ネットワーク内で接続されたさまざまなリソースにアクセスできるため、ラテラル ムーブメントを阻止できません。
- 情報漏洩を防止する能力の欠如：拡張性に欠け、暗号化されたトラフィックを検査できないほか、SaaS アプリでの共有などといった最新の漏洩経路を保護できません。
- 複雑さとコストの増大：セキュリティのための無数のポイント製品の導入やネットワークの無秩序な拡大を招き、購入、構成、保守に高いコストがかかります。
- ユーザーの生産性の低下：中央のデータ センターにトラフィックをバックホールする必要があるため、遅延が増加し、デジタル エクスペリエンスの低下を招きます。

2024 年、**Ivanti**、**Cisco**、**Palo Alto Networks** のファイアウォールや VPN に相次いで脆弱性が発見されました。これらのツールから脱却し、ゼロトラスト アーキテクチャーを採用する必要性が浮き彫りになっています。

ゼロトラスト アーキテクチャー



**接続元のネットワークを問わず、誰が何にアクセスできるかを
ビジネス ポリシーで決定します(ネットワークは単なる輸送手段として機能)。**

アジャイル、シンプル、セキュアで、トランスフォーメーションを促進

図 2: Zscaler のゼロトラスト アーキテクチャー

前述のように、ゼロトラストは境界ベースのアーキテクチャーとは根本的に異なります。ゼロトラストは、城を守る堀 (ネットワーク境界) ではなく、1 対 1 の安全な Any-to-Any 接続を提供するインテリジェントな交換機のようなもので、ユーザーはネットワーク全体ではなく、アプリに直接接続されます。誰が何に対してアクセス権を持つべきかは、コンテキストを用いて判断します。つまり、Zscaler では、セキュリティと接続がネットワークへのアクセスから切り離され、最小特権アクセスの原則が適用されます。このゼロトラスト接続 (および他の多数の機能) は、Zscaler の高パフォーマンスかつグローバルなセキュリティ クラ

ウドである Zero Trust Exchange を通じ、サービスとしてエッジで提供されます。従来のようにトラフィックをバックホールすることはありません。

Zscaler を利用してゼロトラスト アーキテクチャーに移行することで、以下のようなことを実現できます。

- 攻撃対象領域の最小化：際限のないネットワークの拡張に歯止めをかけ、ファイアウォールや VPN とそのパブリック IP アドレスの必要性を排除し、アプリを Zscaler の背後に隠します。
- 侵害の阻止：必要に応じて拡張できる高性能なセキュリティ クラウドを通じて、あらゆる量の暗号化トラフィックを検査し、ポリシーをリアルタイムで適用します。
- 脅威のラテラル ムーブメントの防止：多くの接続されたリソースを抱えるネットワークではなく、本人がアクセスを許可されているアプリにユーザーを直接接続します。
- 情報漏洩の阻止：暗号化されたトラフィック、クラウド アプリ、エンドポイントなど、情報漏洩のすべての経路に対応します。悪意によるものか偶発的なものかも問いません。
- コストと複雑さの削減：アプリケーションへの直接接続でネットワークを簡素化し、包括的なプラットフォームでセキュリティのポイント製品を排除します。
- 生産性の向上：アプリへの直接接続と、宛先への最短パスでのトラフィックのルーティングにより、ユーザー エクスペリエンスを向上させます。

こうした理由から、ゼロトラストは AI/ML を実装するための基盤として理想的なアーキテクチャーと言えます。

業界をリードする AI 技術

Zscaler は AI/ML の分野で明確な優位性を持っています。これは主に、AI の有効性が使用できる学習データの有効性に決定づけられるためです。質の低いデータを利用しても、良い結果を得られません。

世界最大のセキュリティ プラットフォームである Zscaler Zero Trust Exchange は、世界中の 4,000 万人以上のユーザーで構成される数千の組織のほか、無数のワークロード、IoT/OT デバイス、サードパーティーの従業員などに安全な接続をサービスとして提供しています。このような規模を持った結果として、Zscaler では、毎日 5,000 億件以上のトランザクション (Google の 1 日あたりの検索数の 45 倍以上) と、500 兆件のテレメトリー信号を処理しています。Zscaler は IT リソースへのアクセスを安全に管理する目的でコンテキストを精査するため、すべてのアクセス試行について、アイデンティティー、デバイス、コンテンツ、宛先、ネットワークに関する豊富なデータが存在します。さらに、サイバー犯罪者の最新の戦術、技術、テクノロジーを常に研究し、業界をリードする社内の脅威研究部門「ThreatLabz」が持つ大量のデータも抱えています。こうしたデータを通じ、Zscaler はサイバー脅威とその仕組みや巧妙化について、長年の研究を積み重ねています。

Zscaler Data Fabric for Security は、さまざまなセキュリティ ソリューションやビジネス ソリューションとの 150 以上の事前構築済みの統合により、さらに強化されています。セキュリティ データ ソースには、Tenable、Qualys、Wiz などの脆弱性スキャナー、CrowdStrike などのエンドポイントでの検知と対応 (EDR) ソリューション、Okta、Ping Identity、Microsoft などのアイデンティティー管理ツール、60 以上の脅威インテリジェンス フィードが含まれます。ビジネス データ ソースには、コストとライセンス関連のデータを扱う SAP、組織構造情報を扱う Workday、構成管理データベースとしての ServiceNow などがあります。Zscaler は、こうしたすべてのソースからデータを取り込み、独自のデータセットと組み合わせ、重複を排除しながらこれを強化します。複数のソースからのデータを手動で 1 つの場所に集約する必要はなく、Zscaler がプロセスを自動的に処理します。

図 3: 業界をリードする Zscaler の AI 技術

Zscaler では、この大規模で関連性の高いデータ セットで大規模言語モデル (LLM) をトレーニングすることで、データの意思決定への応用を加速できます。Zero Trust Exchange の AI 活用型ソリューションは、分析、自動化、有効性の向上を特徴としています。このホワイト ペーパーの残りの部分では、Zscaler プラットフォームが AI/ML を活用して現代の課題を解決し、組織の保護と最適化を支援するさまざまな方法について詳しく説明します。

Zscaler による組織の保護

ゼロトラスト アーキテクチャーは、境界ベースのアーキテクチャーの弱点を克服するため、単体でも大幅なセキュリティ強化とサイバー リスクの軽減につながります。しかし、ゼロトラスト アーキテクチャーの強みと、AI を組み込んだ最先端のセキュリティ機能を組み合わせることで、サイバー犯罪者や高度な脅威に対する組織の防御はさらに強化されます。Zscaler は、ゼロトラスト アーキテクチャーと AI を活用した機能の両方を提供してリスクを軽減し、さらにはユーザーと管理者の生産性を向上させます。

