cisco SECURE

The bridge to possible

Cisco Secure Access Roadshow

Cisco Secure Access ご紹介

クラウド時代、今必要な SSE

シスコシステムズ合同会社　セキュリティ事業　サイバーセキュリティ製品担当
福留 康修

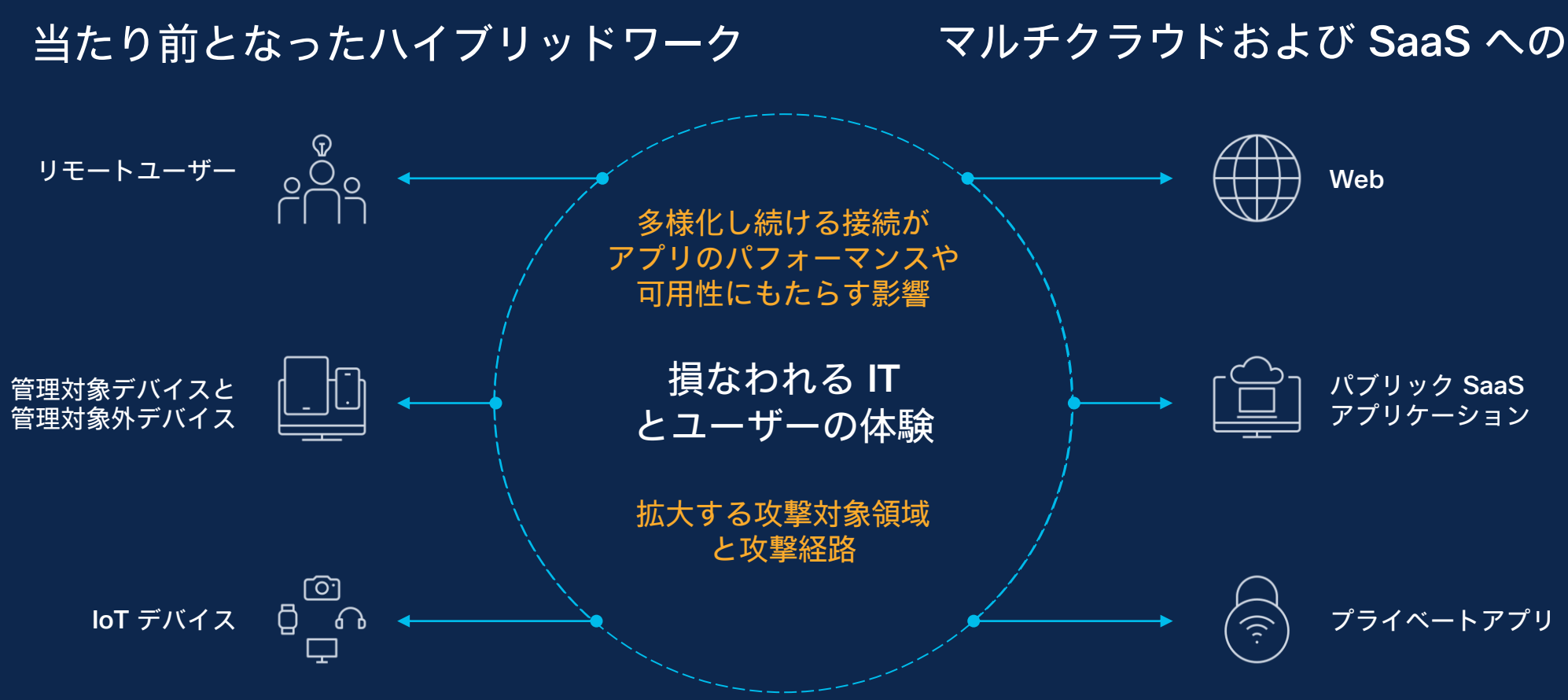
2023/11/28

本セッションの内容

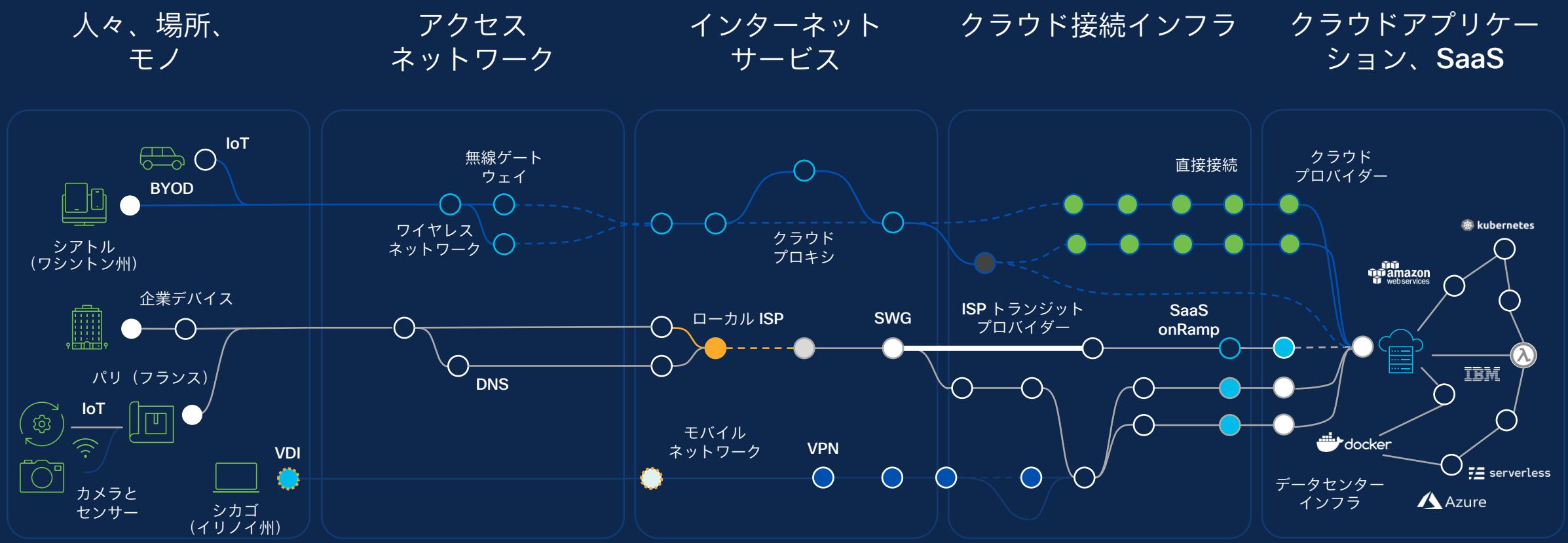
1. クラウド時代、なぜ今 SASE/SSE アプローチが必要なのか？
2. Cisco Secure Access ご紹介

