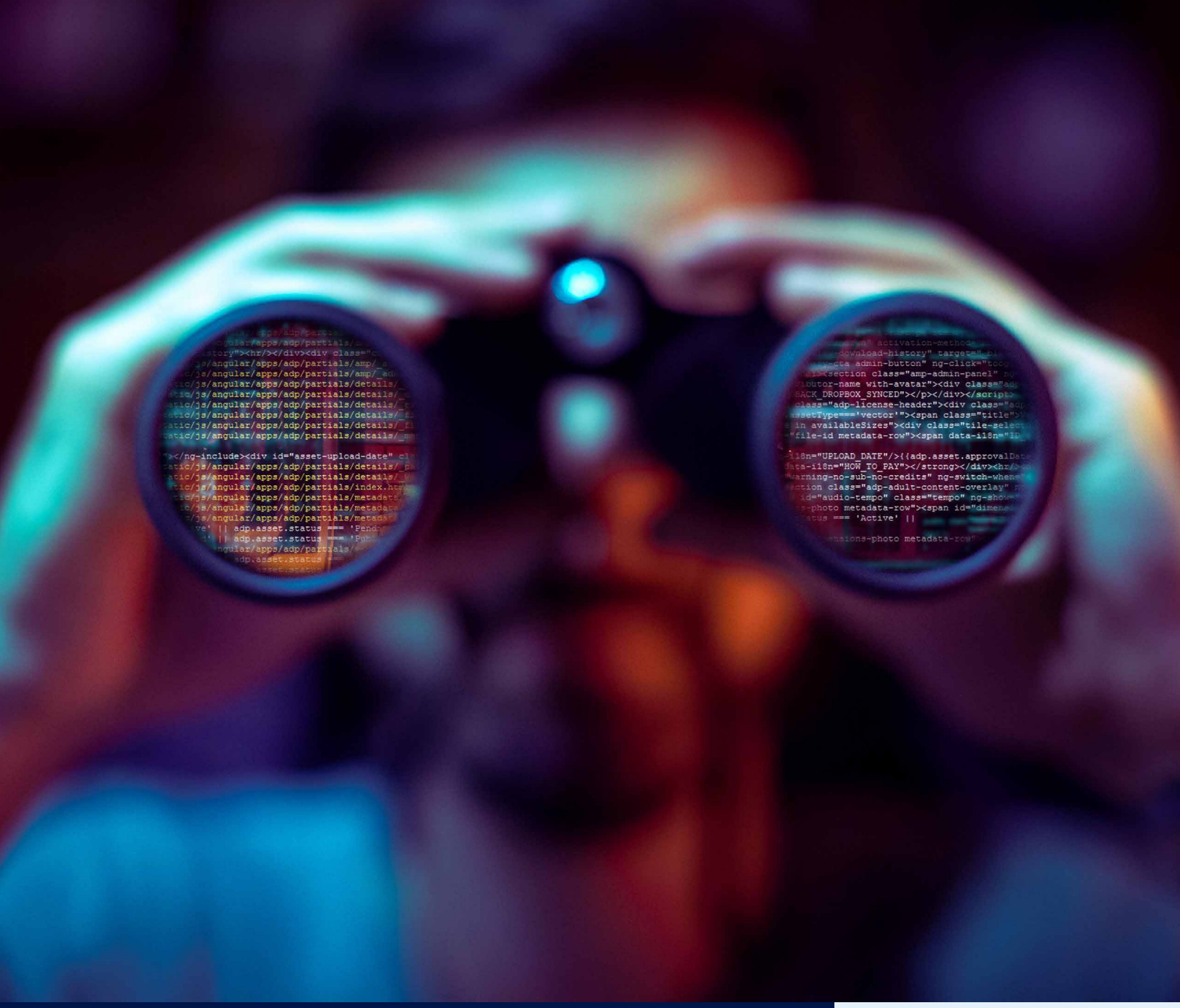


Zscaler Ransomware Kill Switch

OT/IoT ネットワークのための自動インシデント対応

