Pulse Secure®

Pulse Zero Trust Access

ハイブリッドIT環境向けのSaaS型
セキュアアクセスサービス

特長

ユーザー、デバイス、アプリケーション、ゲートウェイの**包括的な可視化、コンプライアンス、ポリシーの適用**

SDP（Software Defined Perimeter）アーキテクチャに基づくダーククラウドのサポートにより、**デバイスからアプリケーションへのセキュアなアクセスを実現**

データセンターおよびクラウド内の企業アプリケーションへの**シームレスなセキュアアクセス**

大規模展開を容易にする**ユーザー単位のサブスクリプション**のみのライセンスとライセンス管理

お客様にとっての価値

攻撃対象領域を削減する**エンドツーエンドのゼロトラストアクセス**

単一画面による可視性、ポリシー管理、分析

コンプライアンスと**ガバナンスの向上**

TCOの削減と生産性の向上

ソリューション

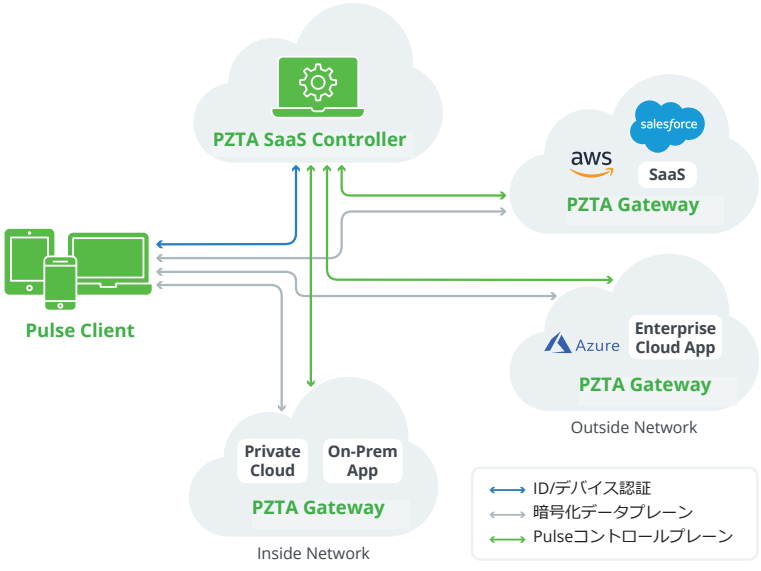
ゼロトラストネットワークアーキテクチャに基づくクラウドベースのPZTAサービスは、SD-Access（ソフトウェア定義アクセス）、継続的な認証、ダーククラウドのサポートを可能にします。このソリューションは、Pulse Secureが運用するZTAコントローラー、お客様がクラウドまたはオンプレミスで展開できるZTAゲートウェイ、ユーザーのデバイスにインストールされるZTAクライアントで構成されます。

- サービスとしてのゼロトラストアクセス
- エンドツーエンドの可視化とポリシー適用
- 統合クライアント：Windows、macOS、iOS、Android
- 幅広いエコシステムとの統合
- 包括的な分析とレポート
- 迅速な展開、柔軟なライセンス

ハイパーコネクテッド社会のためのゼロトラストアクセス

デジタルトランスフォーメーションを契機として、ユーザー、デバイス、アプリケーション、インフラストラクチャの間にもハイパーコネクテッドの時代がやってきています。企業は、セキュアアクセスを可能にしユーザーとアプリケーションを保護し、分散型ネットワークのサイバーセキュリティリスクを管理する必要があります。従来の社内は安全、社外は危険といった境界モデルは限界を迎えており、ゼロトラストの重要性が増しています。企業はギャップを埋めるために複数のポイント製品を次から次へと追加するのではなく、これらの新しい課題に対処するエンドツーエンドなセキュアアクセスソリューションを求めています。場当たり的な方法は管理負荷が高くコストがかかり、セキュリティ上の問題も発生し非効率的である上に、リスクが大幅に増大します。

Pulse Zero Trust Access（PZTA）は、ハイブリッドIT環境全体にわたるアプリケーションとリソースへの信頼できる直接アクセスを提供することにより、ハイパーコネクテッド時代のセキュアアクセスの課題を解決します。PZTAは、包括的な可視性、エンドツーエンドの分析、エンドポイントのコンプライアンス、適応力の高いポリシー適用を提供します。PZTAは、継続的なエンティティ認証と堅牢なエコシステム統合により、オンプレミスでもクラウドでもお客様のニーズを満たす、簡単で保護された接続、効率的な管理、柔軟な展開を実現するアクセスサービスを提供します。