Cloud Sandbox の AI による即時判定

サイバー脅威が巧妙化するなか、組織は脅威をリアルタイムで検出、軽減する機能を必要としています。こうした機能がなければ、進化を続け、検出の難し

い手法を持つ巧妙なサイバー犯罪者によって簡単に侵害される可能性があります。サンドボックス技術は、ユーザーから離れた安全な環境で潜在的に悪意のあるファイルを実行し、そのファイルに安全にアクセスできるかどうかを判断するように設計されています。

残念ながら、従来のサンドボックス分析手法では、本質的にセキュリティと生産性がトレードオフの関係にあります。サンドボックスの基準が緩すぎると、悪意のあるファイルがユーザーのデバイスに侵入し、組織の侵害につながる可能性があります。一方、サンドボックスの基準が厳しすぎると、無害なファイルがサンドボックスで処理され、ユーザーのアクセスが数分にわたって不必要に妨げられ、生産性が損なわれる可能性が高くなります。

Zero Trust Exchange は、AI の力を活用することで従来のサンドボックスに固有の課題を解決し、セキュリティと生産性を両立させます。クラウド ネイティブな Zscaler Sandbox では、長年にわたる分析と 5 億 5000 万を超えるファイル サンプルとのインタラクションに基づいてトレーニングと微調整がなされた ML モデルを統合し、検出精度を向上させています。

管理者は、AI による即時判定をクリック一つで有効にできます。これによって、悪意のある可能性が高い AI/ML 脅威スコア 91 ～ 100 のファイルは自動的にブロックされるため、ユーザーはファイルが他の環境で実行されるのを待つ必要がありません。ファイルベースのゼロデイ脅威に対する保護を直ちに提供しながら、ユーザーの生産性を維持できます。さらに、悪意のある可能性が高いファイルを即座にブロックすることで、調査を要する潜在的なペイシェント ゼロ インシデントの件数が最小限に抑えられ、SOC 部門では作業負荷が軽減され、他の重要なセキュリティ タスクに集中できるようになります。つまり、組織は進化する脅威から身を守りながら、SOC 部門とエンドユーザーの時間を最適化できます。

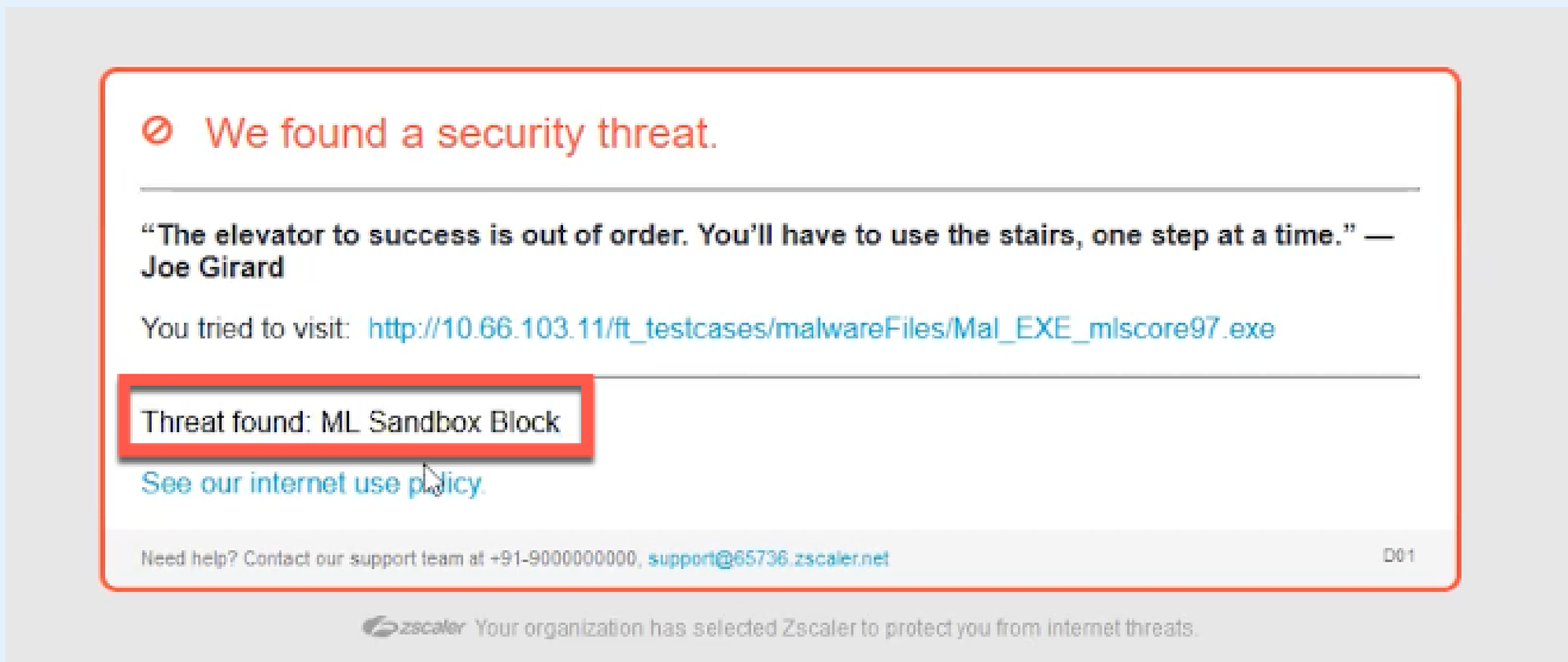


図 4: AI による即時判定に基づくユーザー通知

スマート ブラウザー分離

サイバー犯罪者は、悪意のある Web サイトを使用して、危険なコンテンツをユーザーのブラウザーやデバイスに読み込ませ、ユーザーの組織に攻撃を仕掛けるための足がかりを作ります。この問題への対処にあたりよく使用されるソリューションが、さまざまなWebサイトへのアクセスをブロックできるURLフィルタリング ツールです。通常、アクセスのブロックは、既知の悪意のある Web サイトとまだ信頼性が証明されていない新規登録ドメインをフィルタリングすることで行われます。しかし、残念ながらこのアプローチには重大な弱点があります。まず、実績ある信頼性の高い Web サイトでも、広告やサイバー犯罪者が配置したゼロ ピクセル iframe などを通じて、意図せず悪意のあるコンテンツを配信している可能性があります。さらに、すべての新規登録ドメインをブロックすると、新しい正当な Web ベースのツールや、ドメインを更新しただけの既存の信頼できる Web サイトへのアクセスが妨げられるため、ユーザーの生産性が低下します。いずれのケースでも、ヘルプデスクは大量のチケットに追われることになり、IT 部門の生産性も低下します。