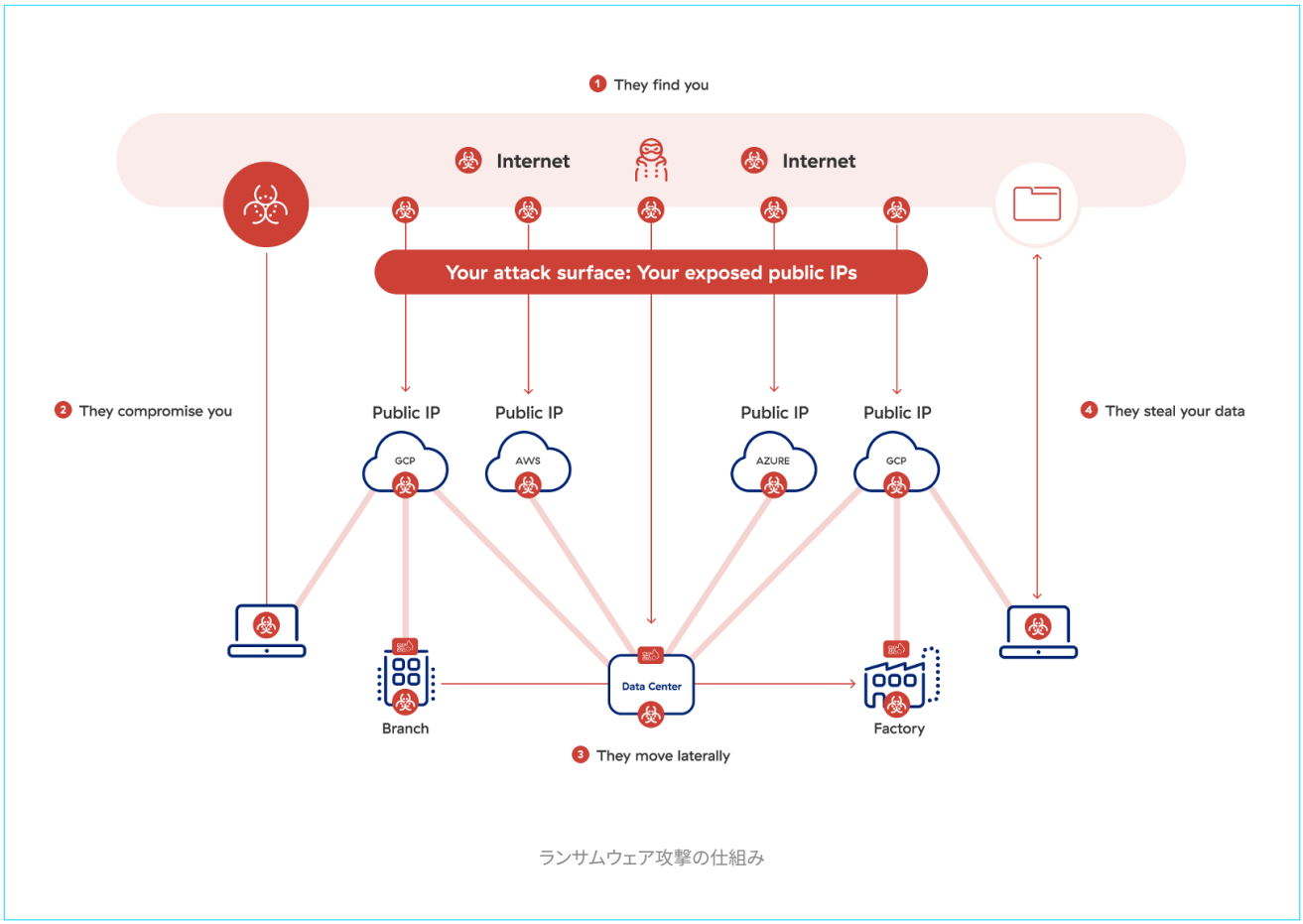
© 2024 Zscaler, Inc. All rights reserved.