ユースケースの概要

Pulse SecureのPulse Zero Trust Access（PZTA）プラットフォームは、あらゆるユーザーがあらゆる場所からパブリッククラウドやプライベートクラウドおよびマルチクラウドのアプリケーションに、さらにはデータセンター内のリソースへのセキュアなアクセスを可能にします。企業では従業員のモバイル化とハイブリッドIT化が進んでいますが、PZTAは拡張可能なゼロトラストプラットフォームの一部として、セキュリティと生産性を強化し、可視性を高め、管理とユーザーエクスペリエンスを大幅に強化します。

オンプレミス、SaaS、ハイブリッドクラウドアプリケーションへのゼロトラストアクセス

Pulse Zero Trust Accessは、データセンター、プライベートクラウド、パブリッククラウド内のアプリケーションへのセキュアなゼロトラストアクセスを可能にします。ZTAクライアントは、ユーザーとデバイスを継続的に認証し、ユーザーデバイス上のZTAクライアントとアプリケーションに最も近いZTAゲートウェイ間の暗号化されたデータチャネルを通じて、企業アプリケーションへの常時保護されたアクセスを提供します。アプリケーションはユーザーから見えない（ダーククラウド）ため、セキュリティリスクが緩和されます。

課題	PULSE ZERO TRUST ACCESS サービス
クラウド内のリソースを管理するのが難しい	PZTAを使用した場合、クラウド内のリソースの管理とアクセスは、オンプレミスのリソース管理とアクセスとまったく同じであり、可視性、コンプライアンス、ポリシー適用、分析のレベルも同じです。ユーザーがアプリケーションサーバーに直接アクセスすることはありません。アプリケーションがオンプレミスからクラウドに移動した場合、ユーザーが次にこのアプリケーションにアクセスしようとすると、ZTAコントローラーがユーザーのZTAクライアントをこのアプリケーションに最も近いZTAゲートウェイに誘導します。
ユーザーとアプリケーションのトラフィックを企業のネットワーク内にとどめる	PZTAは、SDPアーキテクチャに基づいてコントロールプレーンとデータプレーンを分離しています。ユーザーとアプリケーションのすべてのトラフィックは、お客様独自のVPCまたはデータセンターに展開されているZTAゲートウェイのみを流れ、データトラフィックがZTAコントローラーに流れることはありません。このため、データプライバシーは完全に守られます。
生産性を向上させる	管理者は、ZTAコントローラーによりアプリケーションやデバイスの種類、ユーザーの場所を問わず、ユーザー、デバイス、ゲートウェイ、アプリケーションを結び付けるエンドツーエンドのゼロトラストアクセスポリシーを一元的に構成することができます。エンドユーザーにとっては、アクセスしようとしているアプリケーションの種類やどこからアクセスしようとしているかに関係なく、アクセスのメカニズムは同じです。これにより、ユーザーと管理者のエクスペリエンスが簡素化され、統一されたものになり生産性が向上します。
買収した企業を統合するときにアクセスのセキュリティを確保する	PZTAを使用すると、ネットワークアクセスを許可するのではなく、一元管理されたセキュアアクセスポリシーにユーザーグループを追加することで、ユーザーグループ間で共有されるべきリソースを指定できます。さらにハイレベルの分離が必要な場合、管理者は別個のゲートウェイを構成するか、マルチテナント構成のもう1つのテナントとして別のBU（ビジネスユニット）をセットアップするかを選択できます。

可視化、ポリシーの適用、コンプライアンスレポート

Pulse Zero Trust Accessを使用すれば、ユーザーの場所やアプリケーション、リソースの場所を問わず、任意のデバイスから接続しているすべてのユーザーを単一画面で確認できます。IT部門およびセキュリティ部門の管理者は、PZTAポータルに用意されている各種のインタラクティブなダッシュボードでリアルタイムにステータスと履歴を確認し、事前に定義されたカスタムレポートを利用することができます。