1. クラウド時代、なぜ今 SASE/SSE アプローチが必要なのか？

安全な接続上の課題にまつわるリスク



複雑化したインフラ



複雑さの一途をたどるこれからのインフラ設計・管理・運用負担

セキュリティも加わると難易度は指数関数的に高くなる

人々、場所、モノ

アクセスネットワーク

インターネットサービス

クラウド接続インフラ

クラウドアプリケーション、SaaS

さらに難しくなるサイバー レジリエンス向上

セキュリティイノベーションはパッチワーク

データ漏洩

ランサムウェア

ラテラルムーブメント

Web の脅威

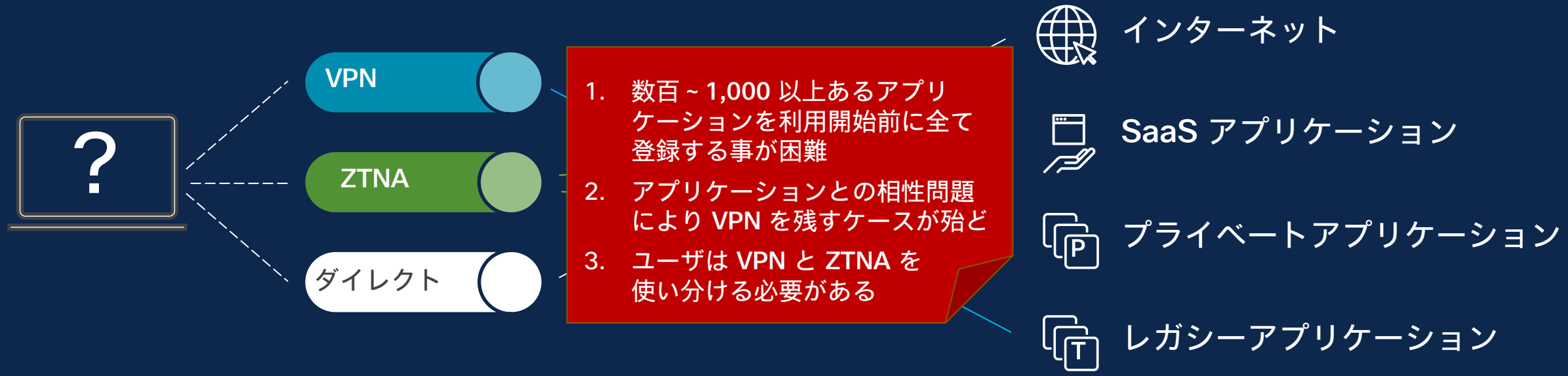
クレデンシャルの盗用

スパム

新たな脅威が新たなベンダーを生み、顧客に重荷を負わせている

進まないゼロトラスト アクセスの展開

アプリケーション接続の複雑さ

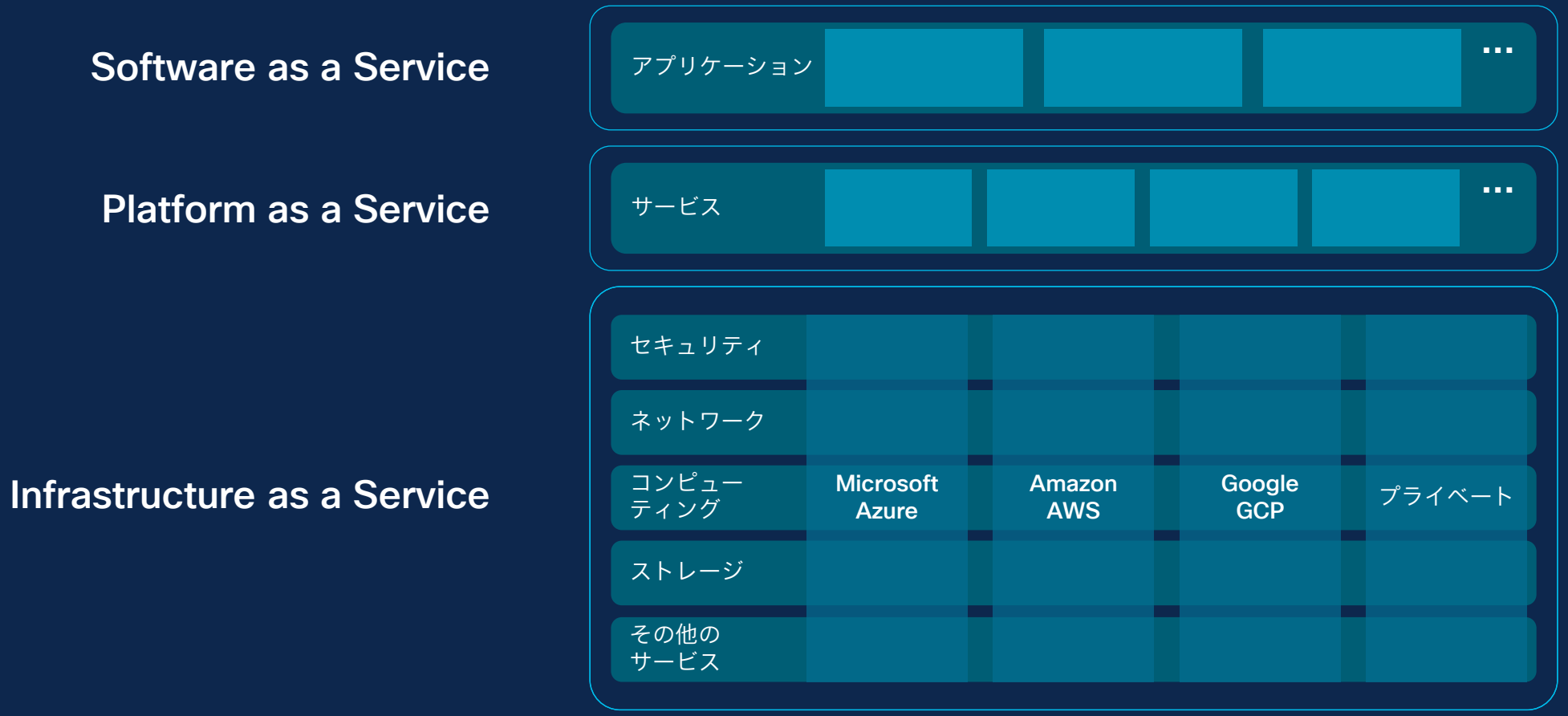


ご参考
ゼロトラストアクセスに不向きなアプリケーション

1. クライアント間トラフィック
   - ピアツーピア VoIP など
2. サーバーからクライアントへのトラフィック
   - リモートデスクトップ、リモートアシスタンスなど
3. 固有のクライアント IP を必要とするアプリケーション
   - SMBv1 など
4. SRV DNS レコード* を必要とするアプリケーション
   - Active Directory、Kerberos、SIP、SCCM など
5. TCP 3 ウェイハンドシェイクの後、サーバーが最初のデータペイロードを送信する必要があるアプリケーション
   - MySQL Studio など

*参考：SRV DNS レコード

ハイブリッド マルチクラウドの世界



さらに状況の悪化が予想される、つぎはぎだらけのセキュリティツール導入

全体把握と整理に役立つ
セキュリティ リファレンス アーキテクチャ

*1 本セッションの対象外 (別途、ご紹介可能)

技術の基盤となる SASE/SSE アプローチ

超分散型の世界におけるセキュリティ戦略の基盤

*リモートワーカーに対応

2. Cisco Secure Access ご紹介

Cisco Secure Access ご紹介

ゼロトラストに基づく統合クラウドセキュリティで防御を近代化

Cisco Secure Access とは

ゼロトラストに基づく統合型クラウドセキュリティで防御体制を近代化した **SSE**

ユーザーにとって より快適に

スムーズなユーザー エクスペリエンスで仕事を支援

IT をより使いやすく

コストを削減し効率を向上

すべての人にとって より安全に

リスクを緩和しビジネスのレジリエンスを強化

想像してみてください

誰にとってもより安全で簡単なサイバーセキュリティを

ユーザにとってより快適に

ユーザーにとってより快適になることによる成果

生産性の向上

~ 50%

プライベート・アプリケーションにアクセスするための手順を 50% 削減 *

アプリへのアクセスを完全に透明化

「生産性は、世界トップクラスの組織が収益性を高め、競争力を強化し、優秀な人材を惹きつけ、維持し、革新と成長を推進するために極めて重要である」**

*ソース：UI デザイン フレームワーク – Cisco 2023

**ソース：国際開発機構（ODI）、2023 年 2 月

Cisco Secure Access – どこへでも利用可能

ステップ 1
認証

ステップ 2
仕事を開始

ZTNA
VPN
SaaS
直接

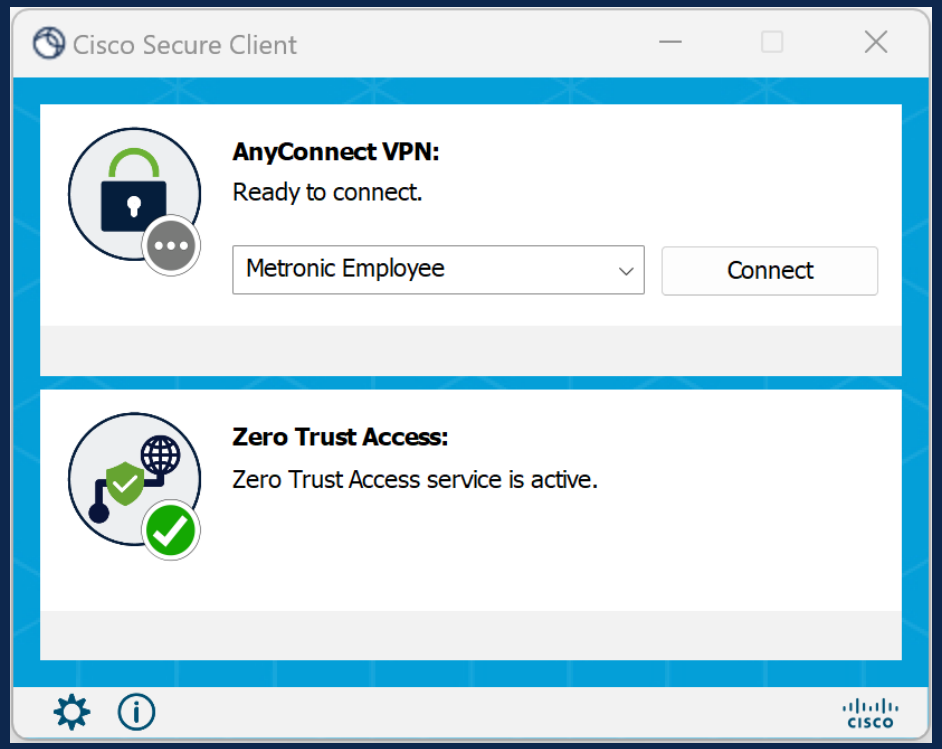
Secure Access

プライベート アプリ
レガシーなアプリ
SaaS アプリ
インターネット アプリ

コネクティビティ、アクセス・コントロール、セキュリティはお任せください

ユーザにとって快適な環境をご提供

Cisco Secure Client Zero Trust Access モジュール

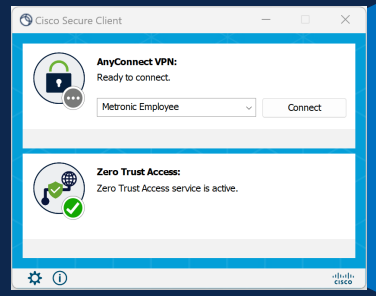


- フリクションレス ユーザーエクスペリエンス
- きめ細かなアクセス制御によるプライベートリソースへのプロキシ (ZTNA Proxy) アクセス
- TPM/hardware enclave キー ストレージによるサービスマネージドクライアント証明書
- TCP および UDP アプリケーションをサポート
- シスコおよび 3rd パーティ VPN クライアントとの相互接続
- 次世代プロトコル (MASQUE + QUIC)