ソリューションの概要

現在の課題

世界中の重要インフラ ネットワークには、保護されていないアイデンティティーと脆弱なエンドポイントが多数存在するため、依然としてサイバー攻撃の主な標的となっています。本当の脅威は初期の侵害だけではありません。アクセスを獲得した後に攻撃者が行うラテラル ムーブメント、ランサムウェアの展開、悪意のあるペイロードの配信も重大な懸念事項です。OT/IoT は現在、サイバー犯罪者の格好の攻撃対象となっており、Zscaler ThreatLabz の調査でも、これらを対象とした攻撃が前年比で 400% 増加していることがわかっています。中でもランサムウェア攻撃は最も頻繁に発生しており、侵害全体の 61% が OT に接続された組織を標的にしています。

最も防御されたネットワークであっても侵害やランサムウェアのリスクはゼロではなく、フィッシング攻撃や資格情報の窃取が発生したり、悪意のある人物が境界をすり抜けて侵入したりするおそれがあります。多くの組織は通常、侵害された VLAN 全体をシャットダウンすることで脅威を封じ込めますが、これは重要なトラフィックを中断し、運用を停止させます。また、調整されていないアラートと不完全な情報では、進行中の攻撃に効果的に対処することはできません。



ランサムウェア攻撃の仕組み

© 2024 Zscaler, Inc. All rights reserved.

必要な対策

EPA、CISA、FBI はシステム オペレーターに対し、サイバーセキュリティを強化するための指針としてゼロトラストの採用を求めた大統領令に従って取り組むことを強く推奨しています。ネットワークおよびセキュリティのリーダーには、OT/IoT 環境のゼロトラスト セグメンテーションに加え、以下の領域にも注力することが求められます。

きめ細かな封じ込めで水平方向への拡散を制限

事前設定された自動インシデント対応で侵害に適切に対処

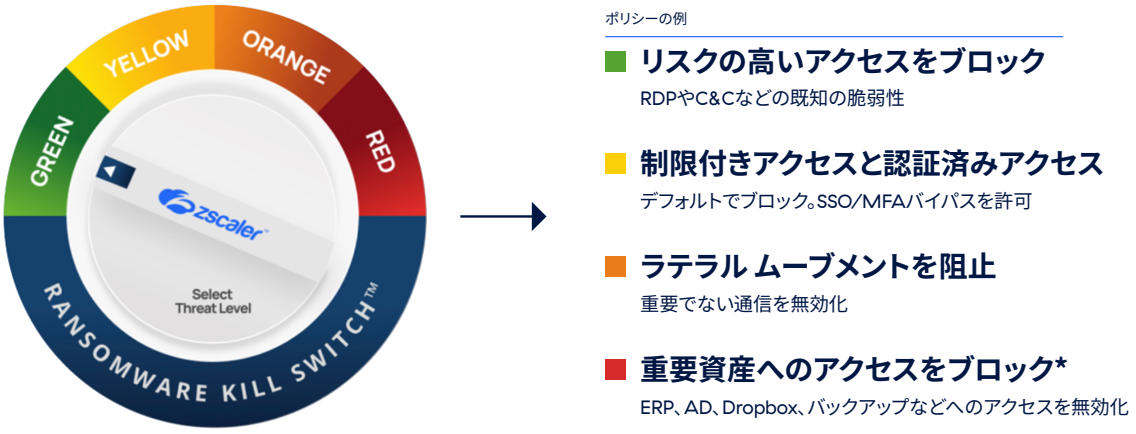
組織の IT ネットワークとコア ネットワーク間など重要な境界層で厳格な封じ込めを実行