課題	PULSE ZERO TRUST ACCESS サービス
可視性のギャップ	PZTAは、ユーザー、デバイス、インフラストラクチャ、およびアプリケーションの包括的な可視性を提供します。すべてのアクセスはZTAコントローラーによって認証および承認されます。また、すべてのアクセスアクティビティはPulse ZTAダッシュボードにキャプチャされ、レポートと監査のためにログとして記録されます。
BYODを許可する必要があるがセキュリティ上のリスクもある	PZTAを使用すると、BYODデバイスでも企業所有のデバイスと同じレベルのゼロトラストアクセスを実現できます。個人所有のデバイスから企業アプリケーションにアクセスしようとすると、その都度、デバイスのコンプライアンスステータスとその他のセキュリティポスチャをチェック（場所、時間、ユーザーの振る舞いなど）してからアクセスが許可されます。

ユーザーとエンドポイントのアクセスコンプライアンスの確保	PZTAは、接続前と接続中にきめ細かいアクセスポリシーに従って、ユーザー、デバイス、セキュリティポスチャを動的に認証します。PZTAはユーザーに違反を通知するか、拒否されたユーザーに対して事前定義されたエンドポイント修復を実行したり、アプリケーションやリソースへの制限付きアクセスのみを許可したりすることができます。

異常の自動検出と緩和

何がセキュアで正常であるかは組織によって異なります。Pulse Zero Trust Accessは、ユーザーがどこからログインするか、通常使用するデバイスは何か、通常アクセスするアプリケーションは何かを観測することにより、継続的な学習と適応を行います。通常のユーザー行動と異なる振る舞いがあった場合には管理者に警告が通知され、管理者は事前設定された対応または提案された緩和アクションをその場で選択できます。

課題	PULSE ZERO TRUST ACCESSサービス
貴重なデータを窃取する目的で悪意のある内部関係者が資格情報を盗み出すことを検出して防止する	従来の境界防御では、悪意のある内部関係者による資格情報の窃取の検出・特定が困難です。疑わしい従業員が別のデバイスを使用したり、別の場所からログインしたりしている場合、PZTAはセキュリティ管理者に警告を通知することができます。その後、管理者はMFAの要求などの事前設定された強制アクションを実行するか、状況が解決するまで手作業で一時的にアクセスを停止することができます。
従業員が危険度の高い場所に移動したときのアクセスを管理者が制限できるようにしたい	PZTAを使えば簡単に実装できます。ユーザーの所在が変わるとアクセス可能なアプリケーションのリストが動的に更新されます。従業員が危険度の高い場所に移動したとき、または従業員がすべてのコンプライアンス要件を満たしていないデバイスを使用しているときに、機密性の高いアプリケーションへのアクセスを一時的にリストから削除することができます。

ユーザー行動分析

アプリケーションにアクセスしようとするすべてのユーザーは、認証と認可のためにZTAコントローラーに送信されます。このプロセスでは、ユーザーエクスペリエンスを強化し、可視性を向上させ、潜在的なセキュリティリスクを最小限に抑える予防的なアクションを実行するために、PZTAが学習した使用状況と振る舞いに関する広範な情報を適用します。

課題	PULSE ZERO TRUST ACCESSサービス
従業員のリスクスコアを測定したい	PZTAは、ユーザーの現在および過去の行動と使用状況に基づいて、すべてのユーザーに「リスクスコア」を割り当てます。このスコアは動的に評価され、ユーザーのアクションと潜在的なリスク要因の両方を反映します。管理者はスコアに基づいてユーザーごとに異なるアプローチを取ることができます。
CIOがアプリケーションやデータの使用率を確認できるようにしたい	PZTAは包括的な使用傾向と詳細な使用状況のレポートを提供するため、利用頻度の最も高いアプリケーションをCIOおよびCレベルの経営幹部が把握することができます。このソリューションは、ユーザーグループ、場所、リソース、ゲートウェイ、または個々のユーザーにまでズームインするZTA分析GUIを使用して、さまざまなリアルタイムクエリをサポートします。これらの情報は、リソースと予算の計画策定にも活用できます。
ネットワークアセットをどこに展開すべきかを管理者がわかるようにしたい	管理者は、PZTAの使用状況レポートから、ユーザーの移動先の物理的な場所とユーザーがアクセスしているZTAゲートウェイに関して、ユーザーグループや個々のユーザーレベルまでの詳細情報を把握できます。管理者はこれらの情報を使用して、ユーザーエクスペリエンスの最大化と運用オーバーヘッドの削減に最適な帯域幅を選択することができます。
従業員の生産性を向上したい	ITチームは、ユーザーがリソースやアプリケーションにアクセスする方法、場所、タイミングについて全方向の視野を得ることで中断を最小限に抑える保守スケジュールの設定およびデバイスやアプリケーションのアップグレードの優先順位といったベストプラクティスを定義することができます。これにより、ユーザーエクスペリエンスと生産性がさらに向上します。