リモートユーザの接続方法

Internet Access
Private Access
Secure Tunnel

Cisco Secure Client



1 つのクライアントで対応

VPN

ZTNA

www

Browser

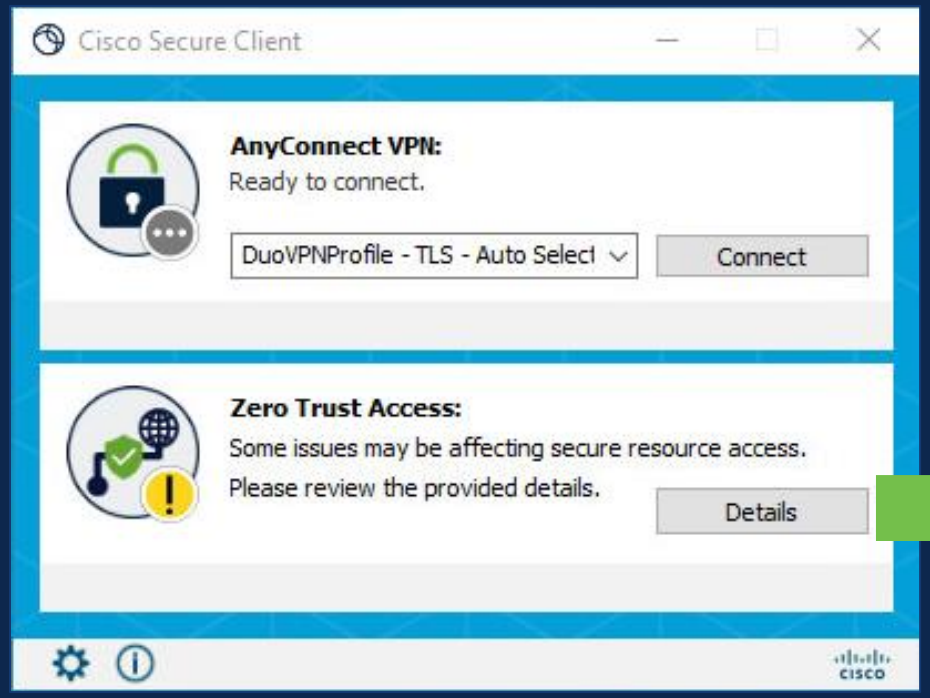
AnyConnect VPN
→ 認証 と ポスチャ @ VPN 接続時
→ TLS/DTLS/IKEv2 トンネル
→ インターネット と プライベートトラフィックを処理 (All ports & protocols)
→ SAML, (+) 証明書, & (+) マルチ証明書 認証

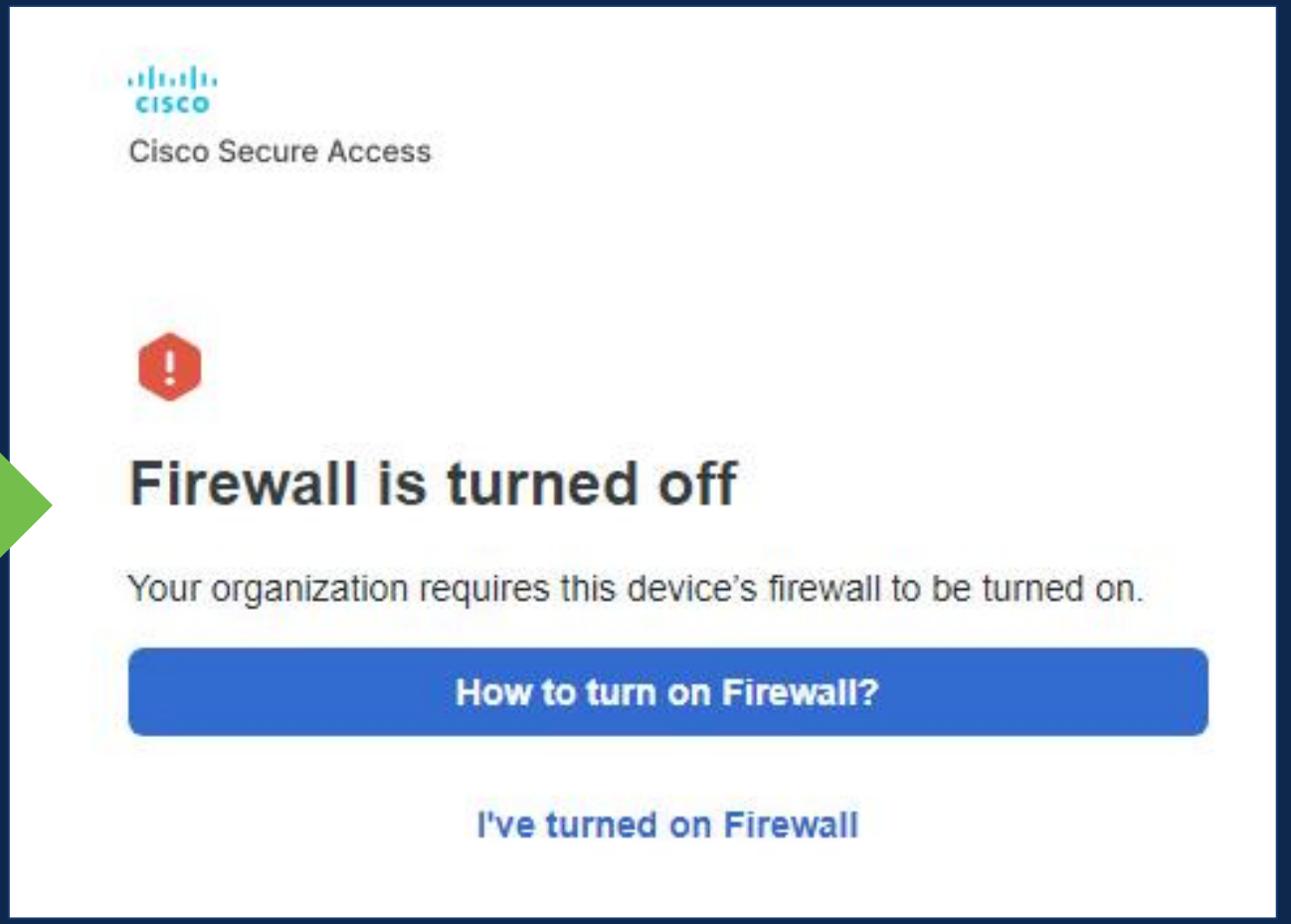
ZTNA Module
→ セッションごとの認証 と ポスチャ
→ QUIC トンネル (MASQUE proxy)
→ プライベートトラフィックを処理 (TCP/UDP All ports & protocols)
→ SAML 認証 + 自動更新

Web Roaming Module
→ デバイス登録 (profile)
→ インターネット Web Traffic を処理 (80/443)

Clientless ZTNA
→ SAML/Cookie をサポートするブラウザからアクセス可能
→ User-Agent ベースのポスチャ (geolocation, browser version, OS)
→ Web アプリケーションのみ

クライアント ベース ポスチャ





ポスチャ チェック機能

アプリケーションへのアクセス前の承認チェック

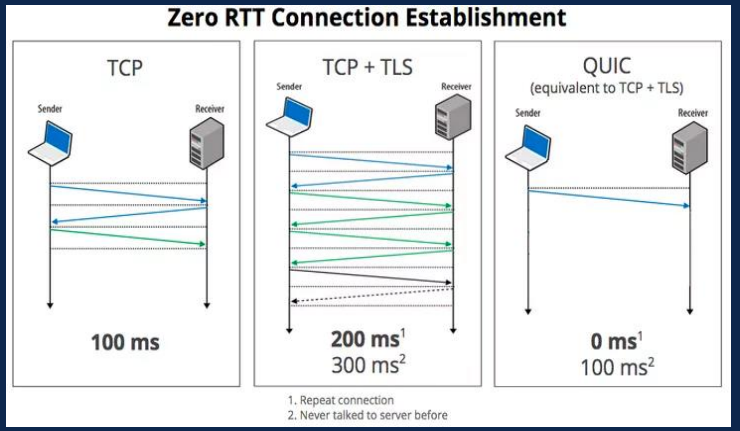
セッションごとの承認とアクセスチェック

サポート対象の **AV** ベンダー：
クライアントベースの **ZTNA**

RAVPN

	VPN	ZTNA ブラウザ	ZTNA クライアントベース
オペレーティングシステム	✓	✓	✓
位置情報チェック（アクセスポリシーに移動）	✓	✓	✓
Firewall	✓		✓
ディスク暗号化	✓		✓
ブラウザチェック		✓	
マルウェア対策	✓		✓
ファイルチェック	✓		
レジストリチェック（**Windows** のみ）	✓		
プロセスチェック	✓		
システムパスワード			✓
証明書チェック	✓		

QUIC と MASQUE による優位性



- QUIC とは：
  - UDP ベースのストリーム多重化/暗号化トランスポートプロトコル
  - 2012 年に Google Chrome で初めて採用
  - HTTP/3, iCloud Private Relay, SMB over QUIC, DNS over QUIC などに使用
  - TLS over TCP に比べてレイテンシーが縮小され、次世代のインターネットトラフィックに最適化
- MASQUE (Multiplexed Application Substrate over QUIC Encryption) とは：
  - IETF のワーキンググループで、QUIC プロトコル上の次世代プロキシ技術に焦点が当てられている
  - HTTP/2 および HTTP/3 のデータとして、複数のプロキシされたストリームおよびデータグラムベースフローのためのメカニズムを提供
  - 2021 年から iCloud Private Relay で使用
  - HTTP/2 と HTTP/3 の拡張は、UDP とIP トラフィックのシグナリングとカプセル化を可能にする