Zscaler Smart Browser Isolation は、こうしたセキュリティと生産性の課題を克服します。「Smart」とあるのは、このソリューションに AI モデルおよび ML モデルが組み込まれており、これを活用して悪意のある可能性のある Web コンテンツを自動的に認識できるためです。これによって、組織は新規登録ドメインの新たな脅威、そして信頼できるドメインに隠された脅威に対応できます。

スマート ブラウザー分離では、AI が悪意のある可能性が高いと判断した Web の宛先をユーザーが訪れた際、ユーザーのセッションが「分離」されます。その Web セッションは Zero Trust Exchange 上で開始され、セッションのピクセルのみが Zscaler クラウドからエンド ユーザーのデバイスに送信されます。分離されたセッションの画像をストリーミングすることで、見た目上は通常と同じように利用できますが、ユーザーは Web サイトと直接やり取りしないため、アクティブ コンテンツがエンドポイントに到達することはありません。脅威がその狙いどおりにデバイスにダウンロードされることはなく、ファイルのアップロードやテキストの貼り付けを防ぐことで、情報漏洩につながる行為も制御できます。これにより、リスクを大幅に低減できます。ユーザーが必要とする正当な Web ツールへのアクセスを妨げるような過剰なブロックもなくなるため、ヘルプ デスク チケットの件数が抑えられ、エンド ユーザーと IT 部門の生産性が向上します。

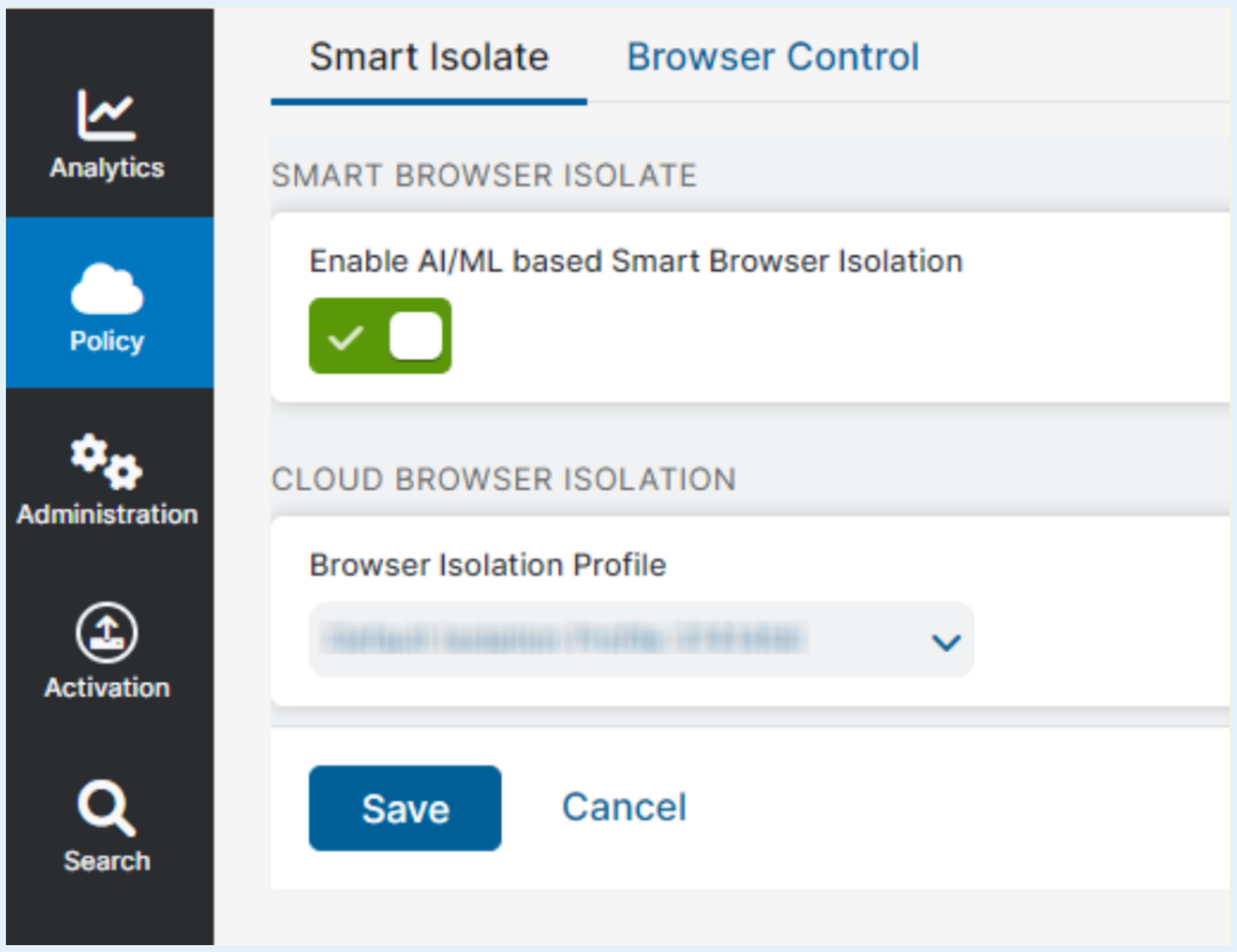


図 5: ワンクリックでのスマート ブラウザー分離の有効化

AI 活用型のアプリ セグメンテーション

ファイアウォールなどの従来のツールで構築されたネットワーク中心のセキュリティ アーキテクチャーに依存する組織は、脅威のラテラル ムーブメントの阻止にあたり、大きな課題に直面します。前述のように、ラテラル ムーブメントとは、ネットワーク上の攻撃者が接続されたリソース間を移動し、その中の機密データにアクセスする方法を指します。これを防ぐための効果的なセグメンテーションを行わなければ、攻撃の影響範囲は広範囲に及ぶ可能性があり、大規模なデータ侵害を招くうえ、評判や財務の面でも大きな損害を被る可能性があります。

残念ながら、組織は通常、堅牢なネットワーク セグメンテーションの実装と維持に苦労しています。従来の方法は手動での構成を要するため、人的ミスが発生しやすく、結果的に重要な資産を露出させてしまう可能性があります。さらに、現代のネットワークは動的な性質を持っているため、クラウド サービスやリモート ワークの採用が拡大するなか、絶えず変化するネットワーク トポロジーとユーザー アクセスの要件に対応することは困難になっています。この複雑さは、管理オーバーヘッドの増加につながり、効果的なセグメンテーション戦略の実装をさらに妨げます。