サービスとしてのゼロトラスト

Pulse ZTAはPulse Secureが提供するサービスです。ZTAコントローラーはPulse Secureによってグローバルにホストおよび管理されています。

オンプレミスとクラウドで利用可能

ZTAゲートウェイは、パブリッククラウドまたはプライベート環境でお客様のVPCに展開できます。

SDPとダーククラウド

ユーザーとデバイスの認証および認可後のみ最小限のアプリケーションにアクセスできる（その他のアプリは見えない）SDPアーキテクチャに準拠しています。

広範な統合

豊富なAPIセットによりエコシステムパートナーのソリューションとの統合が容易です。

マイクロサービスアーキテクチャ

独立した小規模プロセスで構成されるコンテナ化されたマイクロサービスアーキテクチャにより、最大限の拡張性とパフォーマンスを実現します。

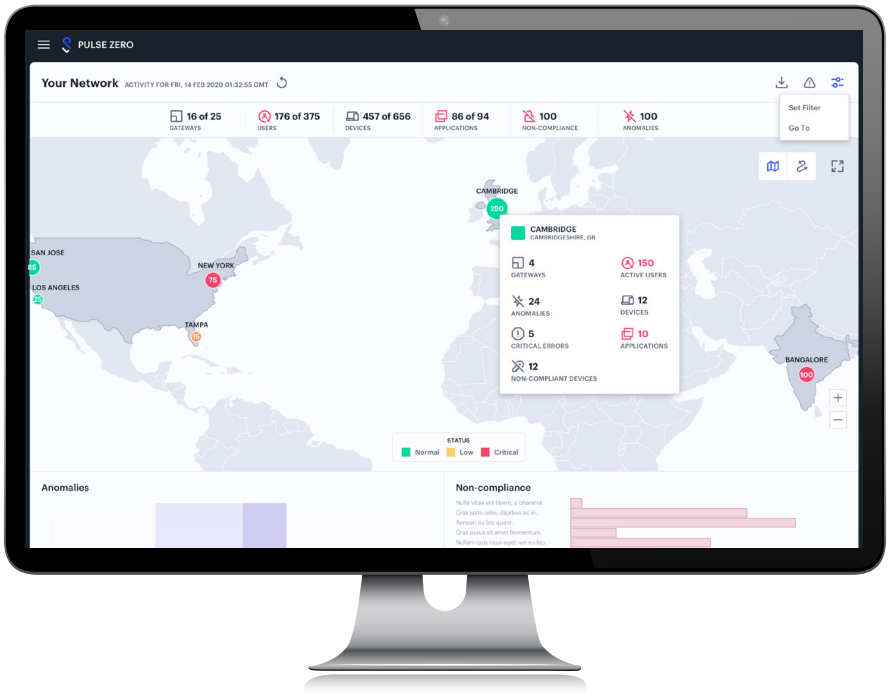
特長	利点
エンドツーエンドのアクセスポリシー	管理者は、すべてのリソースまたはリソースグループについて、エンドツーエンドのアクセスポリシーセットを定義できます。これにより、社外と社内のユーザー、BYODや会社支給のデバイスを使用しているユーザーの区別がなくなり、アプリケーションまたはリソースがデータセンターとクラウドのどちらに存在しているかも区別されません。
ダーククラウド	ZTAクライアントは、アプリケーションとリソースがどこにあるかを知る必要がなく、常にZTAコントローラーを介してアクセスを要求します。アクセスが許可されると、ヘッドレスゲートウェイがクライアントへの暗号化されたデータトンネルを確立して、アプリケーションにアクセスします。このダーククラウド機能により攻撃対象領域が大幅に減少します。
単一画面の可視性とコンプライアンス	管理者向けに、すべてのユーザーグループ、場所、デバイスの種類、オンプレミスおよびクラウドリソース全体にわたり、ユーザー、デバイス、アプリケーション、インフラストラクチャの全体的な可視性とコンプライアンスレポートを単一画面で提供します。
コントロールプレーンとデータプレーンの分離	コントロールプレーンは、ZTAクライアントとZTAコントローラー間の認証および認可のみを担当します。ユーザーとアプリケーションのトラフィックは、コントローラーによって許可された後、ユーザーと指定のゲートウェイ間で直接送信されます。この分離により、ユーザーデータが失われるリスクが緩和され、データプライバシーが守られるうえ、ユーザーエクスペリエンスが最適化されます。
状況に応じたSSO	PZTAは、SAML 2.0により、一般的なIDソリューションおよびサービスと統合し、サポート対象のSaaSおよびサードパーティアプリケーションへのSSOを提供します。管理者は、場所、時刻、ユーザー行動といった追加のセキュリティポスチャに基づいて適応型SSOを有効にすることもできます。
エンドポイントのコンプライアンス	PZTAは、アクセスを許可する前に、きめ細かいアクセスポリシーに照らしてユーザーとユーザーデバイスのセキュリティポスチャを承認することにより、アクセスコンプライアンスを保証し、マルウェアなどのエンドポイントの脅威を緩和します。エンドポイントセキュリティに対する十分なコンプライアンスチェックは、マルウェアやその他の脅威がデバイス経由でもたらされる可能性を減らします。
ユーザー行動分析	ユーザーの行動と使用状況は動的であり常に変化しています。PZTAは分析データを活用して、セキュリティリスクの緩和、異常の検出、ユーザーエクスペリエンスの最適化を行い、モバイル化の進む従業員のニーズに適応します。
データプライバシーとデータ主権	すべてのユーザーデータとアプリケーションデータは、クライアントとゲートウェイ間で完全に暗号化されます。Pulse Secureがホストするデータプレーンにアプリケーションデータが共有されることはありません。
オンプレミスおよびハイブリッドクラウドゲートウェイ	ゲートウェイは、パブリッククラウド、プライベートクラウド、またはお客様のデータセンターに展開できます。この柔軟性により、データを信頼できるドメイン内に保持できるうえ、パフォーマンスも向上します。これにより、最適なトラフィックと帯域幅を利用することができます。