MASQUE + QUIC を組み合わせることで、Web および非 Web プロトコルの両方の TCP、UDP　および IP トラフィックのための効率的かつセキュアなトランスポートメカニズムを提供

Apple デバイスからのゼロトラスト・アクセスを簡単に拡張

COMING SOON

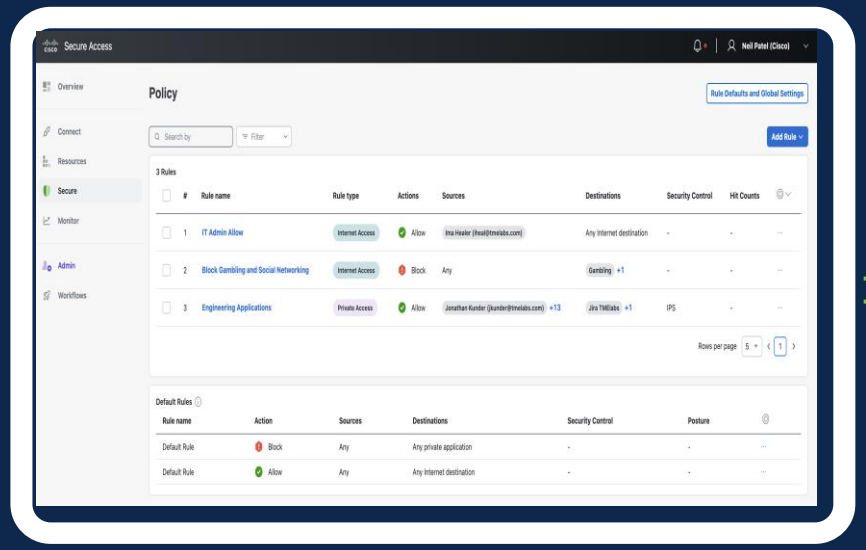
- 前世代の ZTNA ではなくエンタープライズ・リレー
- アプリケーションごと、ドメインごとのプロキシはアプリケーション内で直接実行され、デバイス全体の継続的な VPN とは相違
- ワークロードに直接接続可能なエンタープライズ・プライバシー、iCloud Private Relay 対応
- 100% 標準技術ベース。業界をリードするテクノロジーを基盤： MASQUE とQUIC
- ウェブアプリケーションだけでなく、すべてのアプリケーション、ポート、プロトコルに対応

Apple iCloud プライベートリレーによるエンタープライズリレー

IT をより使いやすく

IT をより使いやすく

クラウドセキュリティの統合によるコスト削減と効率性の向上



より高い効率

- *シングル*エージェント、コンソール、アイデンティティ、ポリシー管理
- デジタル・エクスペリエンス・モニタリング（DEM）*1
- 単一の SLA*1

より低いコスト

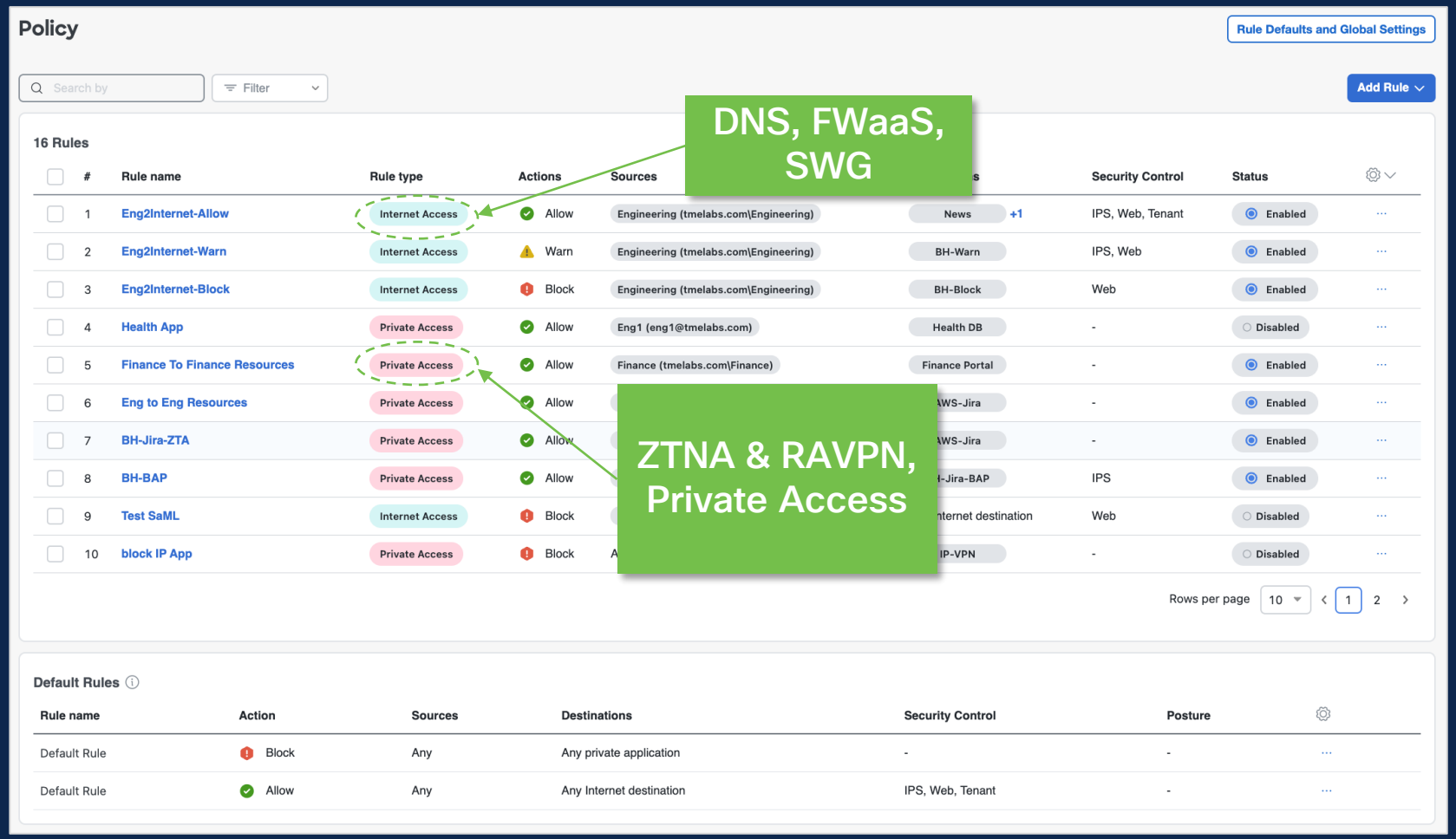
- 統合ライセンス
- ハードウェアの削減
- エコシステム

トラフィックを確認、ポリシーを設定し、リスクを分析するための 1 つの場所

*1 近日対応予定

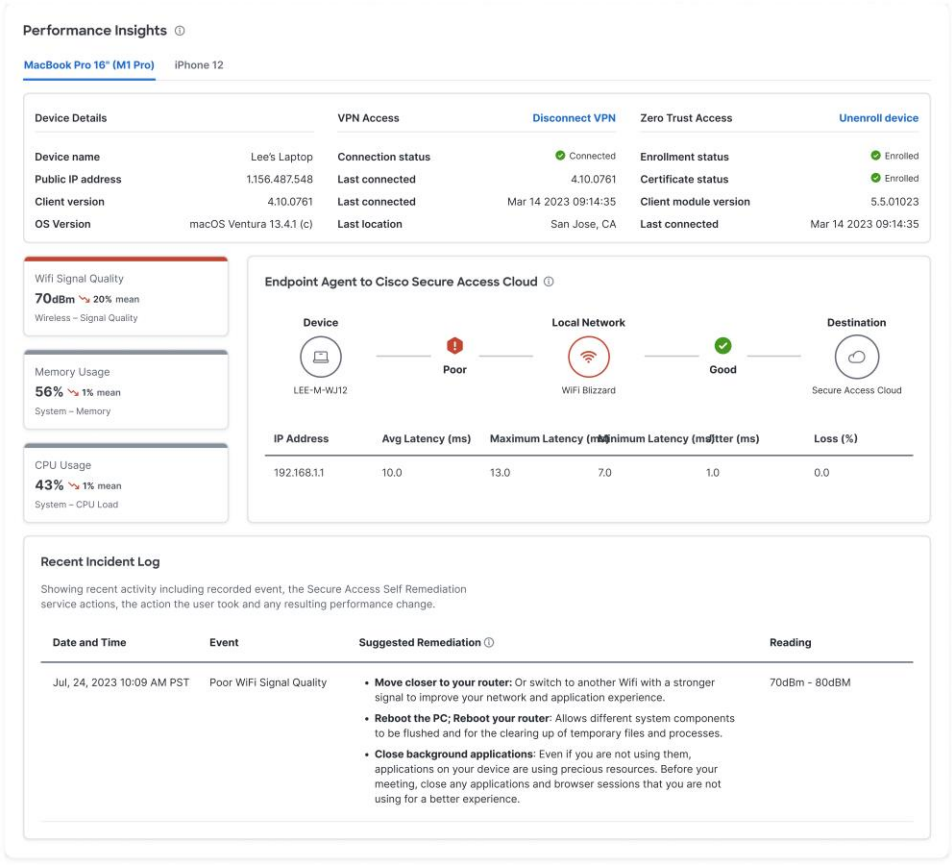
ユニファイド ポリシー

- SSEのポリシーは以下のように構成
  - パブリック・インターネット/SaaSアクセス・コントロール・ポリシー
  - プライベート・アクセス・コントロール・ポリシー
- 各ルールには明示的な「ルール・タイプ」が定義付けされ、ポリシー設定を統一したビュー
- ルールは各実施エンジンで順番に評価される