前述のように、Zscaler のゼロトラスト アーキテクチャーは、ネットワークではなく、アプリケーションへの直接アクセスを提供するものです。このゼロトラスト セグメンテーションが、ユーザー、ワークロード、拠点、デバイス間のラテラル ムーブメントを防ぎます。あらゆる侵害の潜在的な影響範囲をさらに縮小するために、Zscaler は AI 活用型のアプリ セグメンテーションを提供しています。人工知能を活用することで、Zscaler はお客様にとって理想的な App Segment を自動的に生成します。

AI 活用型のアプリ セグメンテーションは、ユーザーの行動とアプリケーションの使用状況を継続的に監視、分析することで機能します。ML アルゴリズムを活用してパターンと異常を特定し、どの従業員がどのアプリにアクセスする必要があるかを判断できます。たとえば、一部の従業員のみが財務アプリにアクセスする場合、Zscaler はそのユーザー グループへのアクセスを制限するセグメントを自動的に作成します。この的を絞ったアプローチにより、すべてのアプリケーションでラテラル ムーブメントの可能性が大幅に減少します。

AI 活用型のアプリ セグメンテーションは、根本的に異なるアプローチでセグメンテーションを行います。機密性の高いアプリへのアクセスを高い精度でプロアクティブかつ自動的に特定、制限し、セグメンテーション プロセスを簡素化することで、従来の方法に付きまとっていた複雑さ、ミス、リスクを排除します。これにより手動での構成の管理負担が軽減され、IT 部門は時間とリソースを節約して、他の重要なセキュリティ タスクに労力を集中させることができます。

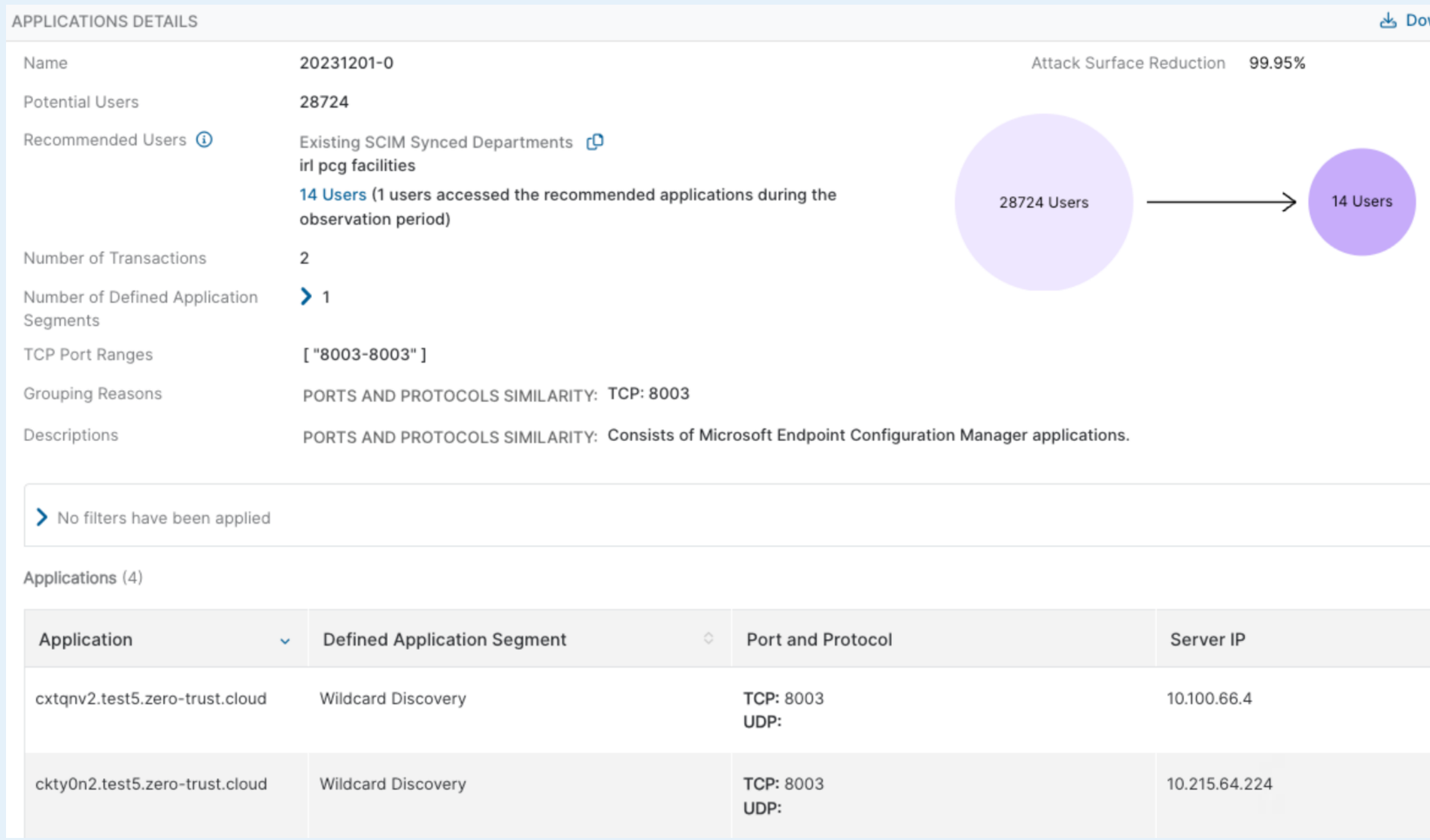


図 6: AI 活用型のアプリ セグメンテーションによる推奨

AI による自動データ検出

今日のデジタル環境は、データ セキュリティにとって大きな課題となっています。データは従来のデータセンターの外に広く分散し、Web、クラウド アプリケーション、リモート ユーザーのデバイスで継続的に保存、アクセスされています。その結果、どの機密情報がどこに転送されているのかを特定しにくくなり、組織は新たな現実への対応を迫られています。CISO やデータ保護部門にとっては、データの安全の確保がますます困難になっています。

分散したデータの保護にあたっては、ポイント製品 (ネットワーク、クラウド、Web、エンドポイント向けのそれぞれ異なる DLP ソリューション) の利用は効果的でないことがわかっています。通常、こうしたツールはサイロ化した環境で動作するため、可視性の穴や応答速度の低下につながります。さらに、別々のソリューション間でポリシーを手動で複製する必要があるため、ミスが起こりやすく、時間がかかります。結局、この断片的なアプローチでは、情報漏洩のリスク、さらにはコストと複雑さが増大します。