Pulse Zero Trust Accessの仕組み

PZTAは、ゼロトラスト方式でセキュアアクセスを実現するSDPアーキテクチャに基づいています。Pulse Secureによってホストおよび管理されるZTAコントローラー、VPC（AWS/Azureパブリッククラウド、ホストされたプライベートクラウド、またはオンプレミス）に展開できるZTAゲートウェイ、Pulse VPN/NACクライアントと同じ統合クライアントであるZTAクライアントで構成されています。

ユーザーが自分のデバイスから保護されたアプリケーションまたはリソースにアクセスするたびに、ZTAクライアントはZTAコントローラーとのセッションを開始してアクセスを要求します。ZTAコントローラーは、ユーザーの資格情報、デバイスのコンプライアンスおよびその他のセキュリティポスチャ（場所や振る舞いなど）を検証し、要求されたアプリケーションまたはリソースに最も近いZTAゲートウェイを承認し、ZTAクライアントとの暗号化されたデータ通信を許可します。通信全体を通じてエンドポイントのセキュリティポスチャが継続的に評価されセッションのセキュリティが確保されます。

ゼロトラストのアクセスフローは、ユーザーが企業ネットワークの内部と外部のどちらにいるか、企業所有デバイスと個人所有デバイス（BYOD）のどちらを使用しているか、SaaSアプリケーションにアクセスしているかオンプレミスのリソースにアクセスしているかを問わず同じです。



ユーザー、場所、異常などを一目で確認できるPZTA管理者ポータル

Pulse Zero Trust Accessの主なメリット

シンプルなユーザエクスペリエンス

ZTAクライアントは、2千万件以上のお客様が利用されている、実績のあるPulse VPN/NAC統合クライアントと同じです。Windows、macOS、iOS、Androidなどの一般的なオペレーティングシステムをサポートし、多要素認証（MFA）、シングルサインオン（SSO）、VPNサービスの利用が可能で、PZTAの実装やVPNからPZTAへの移行も簡単です。