Digital Experience Monitoring

IT / セキュリティチームは問題の特定と解決を加速できる



画面は開発中のものであり変更されることがあります

ユーザー、アプリケーション、ネットワーク接続の健全性とパフォーマンスを監視

ユーザーのエンド・ツー・エンド・エクスペリエンスの詳細を自動的にマイニングし、IT / セキュリティ・スタッフが問題を迅速に解決できるようにすることで、ユーザーの生産性を最適化

DEM* モニタリング例

- エンドポイントのパフォーマンス - CPU、メモリ、WiFi
- ネットワーク・パフォーマンス - エンドポイントからセキュア・アクセスまで
- トップ 20 の SaaS アプリケーション パフォーマンス
- ユーザー固有のイベント

*1 近日対応予定

セキュリティ / IT チームの成果

導入初期の顧客は大きな価値を見出している

ビジネス インパクト

セキュリティ担当者は、よりインパクトの大きいタスクに集中

65% ポリシーの確立と実施に費やす時間を節約

オペレーション・コストの削減

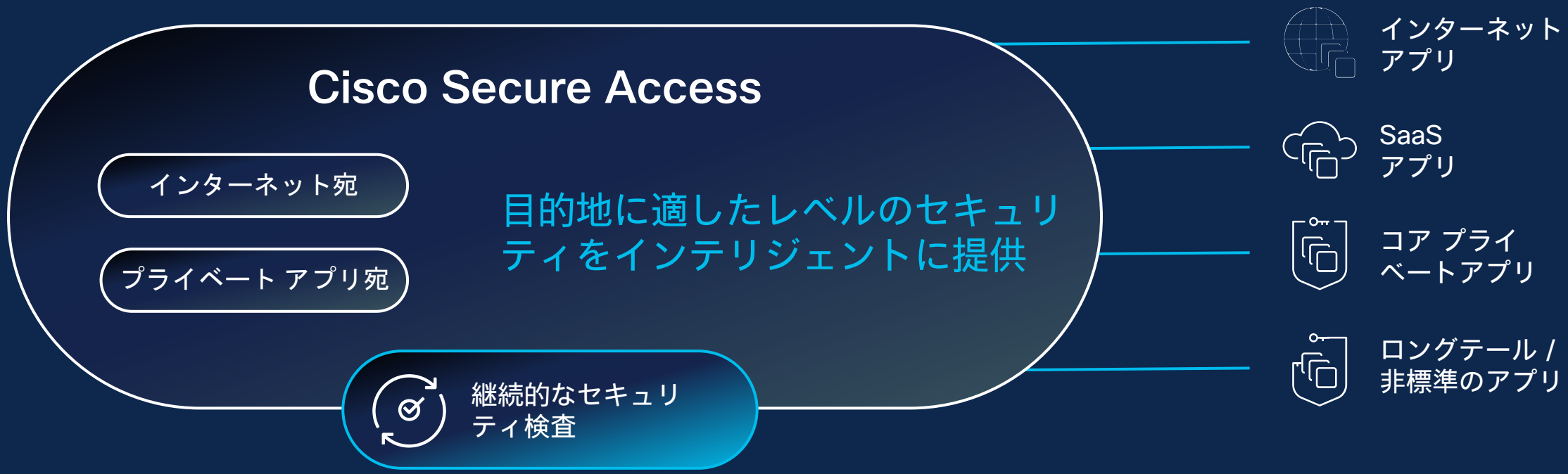
67% サービスおよび物理的機器の管理が減少

*出典 Forrester Total Economic Impact 調査、Umbrella SIG/SSE、2022 年

すべての人にとってより安全に

高度なサイバーセキュリティのメリット

より多くのブロック、より迅速な調査、完全な修復



改善された セキュリティの有効性

- より深い可視性と洞察
- アラート量の削減
- より強力な脅威相関
- より迅速な検知

- 高いアナリスト効果
- 最も特権的なアプリへのアクセス
- 露出の低減

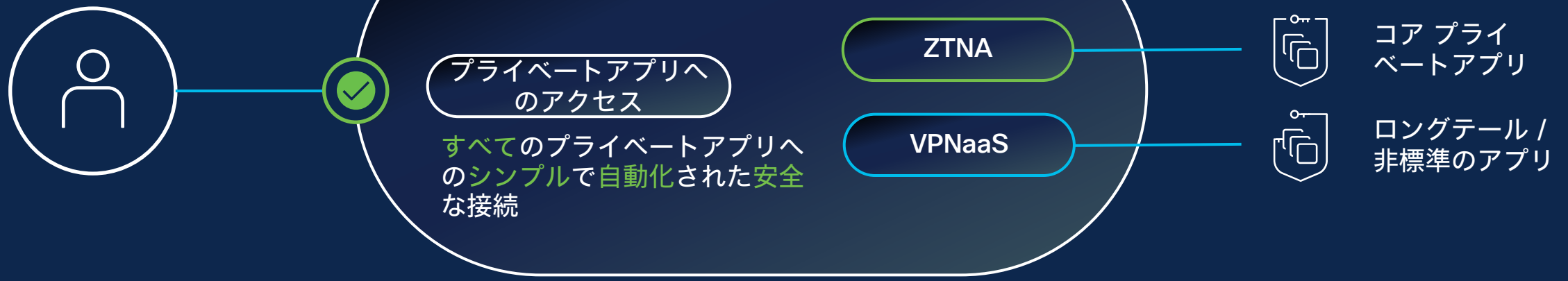
攻撃成功の減少

Zero Trust Network Access (ZTNA) への道のり

どこからでもアクセスできるインテリジェントなプライベート・アプリケーション

ユーザ
比類なきシンプルさ

ZTNA
比類ない移行柔軟性



メリット

- アプリ固有のアクセス
- 発見不可能な IP アドレス
- 最小特権ユーザーアクセス
- アタック サーフェスの低減
- ZTNA または VPNaaS の自動選択
- ポスチャ検証
- アクセス・セグメンテーション