Zscaler AI Auto Data Discovery を使用すると、組織はデータを自動的に検出、分類、制御する能力を強化し、新たなデータの生成やあらゆる場所への移動に対処できます。また、Zscaler の AI はあらゆる状況で機密性の高いファイルやデータを特定できるよう徹底的にトレーニングされており、SaaS、IaaS、PaaS に保存されているものか、ユーザーのエンドポイントで使用中のものか、暗号化されたトラフィックを介して Web に転送中のものかを問わず対応できます。管理者は、機密データの検出のために別々のツール間でルールを複製する必要がありません。Zscaler の辞書やデータ分類ポリシーの構成も不要です。このソリューションは、包括的な対応範囲と自動的な実行によって、他のツールでは残る可視性

の穴を最小限に抑え、手動でのルール作成から起こるミスを減らします。結果として、組織はより迅速かつ正確にデータを検出、保護し、情報漏洩のすべての経路にわたり機密情報を確実に保護できるようになります。

AI による自動データ検出を利用することで、保護を強化するだけでなく、データ セキュリティの監視の複雑さも軽減できます。前述のとおり、ポイント製品のダッシュボードの数が最小限に抑えられるほか、手動でのポリシーの複製や DLP 辞書の構成も不要になります。AI を活用した自動化により、専門知識の必要性が抑えられ、組織はデータ保護プログラムをより迅速に展開、管理できるようになります。これが結果的にセキュリティの改善と管理者の生産性向上につながります。

図 7: AI による自動データ検出のダッシュボード

Zscaler による組織の最適化

クラウド型である Zscaler プラットフォームは、セキュリティと接続をサービスとして提供しており、すべてのお客様のトラフィックが Zero Trust Exchange を経由します。Zscaler は、インラインに配置されたプラットフォームならではの視点と、150 以上のセキュリティ ソリューションやビジネス ソリューションとの事前構築済みの統合によって、データの集約と収集の複雑さを伴わずに、強力なインサイトを生成し、AI による分析と意思決定を完全に自動かつリアルタイムで提供します。つまり、Zscaler を通じてゼロトラストと AI を活用することで、セキュリティの強化以上のメリットを得られます。以下に紹介するツールを通じ、組織の最適化を図ることが可能です。

Zscaler Digital Experience (ZDX)

クラウド アプリケーションやハイブリッド ワークは、従来のオンプレミスのみの環境に比べ柔軟性に優れているため、瞬く間に世界中のユーザーに受け入れられています。しかし、デジタル トランスフォーメーションは、ネットワークとルーティング リンクの複雑な集合体を生み出します。これは、世界全体、ISP、ホーム Wi-Fi ネットワーク、従業員所有のデバイス、SaaS アプリなどにまたがるもので、その多くは企業ネットワークの境界外に存在します。結果的に、この進化が組織の生産性に 2 つの大きな問題をもたらします。

まず、新たなクラウド、ネットワーク、デバイス、ロケーションが増えるごとに複雑さが増し、潜在的な障害点が 1 つ増えることになります。その結果、デジタル エクスペリエンス (およびユーザーの生産性) が妨げられる可能性が高くなります。次に、多面的な環境は、デジタル エクスペリエンスに対する可視性の断片化につながります。各部門が使用するデバイス、ネットワーク、アプリの監視ツールは、それぞれアプリ配信チェーンのごく一部しか可視化できません。ユーザーのデバイスとアプリの間に死角が残るため、各ツールからデータを手動でエクスポートして関連付けるために別のチームが必要になります。結果として、ヘルプ デスクは問題解決に膨大な労力を費やし、ヘルプ デスクとエンド ユーザーが貴重な時間を浪費することになります。

Zero Trust Exchange の一部である Zscaler Digital Experience (ZDX) は、こうした問題に対処するために設計されました。ZDX は、Zscaler のインライン プロキシ アーキテクチャーを活用することで、デバイス、ネットワーク、アプリの監視のサイロ化を解消し、ユーザー エクスペリエンスに対するエンドツーエンドの完全な可視性を提供するために必要な基盤を確保しています。

このソリューションは、その可視性を使って AI を活用した根本原因分析を促進します。ボタンのクリック操作だけで、ユーザー エクスペリエンスの問題についてのトラブルシューティングを自動的に行い、その根本原因を明らかにして迅速な解決を図れます。インシデント ダッシュボードでは、これと同じ AI を活用して自動的な関連付けを行い、アプリ、Wi-Fi、ISP、エンドポイント、その他の何に起因するかを問わず、複数のユーザーに影響を与える隠れた問題を検出します。直近では、ユーザー向けのセルフサービス機能も追加されました。**Zscaler Client Connector** エージェントで実行されている AI エンジンが、Wi-Fi の通信品質の低下や CPU 使用率の増大などの問題をユーザーに通知し、チケットを作成せずに自分で問題を解決する方法を提案します。最後に、これらの機能はすべて ZDX Copilot による自然言語処理に拡張されたため、管理者は生成 AI アシスタントへの質問を通じて、タスクを自動化したり、デジタル エクスペリエンスに関するインサイトを取得したり、詳細な分析を実行したりすることができます。