疑わしいポートとプロトコルを効果的にシャットダウンしビジネスの稼働時間を最大化

Zscaler のソリューション

新しい Zscaler Ransomware Kill Switch では、ワンクリックで攻撃対象領域を削減できます。Zscaler Zero Trust Device Segmentation ソリューションに統合されたこの機能は、既知の脆弱なプロトコルやポートを段階的に制限し、病院全体や工場のフロアなど重要なネットワークへのアクセスを瞬時に無効化します。すべてに重大度が事前に設定されているため、ビジネスのダウンタイムを最小限に抑えられます。

Ransomware Kill Switch は、多層型のポリシー施行ポイントとして機能し、進行中の侵害に対して段階的なインシデント対応を行うため、既存のセキュリティ ツールへの投資の増強につながります。Ransomware Kill Switch の各層には、「仮想ヒューズ」またはデフコン レベルに類似した機能があります。この機能により、事前定義されたエスカレーション パスに従ってエンドポイントとの間の不要なネットワーク通信がすべてブロックされるため、水平方向への拡散の阻止と攻撃対象領域の大幅な削減が可能になります。



Zscaler Ransomware Kill Switch

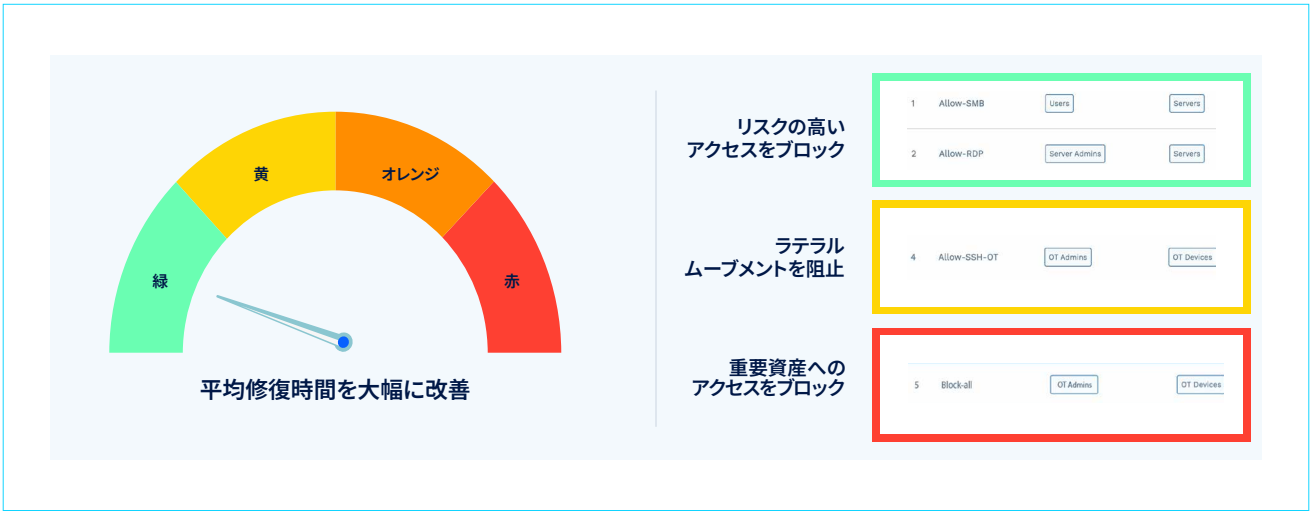
© 2024 Zscaler, Inc. All rights reserved.