ゼロ トラスト アクセスへの移行が容易

- ✓ お客様自ら ZTNA 採用のペースを決定可能
- ✓ 同じクライアント
- ✓ 共通のポリシー

従来の VPN
ネットワークレベルのアクセス - アプリレベルでは制御できない

サービスとしての VPN
VPN をクラウドに移行 - コントロールと管理がより簡単に

統合 ZTNA
アプリケーション・レベルでのきめ細かな制御 + VPNaaS とデジタル・エクスペリエンスのモニタリング

Talos のインテリジェンスでセキュアアクセスを強化

より多くを見、より多く自動化することで、より多くの脅威をブロックし、より迅速に対応することが可能

2.1M+ 毎日解析されるマルウェア サンプル

625B 毎日処理されるWeb リクエスト

200+ 毎年発見される新たな脆弱性

- 専任の研究者とデータサイエンティストからなる強固な専門家チームがバックアップ
- 機械学習と自動化のインテリジェンス

400 B
毎日観測されるセキュリティイベント

セキュリティ強化の成果

大きな価値を見出している導入初期のお客様

ビジネスインパクト

より多くの脅威を感染前にブロックすることで、ビジネスの中断を回避

30%

クラウドセキュリティ * の統合されたセットを使用することで、より高いセキュリティ効果が得られた

インシデントの調査、修復作業、過重な負担を強いられているセキュリティスタッフの人員削減を大幅に削減

48%

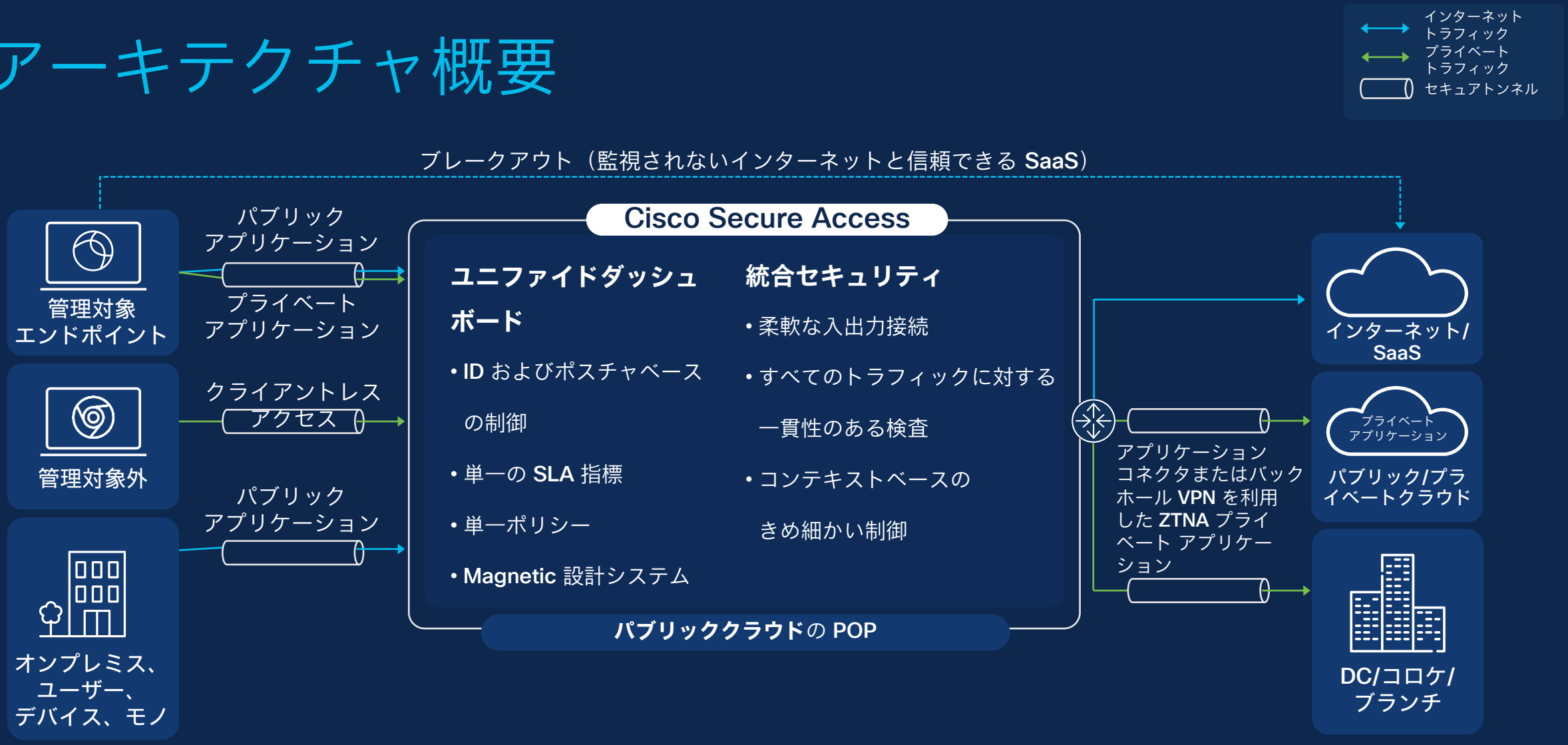
調査対象の組織のうち、マルウェア感染を 50 ~ 75 % 削減 **

* 出典 Forrester Total Economic Impact 調査、Umbrella SIG/SSE、2022 年

** 出典 Tech Validate 顧客調査、Umbrella、2022 年

Secure Access アーキテクチャ・機能

アーキテクチャ概要



Cisco Secure Access の機能

基本のセキュアサービスエッジ（SSE）の一歩先を行くサービスで快適な接続を実現しビジネスを強力に保護

基本となる SSE

- セキュア Web ゲートウェイ（SWG）
- クラウド アクセス セキュリティ ブローカ（CASB）と DLP
- ゼロトラスト ネットワーク アクセス（ZTNA）
- サービスとしてのファイアウォール（FWaaS）と IPS

＋

シスコは基本の機能も追加の機能も 1 つのサブスクリプションで提供

- DNS セキュリティ
- マルチモード DLP
- 高度なマルウェア防御
- サンドボックス
- Talos 脅威インテリジェンス
- サービスとしての VPN
- デジタル エクスペリエンス モニタリング（DEM）*
- リモートブラウザ分離

アドオンタイプのソリューション

- SD-WAN
- XDR
- Duo MFA/SSO
- CSPM

* 統合エクスペリエンスに付帯 / 個別のライセンス（オプション）

セキュリティ機能詳細

セキュア Web ゲートウェイ：フルプロキシ

Web トラフィックの詳細な検査と制御

- 完全な URL ロギングとクラウドアプリディスカバリーによる可視性の向上
- きめ細かなアプリ制御、コンテンツフィルタリング、URL ブロック / 許可リストによる利用ポリシーの実施
- SSL 復号とファイル検査によるマルウェアからの保護の拡張
- コンテンツ・セキュリティの向上： サンドボックス機能と、初期検出を回避したマルウェアの事後警告機能
- 完全な URL アドレス、ネットワーク ID、許可 /ブ ロックアクション、外部 IP アドレスによる詳細なレポート表示

VPN をクラウドに移行 (VPNaaS)

すべてのプライベートおよびパブリック
アプリへの効率的で安全なアクセス

- ✓ 煩雑な VPN をオフロード
- ✓ 優れたユーザー / リソース保護

- VPN をアウトソーシングのクラウドサービスとして提供
- ハードウェアのインストールとメンテナンスが不要
- すべてのアプリケーション/リソースへのユーザーアクセスによる生産性の向上
- 単一のコンソール、エージェント、ポリシーエンジンによる運用の簡素化
- アプリケーションのアクセス制御を強化
- ユーザー数の増加に合わせて高いパフォーマンスで簡単に拡張可能

Cisco Secure Access は VPNaaS と ZTNA を 1 つにまとめて提供

究極のセキュア プライベートアクセスを実現する ZTNA

すべてのプライベートアプリへの
効率的で安全なアクセス

- ✓ 画期的なセキュリティ
- ✓ 非常に使いやすい
- ✓ VPNaaS との相乗効果

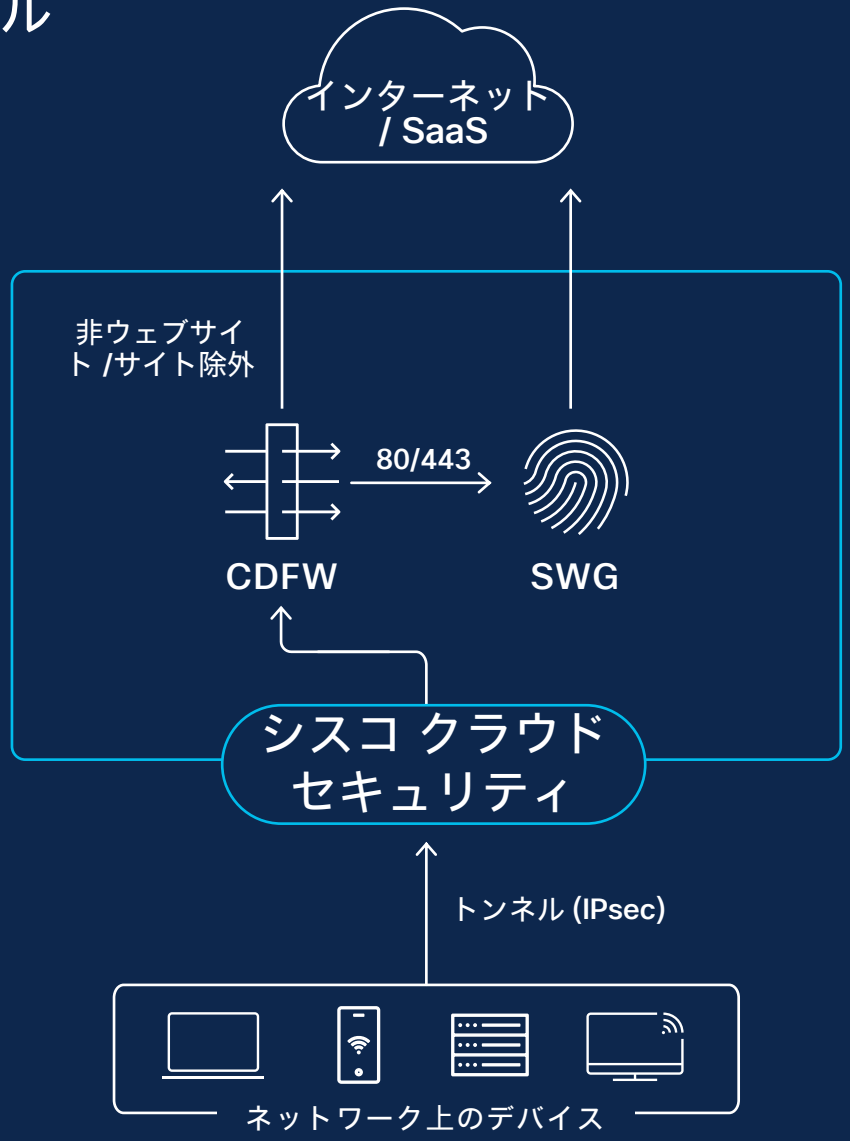
- ユーザーごと、アプリごとのきめ細かなアクセス・コントロール
- シームレスでシンプルなユーザー体験
- 継続的なデバイス・コンプライアンスとユーザー ID 検証
- リソースを難読化して発見を防止
- 統一されたダッシュボード、エージェント、ポリシーエンジン
- 最適化されたスループットによる優れたパフォーマンス

Cisco Secure Access は ZTNA と VPNaaS を 1 つとして提供

クラウド提供型ファイアウォール (CDFW)