この強力な機能の組み合わせによって、IT 部門のトラブルシューティングを効率化し、最大限の生産性を実現するデジタル エクスペリエンスをユーザーに提供できます。

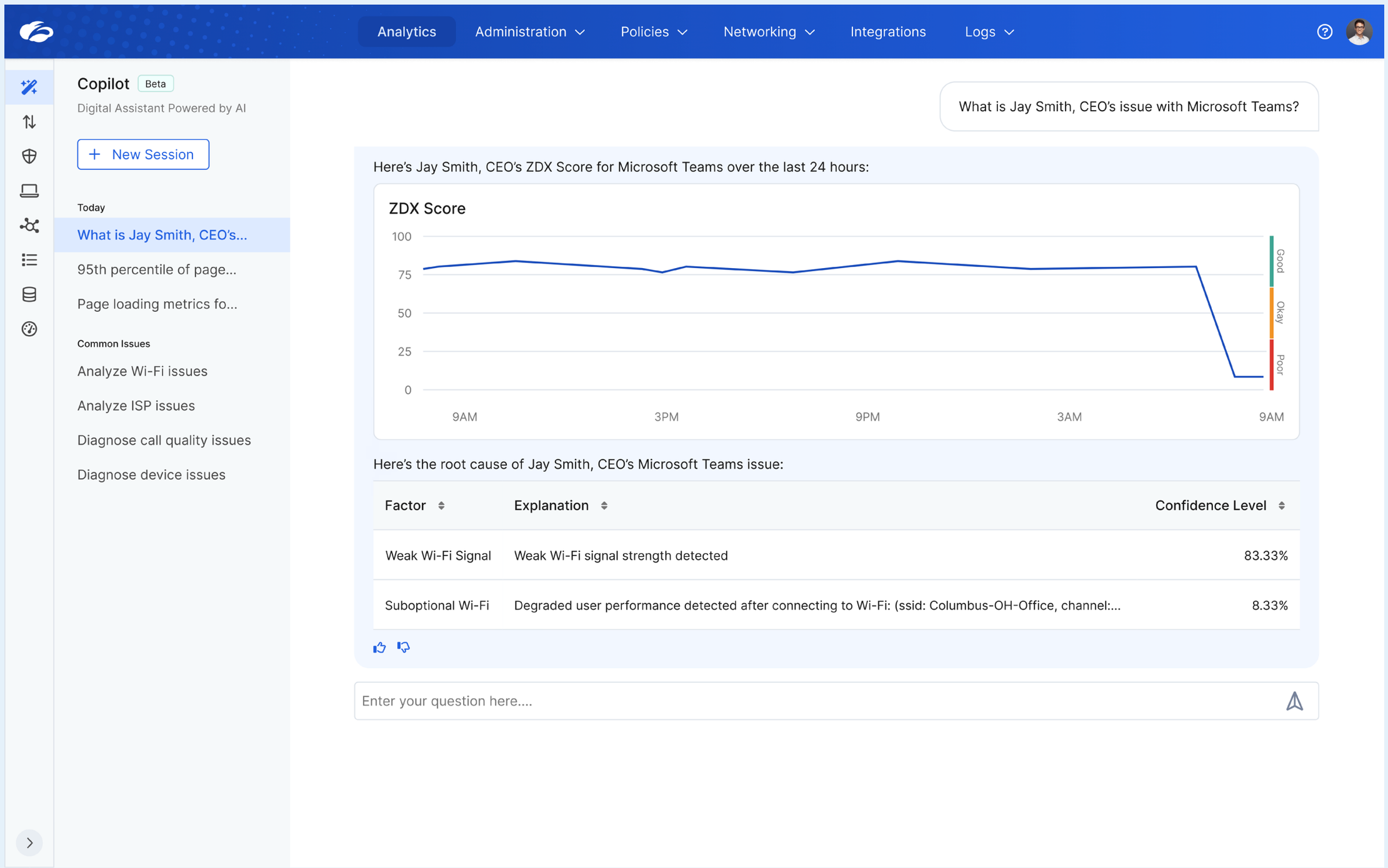


図 8: プロンプトに応答する ZDX Copilot

ビジネス インサイト

SaaS アプリケーションは、組織の生産性と柔軟性を向上させます。ただし、展開が容易なために、SaaS の利用状況の管理や最適化に関する課題も生じます。Box、Dropbox、Google Drive など、機能の重複する複数の SaaS アプリケーションのライセンスを持っていると、SaaS の費用や運用上のオーバーヘッドが増加します。未使用の SaaS のライセンスやシートもリソースの浪費につながります。

リモート ワークやハイブリッド ワークは、従業員の柔軟性と生産性に良い影響を与えます。ただし、仕事をする場所が変わるということは、本質的に従来のオフィス利用のパターンが大きく変わることを意味します。その結果、組織はオフィス スペースの利用の最適な管理方法をなかなか見つけることができず、必然的にリソースや資金が浪費されることになります。

運用を最適化し、不要なコストを排除するには、SaaS とオフィスの使用状況を可視化する必要があります。しかし、こうした可視性を得るための方法は、多くの場合、手動で時間がかかり、不正確な結果につながりがちです。データがサイロ化され、ツールが断片化されるため、IT 部門、調達部門、施設管理部門が情報に基づいた意思決定を通じてコスト削減を促進することは難しくなります。

Zscaler Business Insights は、SaaS アプリとオフィスの使用状況を正確かつ包括的に可視化します。これが可能なのは、Zscaler のインライン セキュリティ クラウドである Zero Trust Exchange が、すべてのお客様のトラフィックを処理し、誰がいつどこで稼働していて、どのリソースを使用しているかを把握できるためです。さらに、Zscaler のデータは、SAP や Workday などのビジネス ソリューションとの事前構築済みの統合によって、コスト、ライセンス、組織構造に関する情報で強化されます。AI は、結合されたデータセットを活用し、各部門のリーダーがデータに基づく意思決定を行い、リソースの割り当てや支出をより効率的なものにできるよう支援します。

SaaS を最適化するために、Business Insights はアプリケーションの使用状況を完全に可視化します。冗長なアプリを特定し、SaaS アプリのエンゲージメント、購入したプランやシート、アクティブ ユーザーに関するインサイトを提供します。また、従業員が現場にいる曜日と時間、部門ごとの利用状況など、オフィス スペースの傾向に関する有用な情報を提供し、オフィス計画やオフィス利用の最適化を支援します。