エンドツーエンドのセキュアアクセスポリシー

PZTAでは、管理者はアプリケーションおよびリソースにアクセスできるユーザーやユーザーグループを定義するエンドツーエンドのセキュアアクセスポリシーを公開するだけです。ユーザーがリモートであるかオンプレミスであるか、個人所有デバイスと会社支給のデバイスのどちらを使用しているか、アクセスしているアプリケーションがデータセンターにあるかクラウド内にあるかを問わず、ユーザーがエンドポイントからリソースへのアクセスを選択するたびに、ユーザーの資格情報とデバイスのコンプライアンスだけでなく、場所やユーザー行動などのセキュリティポスチャに基づいて認証および認可が行われます。これがゼロトラストアクセスの仕組みです。

攻撃対象領域の削減

PZTAサービスは、SDP（ソフトウェア定義境界）アーキテクチャを活用して攻撃対象領域を大幅に削減します。エンドユーザーデバイスがアプリケーションまたはリソースに直接接続することはなく、ZTAコントローラーとのセキュアな接続を介してのみすべてのアクセス要求を開始できます。ZTAコントローラーは、ゲートウェイと保護されたアプリケーション間のリストとマッピングを維持します。認証と認可が正常に行われた場合にのみ、ZTAクライアントは対応するZTAゲートウェイとの暗号化されたデータトンネルを確立します。アクセスが完了するとデータトンネルは終了します。エンドユーザーが接続を再確立する場合は、ZTAコントローラーによる認証および認可が再び必要になります。これにより、ZTAゲートウェイとアプリケーションを信頼されていないホストとデバイスから保護することで、攻撃対象領域と潜在的な脆弱性を劇的に削減します。

包括的な可視化とコンプライアンス

Pulse ZTAでは、CIO、CSOおよびIT管理者がコンプライアンスの対応状況を可視化して1つの画面で確認することができます。管理者は、ユーザー、デバイス、ゲートウェイ、アプリケーションとそのステータス、および統計データの全体像をPZTAダッシュボードから確認することができます。任意の領域にワンクリックでズームインし、アラートやどのようなコンプライアンス違反があるのかを確認できます。管理者やCIO/CSOは、カスタマイズされたフィルターとフォーマットを使用して作成された事前定義のレポートをPZTAダッシュボードで閲覧することから1日の作業を始めることができます。

ユーザーの振る舞い分析

すべてのアクセスがZTAコントローラーを経由するため、ユーザーの行動情報をすべて収集して機械学習の対象にすることができます。詳細な行動分析には、通常のルーチンとは異なる振る舞いがあった場合、場所、デバイス、アクティビティに基づいて疑わしい状況を自動検出するなど、多くの実用的なアプリケーションがあります。PZTAは、ユーザーの使用パターンと履歴に基づいてすべてのユーザーに固有の「リスクスコア」を割り当てます。管理者は、リスクスコアに基づいて特定のアプリケーションへのアクセスを止めたり、場所、デバイスの種類、セキュリティポスチャに基づいてアクセスを制限したりできます。

ユーザー
- 従業員
- 請負業者
- ゲスト

デバイス
- モバイル
- PC/Mac
- 会社支給
- 個人所有

アプリケーション
- SaaS &クラウドネイティブ
- オンプレミス
- サードパーティ
- カスタム

インフラストラクチャ
- オンプレミス
- クラウド

Pulse Secure®

パルスセキュアジャパン株式会社
〒107-6012 東京都港区赤坂1-12-32
アーク森ビル
(03) 4360-8288
info_jp@pulsesecure.net
https://jp.pulsesecure.net/

PULSE SECUREについて

Pulse Secureは、ユーザー、デバイス、IoT、サービスの可視化と保護、生産性向上を可能にするセキュア アクセス・ソリューションを提供するベンダーです。当社は、クラウドやモバイル・アプリケーションとネットワークアクセス制御を統合したスイート製品やSaaSによるサービスによりハイブリッドなIT環境で ゼロトラストの実現を支援します。あらゆる業界の24,000社以上の企業とサービスプロバイダーがPulse Secureを活用しており、モバイルワーカーにビジネスのコンプライアンスを確保しながらデータセンターやクラウドのアプリケーションや情報への安全なアクセスを提供しています。

linkedin.com/company/pulse-secure
www.facebook.com/pulsesecure1
twitter.com/PulseSecure
info@pulsesecure.net

VERSION 07272020