クラウドエッジのアウトバウンド 通信むけ ファイアウォール

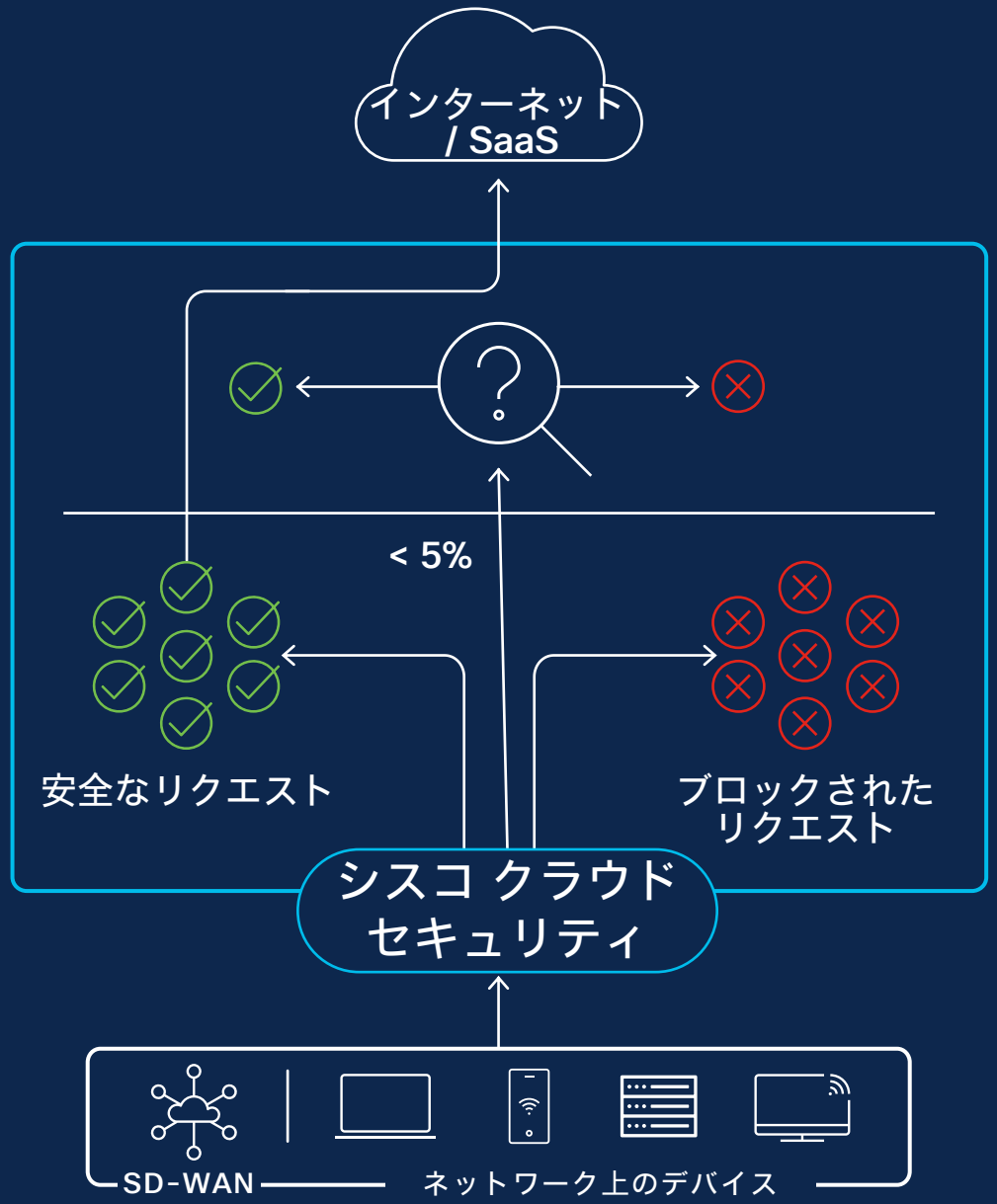
- 高リスクの非 Web アプリケーションをブロック
- IP、ポート、プロトコル、アプリケーションのルールを一元管理 （ レイヤー 3、 4、7 ）
- Snort 3 IPS でセキュリティを強化
- Webト ラフィック （ ポート 80/443 ） を安全な Webゲートウェイに転送
- IPsec トンネル終端



DNS レイヤ セキュリティ

差別化された第一線のディフェンス

- 数分で企業全体に展開 可能
- どこからでもマルウェア、フィッシング、C&C コールバックをブロック
- ゲスト Wi-Fi ネットワークからの悪質なウェブサイトへのアクセスを防止または制限
- 最も早い段階で脅威を阻止し、アラートのトリアージを削減
- インターネットアクセスを高速化し、危険なドメインのみをプロキシ化



クラウドアクセス セキュリティ ブローカー (CASB)

可視性、コントロール、保護

- SaaS アプリの利用をコントロール
  - コンテンツ、アプリ、テナントのコントロール
  - アップロード、投稿、共有などのきめ細かなコントロール
- リスクのあるアプリやアクティビティに関するアラートの自動化
- インラインおよび帯域外のデータ損失防止（DLP）により、アウトバウンドの Web トラフィックを安全に維持
- クラウドファイルストレージアプリからマルウェアを検出・除去

アプリケーションの可視性と制御

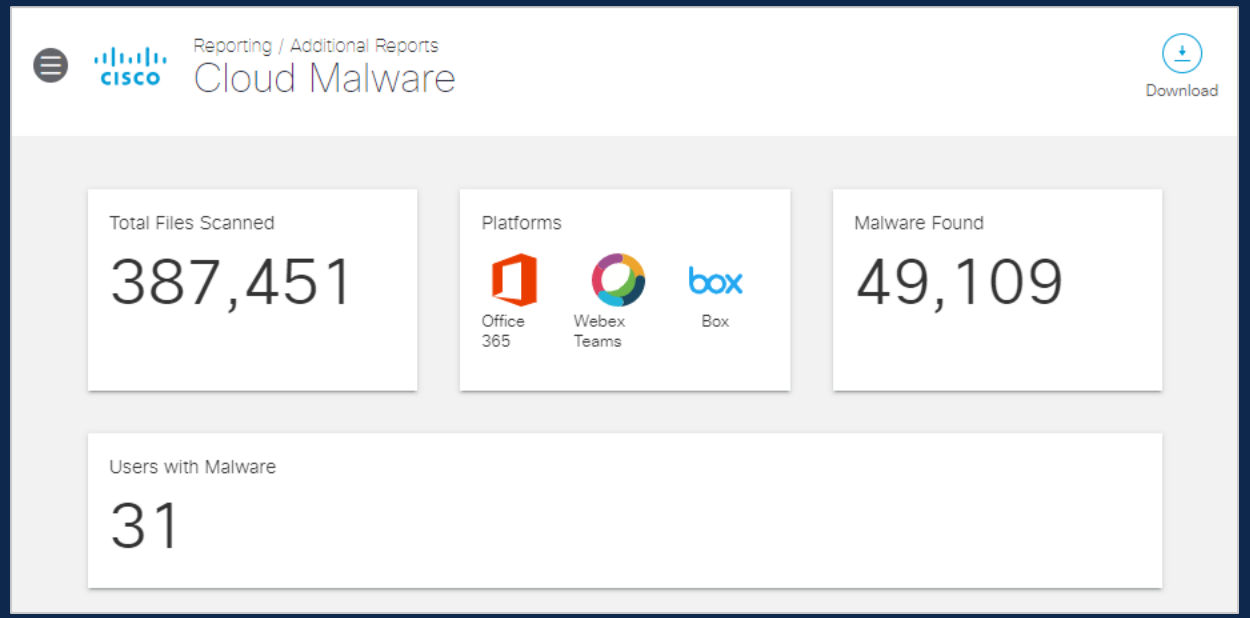
管理対象および非管理対象のクラウド・アクティビティ全体を把握

- 生産性、経費、セキュリティ、サポート問題への悪影響を最小限に抑える
- 環境全体で使用されているクラウドアプリの検出と監視
- アプリ名、ベンダー、カテゴリ、アクティビティ、リスクランキングなどを検出
- 必要不可欠なクラウドアプリへのアクセスを確保し、承認されていないアプリへのアクセスをブロック

クラウド上のマルウェア対策 (Cloud Malware Protection)

より優れたインテリジェンスがより優れたセキュリティを実現

- 包括的な Cisco Talos 脅威インテリジェンスの活用
- サポートされているクラウドアプリケーション内の悪意のある可能性のあるファイルをシステム管理者に警告します。
- 安全でないファイルがエンドポイントに到達する前に、管理者が隔離または削除できるようにします。
- 新しい脅威データを継続的に収集



第三者評価とパッケージング

2023 PeerSpot Tech Leader Award

毎年恒例の PeerSpot アワードとは

PeerSpot アワードは、毎年3つのカテゴリーでトップ企業 IT 製品をランキングするもので、検証されたレビュアーによるタイムリーなユーザーレビューに基づいています。PeerSpot のランキング方法によって決定された、対象カテゴリーの上位 3 つのソリューションに贈られます。

- ライジングスター賞は、過去 12 ヶ月間に PeerSpot レビューサイトのトラフィックボリュームが大幅に増加した上位 25 製品を、選択された Peer アワード カテゴリーで表彰するものです。
- User‘s Choice アワードは、選択したPeer アワード カテゴリーからユーザーがお気に入りの製品に投票する機会を提供します。