Business Insights を使用することで、組織は情報に基づいた意思決定を行い、SaaS やハイブリッド ワークの導入をより効率的に進められます。

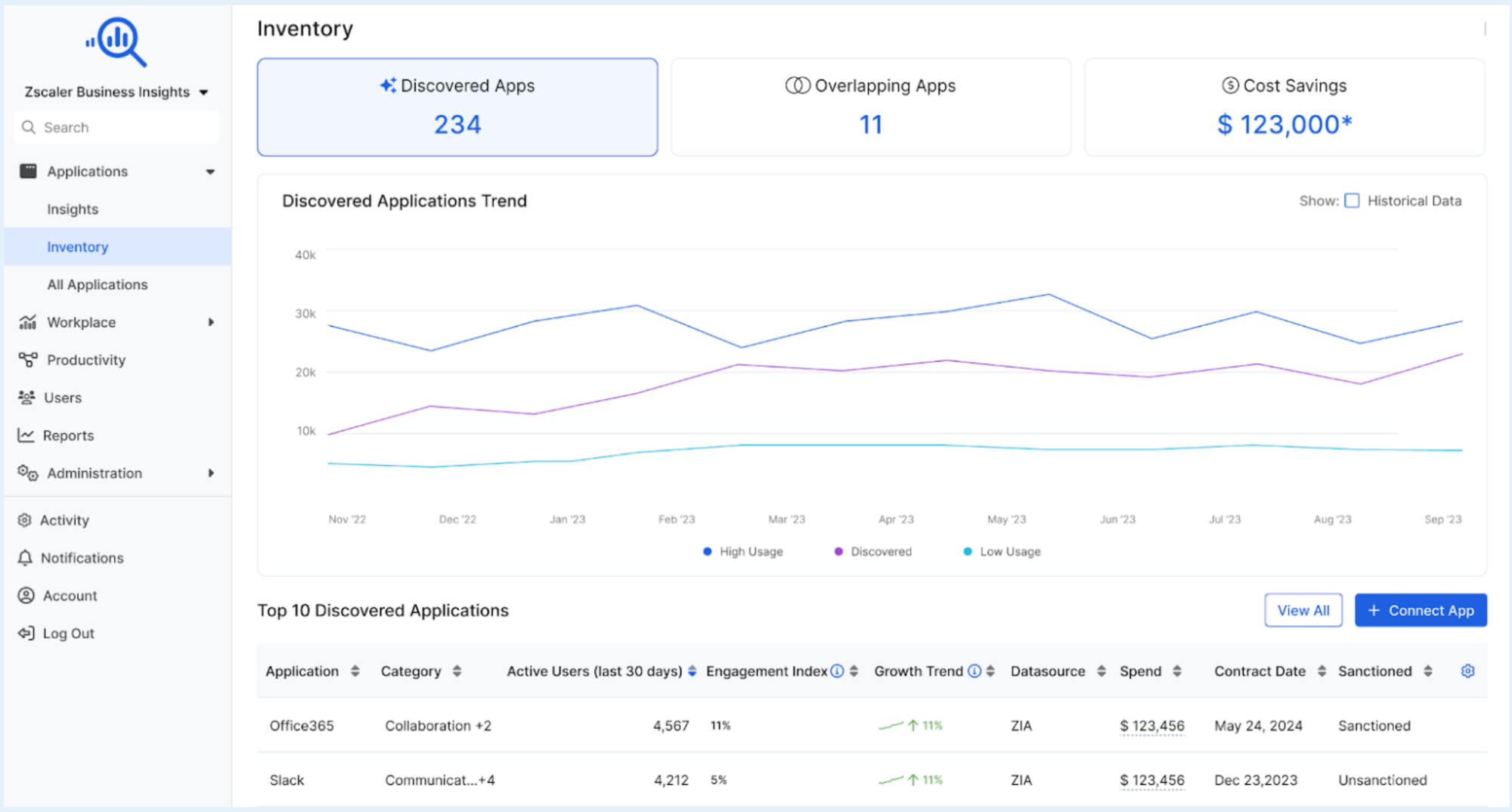


図 9: Business Insights のダッシュボード

Risk360

急速に進化する今日のデジタル環境において、組織はいっそう複雑化し、ますます多くの脆弱性に直面しています。さらに、サイバー犯罪者はその手法を進化させ続けており、最新の手口を取り入れながら、攻撃をより巧妙化させています。これらのリスクを包括的に把握するには、従来のセキュリティ ツールや手動のプロセスでは不十分です。セキュリティ ダッシュボードのサイロ化やデータの断片化によって、セキュリティ リーダーがリスクを効果的かつ総合的に評価、修復することが困難になっているためです。

さらに課題となるのが、セキュリティ規制への準拠です。組織は、業界規制の順守を示すプロセスの一環として、十分なリスク管理を実践している証拠を用意する必要があります。しかし、統一および統合されたリスク管理フレームワークがなければ、自社のセキュリティ管理の取り組みを規制要件にマッピングしにくく、リスク ポスチャーの報告やコンプライアンスの証明も難しくなります。

リスクの把握とコンプライアンスの証明のために、セキュリティ管理者はさまざまな断片的ソースから情報を集約し、レポートを作成しなければなりません。しかし、この多大な労力を要する手動のプロセスは、時間の浪費や管理オーバーヘッドの増大につながります。

こうした課題に対処するために、Zscaler では Risk360 を提供しています。これは、サイバー リスクの強力な定量化を実現する包括的かつ実用的なフレームワークです。Risk360 では、組織の Zscaler 環境、外部ソース、世界トップクラスの脅威調査チームである Zscaler ThreatLabz の長年のセキュリティ調査から得られるリアルタイムのデータが自動的に活用されます。手動でデータを集計したり、レポートをつなぎ合わせたりする必要はありません。

Risk360 は、組織のセキュリティ態勢の全体像を把握し、攻撃対象領域に関連するリスク、不正侵入、ラテラル ムーブメント、情報漏洩の可能性を定量化します。また、AI を活用したサイバーセキュリティの成熟度評価によって、高額なコンサルティングを利用することなく、ゼロトラスト化の取り組みの進捗をより正確に把握できます。このソリューションは、直感的なリスクの視覚化、リスク要因に関する詳細な情報、財務面への影響の詳細、取締役会向けレポートの作成、リスク軽減のためにすぐに応用できる実用的なインサイトを提供します。また、MITRE ATT&CK や NIST CSF などのフレームワークへの事前構築済みマッピングや、**SEC Regulation S-K Item 106** に対応した報告のサポートなどを通じて、セキュリティ コンプライアンスを支援します。

Risk360 は、リスクの体系的な評価と最小化、規制への確実な準拠、管理負担の低減、管理オーバーヘッドの軽減を実現します。このソリューションもまた、ゼロトラストと AI を活用して組織を保護、最適化する Zscaler の力の一例と言えます。

Risk 360
Dashboard
Factors
Insights
Financial Risk
Resilience Risk
Reports
Administration
Alerts

Dashboard

Organization Risk Score

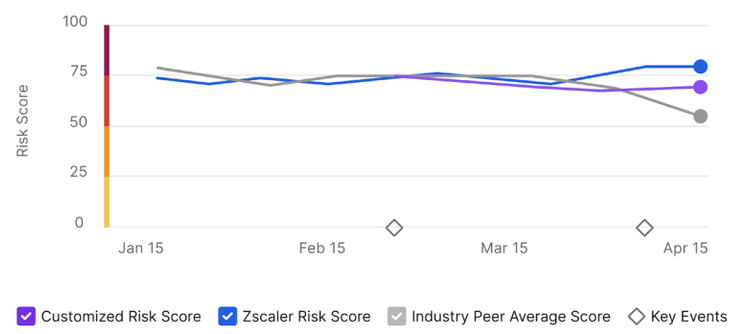
External Attack Surface 75
Low Medium High Critical