ユース ケース

Ransomware Kill Switch の代表的なユース ケースとして、以下が挙げられます。

インシデント対応の自動化

Zscaler Ransomware Kill Switch では、ユーザーが選択した方法で攻撃対象領域を削減できます。事前に設定された重大度を選択すると、脆弱な既知のプロトコルやポートが段階的に制限され、製造ラインや病院フロアなどのネットワーク全体へのアクセスが即座に無効化されます。脅威に合わせて調整するだけで業務の生産性を維持できるため、侵害の混乱の中で不確かな推測をする必要がなくなります。



このソリューションは、業務を中断することなく、重要でないデバイス通信を無効化して脅威のラテラル ムーブメントを阻止します。また、IoT デバイスや OT システム、エージェントをインストールできないデバイス上のランサムウェアなどの高度な脅威も無力化します。

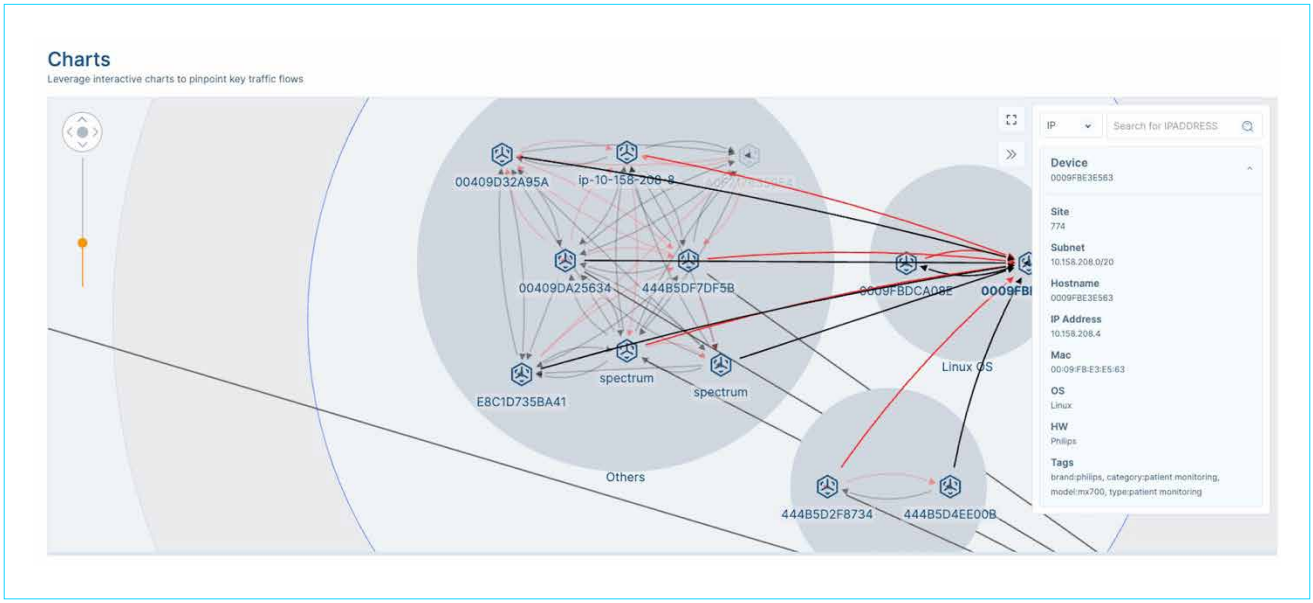
可視性と制御の強化

課題

- **可視性：**ネットワーク デバイスのインベントリーは常に流動的です。すべてのデバイスが特定されないまま、常に変化している状況においては、デバイス間の通信を保護することは不可能です。
- **制御：**このような複雑で変化し続ける環境では、通信できるデバイスと通信すべきデバイスを制御することが不可欠であるものの、基本的なセキュリティ対策の実施すら非常に難しくなります。

見えないものは保護できません。ほとんどの IT 組織では、すべてのアクセス スイッチから東西のトラフィックを把握することは不可能であるため、水平方向のトラフィックを視覚化することはできません。Zscaler ソリューションは、保護されたすべてのエンドポイントに出入りするトランザクションを完全に可視化し、リアルタイムのビジネスおよびセキュリティ ポリシーの作成と施行を可能にします。

© 2024 Zscaler, Inc. All rights reserved.