Company	Product	Category	Award
Cisco	Cisco AnyConnect Secure Mobility Client	Enterprise Infrastructure VPN	Tech Leader Awards
Cisco	Cisco SD-WAN	WAN Edge	Tech Leader Awards
Cisco	Cisco Secure Firewall	Firewalls	Tech Leader Awards
Cisco	Cisco Umbrella	Cloud Access Security Brokers (CASB)	Tech Leader Awards
Cisco	Cisco Umbrella	Internet Security	Tech Leader Awards
Cisco	Cisco Umbrella	Secure Access Service Edge (SASE)	Tech Leader Awards
Cisco	Cisco Umbrella	Secure Web Gateways (SWG)	Tech Leader Awards
Cisco	Duo Security	ZTNA as a Service	Tech Leader Awards

Cisco Secure Access は、Tech Leader Award 製品の技術を活用して開発された SSE

Source: PeerSpot (https://marketing.peerspot.com/)

第三者評価

- 主要統計
  - 企業が BYOD やリモートワークへの投資を続ける中、リスクは継続
  - 「 IDC の米国企業通信調査によると、企業の 40% が今後 2 年間にセキュリティ・サービス・エッジ（ SSE ）への支出を増大
  - IDC の「 2023 年仕事の未来調査」によると、ハイブリッド専用のセキュリティ・ポリシーと信頼のカルチャーを採用すれば、組織がセキュリティ侵害に遭う可能性は 3 倍低下
  - 「 IDC の 2022 年 12 月の Future Enterprise Resiliency and Spending Survey, Wave 11 によると、回答者の 41% が 2022 年の最優先投資として「リモートワーカーとオフィス内ワーカーの両方に対するネットワーク帯域幅とセキュリティの改善」を検討
- キーポイント
  - ゼロ・トラスト・ネットワーク・アクセス（ ZTNA ）や SSE などのセキュリティ近代化戦略にスマートに取り組むことで、企業はパフォーマンスとセキュリティのメリットを両立

IDC は、シスコが本稿で説明した課題に対処し、実行し続けることができる限りにおいて、シスコは市場を牽引する次世代のネットワークセキュリティ・リーダーの一角を占めることができると考える

IDC

SPOTLIGHT

Sponsored by: Cisco

User access decisions must be based on the most secure route for a seamless user experience across *all* private and public applications and resources.

Looking to Deliver on the Promise of Security Service Edge

September 2023

Written by: Frank Dickson, Group Vice President, Security and Trust, and Christopher Rodriguez, Research Director, Security and Trust

Introduction

The security needs of the modern digital business are vastly complex, spanning various devices, user groups, and locations. Users need secure access to enterprise applications and resources via a consistent, frictionless experience — whether they are onsite, in a branch office, at home, or on the road. Businesses that used remote and hybrid work models in some form reported higher productivity in 2022. Unsurprisingly, networking and security systems for these remote and in-office users remain a top priority as business leaders hope to foster greater communication and collaboration.

In recent years, applications and data have left the confines of the datacenter, users are working remotely more now than ever, and the proliferation of cyberthreats is driving a necessary change in networking and security architecture. Enterprise IT organizations use multiple clouds in hybrid models to balance the privacy, scalability, performance, and cost considerations that come with aggressive digital expansion. Web and software-as-a-service (SaaS) applications are also increasingly playing a role in enterprise IT architecture. Overall, the rapid adoption of SaaS applications, cloud computing, BYOD, and remote access use cases has increased complexity, expanded the attack surface for cybercriminals, and introduced a slew of specialized security concerns.

AT A GLANCE

KEY STATS

Risk is unlikely to abate as businesses continue to invest in BYOD and remote work. In detail:

- 40% of enterprises will increase spending on security service edge (SSE) in the next two years, according to IDC's U.S. *Enterprise Communications Survey*.
- Organizations are three times less likely to suffer a security breach if dedicated hybrid security policies and a culture of trust are adopted, according to IDC's 2023 *Future of Work Survey*.
- 41% of respondents cited "improved network bandwidth and security for both remote and in-office workers" as a top investment in 2022, according to IDC's December 2022 *Future Enterprise Resiliency and Spending Survey, Wave 11*.

KEY TAKEAWAY

By approaching security modernization strategies such as zero trust network access (ZTNA) and SSE in a smart manner, businesses can unlock performance and security benefits.

2023 年 10 月

パッケージ概要

リモート プライベート アクセスとダイレクト インターネット アクセスの個別のユーザ数

Cisco Secure Access Advantage

Essentials パッケージの
すべての機能プラス

レイヤ 7 ファイアウォール、IPS、DLP、RBI（レベル All）など*

Cisco Secure Access Essentials

Base パッケージ

安全なインターネットアクセス、安全なプライベートアクセス、SWG、ZTNA、レイヤ 3 および 4 のファイアウォール、CASB、RBI（レベル Risky）など

- ユーザー単位のライセンス
- サブスクリプションの期間
  - 1、3、5 年間のサブスクリプション
  - 契約別の非標準契約

* Private Access の DLP については以降のリリースにて対応予定

パッケージ詳細

ユースケースにあわせて、セキュア インターネット アクセス (SIA) とセキュア プライベート アクセス (SPA) も選択可能

カテゴリ	機能	Essentials	Advantage
セキュアなアクセス	セキュア インターネット アクセス (SIA) ローミングセキュリティ SD-WAN DIA RA-VPN	✓	✓
	セキュア プライベート アクセス (SPA) • クライアントベースの ZTNA • クライアントレス ZTNA • 安全なリモートアクセス（RA-VPN）	✓	✓
基本セキュリティ	Web アプリおよびプライベートアプリのレイヤ 3 およびレイヤ 4 を制御するクラウド提供型ファイアウォール	✓	✓
	セキュア Web ゲートウェイ（プロキシ Web トラフィック、URL フィルタリング、コンテンツフィルタリング、高度なアプリ制御）	✓	✓
	CASB - クラウドアプリの検出、リスクスコアリング、ブロック、クラウドマルウェアの検出、テナント制御	✓	✓
	リモートブラウザ分離（Risky）	✓+	✓+
	安全なマルウェア分析（サンドボックス）	制限付き	無制限
高度なセキュリティ	クラウド提供型のレイヤ 7 ファイアウォール		✓
	IPS 保護		✓
	Web アプリケーションのデータ損失防止（DLP）		✓+
	リモートブラウザ分離（ALL）		✓+
サポート	電子メールと電話による 24 時間年中無休のシスコサポートへのアクセス	✓	✓

導入パターン

1．SIA のみ

Secure Internet Access (SIA) × ユーザ数

2．SPA のみ

Secure Private Access (SPA) × ユーザ数

3．SIA + SPA

Secure Internet Access (SIA) × ユーザ数

Secure Private Access (SPA) × ユーザ数

注） Advantage と Essentials の混在は非サポート

ライセンスモデル

項目	Essentials	Advantage
ライセンス タイプ	サブスクリプション	サブスクリプション
ライセンス単位	ユーザ数	ユーザ数
最小ユニット	500	500
ライセンス期間	12 ～ 60 ヶ月	12 ～ 60 ヶ月
サポートモデル	Enhanced or Premium Support	Enhanced or Premium Support
エンドポイント クライアント (付属)	Secure Client	Secure Client

ユーザ数の区分
500 ～ 999
1000 ～ 4999
5,000 ～ 9,999
10,000 ～ 24,999
25,000 ～

型番： SECURE-ACCESS-SUB

注)
- ライセンス数、サブスクリプション アップグレードは、サブスクリプション期間中はいつでも可能
- Secure Client のユースケースによっては、別途ライセンスが必要となる場合があります

Secure Access の POP

当初

- 米国西部（オレゴン）
- 米国東部（バージニア北部）
- ヨーロッパ（フランクフルト）
- イギリス（ロンドン）
- アジア太平洋（シンガポール）
- アジア太平洋（東京）
- アジア太平洋（ムンバイ）
- オーストラリア（シドニー）

今後

- 米国西部（ノースカロライナ）
- 米国東部（オハイオ）
- ヨーロッパ（ミラノ）
- ヨーロッパ（スペイン）
- ヨーロッパ（パリ）
- ヨーロッパ（ストックホルム）
- ヨーロッパ（チューリヒ）
- アジア太平洋（大阪）
- アジア太平洋（ソウル）
- アジア太平洋（ジャカルタ）
- アジア太平洋（香港）
- アジア太平洋（中国）
- オーストラリア（メルボルン）

他

注） 今後の予定については変更されることがあります （ビジネスニーズその他影響を含みます）

Secure Access ロードマップ

短期

1. Cisco SD-WAN Integration
2. Digital Experience Monitoring
3. Reserved IP
4. ISE Integration for RA-VPN

中長期

1. Full AnyConnect (Secure Client) Migration
2. ISE Integration for Security Group Tagging (TrustSec integration with LAN/Cloud)
3. IPv6

他

サポート
Secure Access Software Support Service 概要

提供内容	Software Support Enhanced	Software Support Premium (オプション)
TACサポート（Solution Supportレベル）	✓	✓
ソフトウェアアップデートのダウンロード利用	✓	✓
ケースの優先対応		Enhanced より優先
ソフトウェア専門家への直接コンタクト	✓	✓
設定ガイダンスを含むオンボーディング時の技術支援	✓	✓
システムリスク評価やソフトウェア使用上のアドバイスなどの定期的な技術支援	✓	✓
サポートケースの分析		✓
専任サービス技術員: お客様の環境を理解した専任技術員による、インシデント、ケース、および変更の管理、相談、推奨事項の提供		✓

トライアルのお申し込みはアンケートにお寄せください


cisco SECURE