Compromise 85
Low Medium High Critical

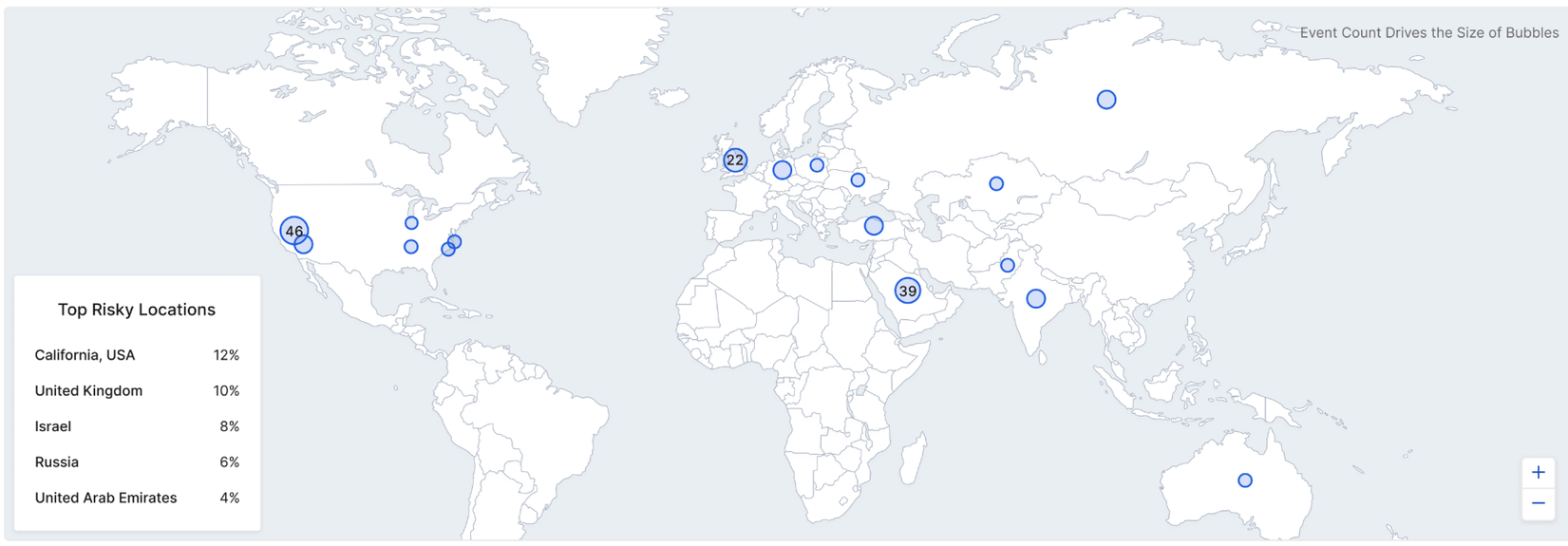
Lateral Propagation 79
Low Medium High Critical

Data Loss 93
Low Medium High Critical

Risk Score Trend



Risk Events by Location



Top Risky Locations

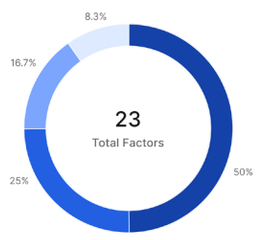
California, USA	12%
United Kingdom	10%
Israel	8%
Russia	6%
United Arab Emirates	4%

Distribution of Contributing Factors to Your Risk

By Category | By Entity

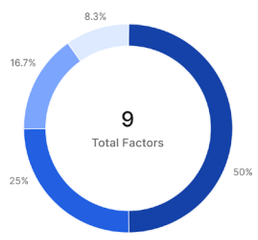
View All

Workforce



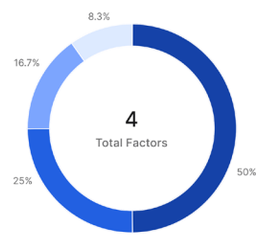
Short key takeaway sentence (dynamic) goes here

3rd Parties



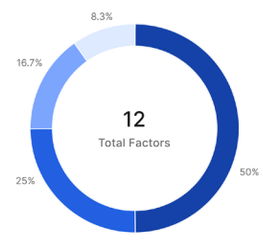
Short key takeaway sentence (dynamic) goes here

Applications



Short key takeaway sentence (dynamic) goes here

Assets



Short key takeaway sentence (dynamic) goes here

External Attack Surface | Compromise | Lateral Propagation | Data Loss

Top 10 Factors

View All

Category	Factor Name	Your Score ↓	Last 30 Days	Entities	Licensed?	Recommended Actions
External Attack Surface	Outdated SSL / TLS - servers running vulnerable SSL/TLS versions that should be removed	10 / 10			Y	Remove older TLS version support.
Data Loss	DLP Policies configured	9 / 10			N	Apply patches and retire old services.
Lateral Propagation	Posture profile being used in access policies	8 / 10			Y	Rename to use ambiguous namespaces or prevent leakage it...
Compromise	Advanced Threat Settings	7 / 10			N	Configure Advanced Threat Settings to protect against attacks.
External Attack Surface	Known vulnerabilities (CVEs) - X	6 / 10			Y	Investigate X CVEs
Compromise	Scanned SSL Traffic	5 / 10			Y	PulseSecure VPN deprecated in last 3 months
Lateral Propagation	Application segments (ports) defined with wide open ports	4 / 10			N	Harden consumer facing servers that can't be made invisible
Data Loss	Data being uploaded by risky regions by volume	3 / 10			Y	PulseSecure VPN deprecated in last 3 months
External Attack Surface	Public Cloud Instance Exposure - Bad actors can discovery and leverage these exploits	2 / 10			Y	Harden consumer facing servers that can't be made invisible
Compromise	Browser Control Settings	1 / 10			N	PulseSecure VPN deprecated in last 3 months

図 10: Risk360 のダッシュボード

まとめ

サイバー リスクと競争圧力をめぐる課題は、かつてないほどその厳しさを増しています。組織が生き残るためには、サイバー脅威や情報漏洩を阻止すると同時に、可能な限り効率的な事業運営を実現しなければなりません。幸い、ゼロトラストと AI という強力な組み合わせによって、これら両方の課題に最適な形で対処できます。

Zscaler はゼロトラスト アーキテクチャーの先駆者であり、継続的にイノベーションを実現し、世界中の無数のお客様のリスクを体系的に軽減しています。Zero Trust Exchange プラットフォームは、前例のない規模と多様な統合を誇り、データと AI/ML において戦略的優位性を備えています。Zscaler によって、これまでにない方法で組織を保護、最適化することが可能なのです。

毎月開催のウェビナー「**Zero Trust 101: Start Your Journey Here**」では、ゼロトラストの詳細や、Zscaler が他社にない形でこの最新のアーキテクチャーを実現できる理由について紹介しています。ぜひご登録ください。なお、このウェビナーは、ゼロトラストの取り組み全体のガイドとして設計された 3 部構成シリーズの第 1 部です。

このホワイト ペーパーで取り上げた AI 機能などを実際にご覧になりたい場合は、**こちら**からデモをご依頼ください。

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™ プラットフォームは、ユーザー、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、数多く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 150 拠点以上のデータ センターに分散された SSE 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.com/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. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com/jp**

Zero Trust Everywhere