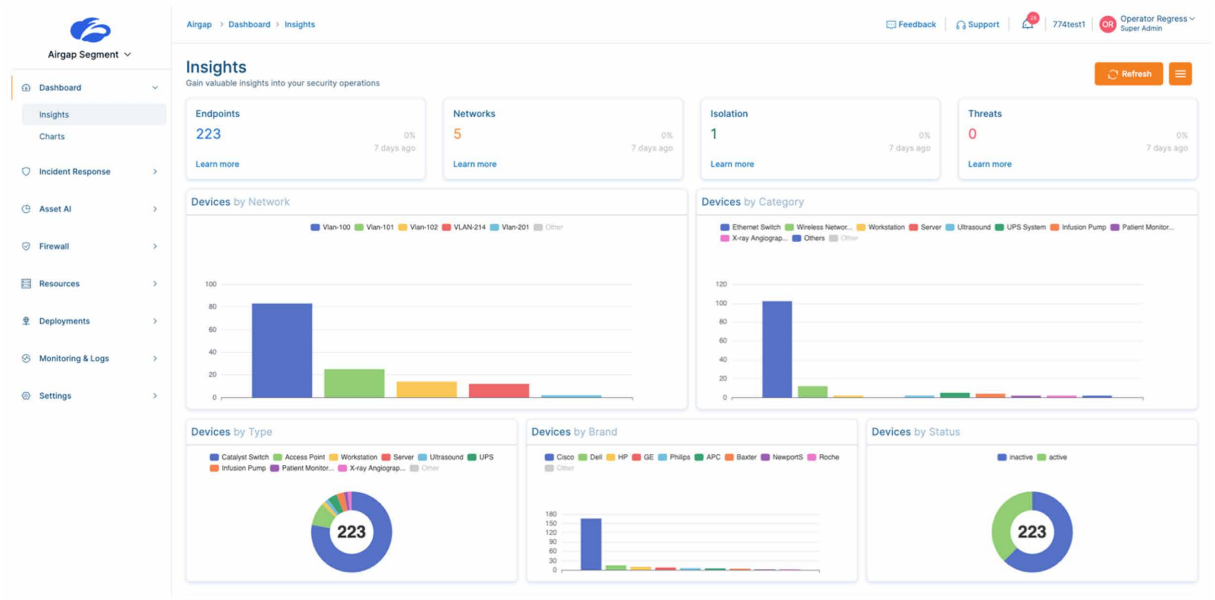
重要インフラの保護

Zscaler は、API を介して Ransomware Kill Switch を完全に制御します。IT 組織は、これらのプログラム可能なインターフェイスを使用して、セキュリティ情報とイベント管理 (SIEM)、セキュリティ オーケストレーションの自動化と対応 (SOAR)、EDR/XDR ソリューションなどの既存のセキュリティ オーケストレーション ツールを有効にできます。こうすることで、インシデント対応の自動化、侵害されたエンドポイントの瞬時の隔離、感染の影響範囲の封じ込めが可能になります。

これにより、既存のネットワークとセキュリティのインフラへの投資を保護しながら、セキュリティ態勢をすぐに改善できます。

侵害の混乱の中でも、事前設定された重大度で脆弱なプロトコルとポートを瞬時に制限すれば、生産性を維持できます。

© 2024 Zscaler, Inc. All rights reserved.



Zscaler Zero Trust Device Segmentationのダッシュボード

Zscaler の技術専門家によるデモ

当社の技術専門家とのデモを依頼して、重要インフラを保護する Zscaler ソリューションの詳細をご確認ください。

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。

© 2024 Zscaler, Inc. All rights reserved. Zscaler™、Zero Trust Exchange™、Zscaler Internet Access™、ZIA™、Zscaler Private Access™、ZPA™、**zscaler.com/jp/legal/trademarks**に記載されたその他の商標は、米国および/または各国の Zscaler, Inc.における(i)登録商標またはサービス マーク、または(ii)商標またはサービス マークです。その他の商標はすべて、それぞれの所有者に帰属します。

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com.jp