

Absolute Secure Access

ハイブリッドワーク時代の
高信頼、レジリエントなアクセス



リモートワーク環境で安全で生産性の高い環境を実現するためにはサイバーレジリエンスの概念を、エンドポイントの枠を超えて、ネットワーク接続や重要なアプリケーションにまで広げることが重要です。その中では、モバイルファーストの企業向けVPN（仮想プライベートネットワーク）とZTNA（ゼロトラスト・ネットワークアクセス）は、SASE（セキュアアクセス・サービスエッジ）パラダイムを確立するための重要な基盤です。ネットワークは、常に移動し、パブリッククラウド、オンプレミス、データセンター内の組織資産にアクセスするエンドポイントデバイスと、必ずしも組織が所有していないWi-Fiや携帯電話ネットワークのホストを使用して信頼関係を構築する必要があります。

今日のワーカーは、セキュリティと信頼性に加え、ビジネスアプリケーションへのシームレスなアクセスを必要としています。ネットワーク間を定期的にローミングしたり、地方や遠隔地に移動したり、トラフィックの多い地域で作業したりする場合には、困難な場合があります。接続が滞ったり、完全に切れたりすることで、パフォーマンスの問題、ユーザーエクスペリエンスの低下、ダウンタイムなどが発生することがあります。また、問題の根本的な原因を可視化できないため、ITチームに非効率的な作業を強いることとなります。

リモートワークする従業員、常に移動している救急隊員、現場でプロジェクトを遂行する公共事業従事者などは、シームレスで弾力性のある接続性を提供することで、モバイル関連のIT問題を大幅に軽減できます。また、技術的な問題のトラブルシューティングではなく、仕事に集中することができるようになります。

レジリエンスパワーの成果

現代のデジタルビジネスの中では、安全で信頼性の高いアクセスを実現することがミッションクリティカルです。そこで、Absolute®の出番となります。Absolute Secure Access™ 製品ポートフォリオは、パブリック・クラウド、プライベート・データセンター、またはオンプレミスの重要なリソースに安全にアクセスするための、信頼性と回復力に優れたネットワーク接続をユーザーに提供します。Absolute Secure Accessにより、生産性や管理制御に影響を与えることなく、モバイルファーストのエンタープライズVPNを内蔵したような従来の安全なリモートアクセス技術からゼロトラストアプローチに移行することができます。

しかし、それだけではありません。Absolute Secure Accessは、改ざんされたり、誤って削除されたり、あるいは動作しなくなったりした場合に、自動的に自己修復または再インストールすることができる唯一の削除不能なセキュアアクセス・テクノロジーです。Absolute Secure Accessにより、健全な状態を維持し、本来の価値を十分に発揮することができます。Absolute Network Resilience™ テクノロジーは、不健全なネットワーク接続を監視して自動的に修復し、最適化します。これにより、アプリケーションの再起動やネットワークの再接続、再認証が必要になるような、エンドユーザーに影響を与えるような中断が発生することなく、ネットワーク上のアプリケーションの運用が継続されます。その結果、優れた接続性と信頼性を実現し、エンドユーザーはネットワークの動作ではなく、自分のタスクに集中できるようになります。

IT、セキュリティ、ビジネスを強化

Absolute Secure Accessの製品群は、その汎用性の高さから、組織内のさまざまなステークホルダーのさまざまなユースケースに活用することができます。

Absolute Secure Access の特長

Absolute Insights for Network

プロアクティブな
診断

レジリエントな Windows エージェント

自己復活

エンドポイントでの ダイナミックな ポリシー施行

デバイスデータを
保護

ネットワークの レジリエンス

生産性と
パフォーマンスを
向上

VPN、ZTNA、DEM をひとつのプラット フォームで実現

ベンダー統合

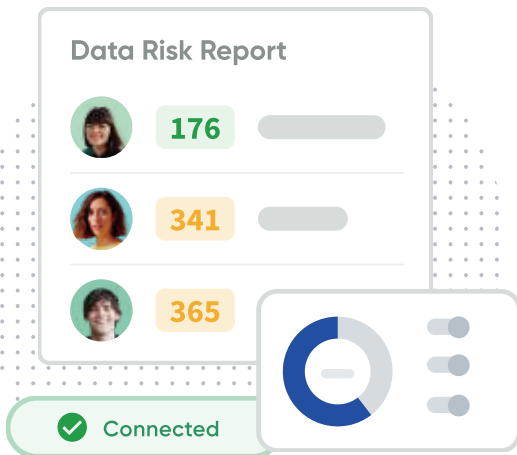
レジリエントな インフラ ストラクチャ

高可用性

Absolute Secure Access Key ユースケース

ゴール
オペレーションの
効率と生産性を
向上

- ✔ **ネットワークパフォーマンスを最適化** 従業員エクスペリエンスを積極的に改善し、トンネルとセッションの回復力を利用して常時接続を実現し、デバイスとネットワークの診断を行い、組織境界の外でネットワークパフォーマンス分析を実行することができます。
- ✔ **どこでも仕事できるワークフォースを強化** シームレスなリモートアクセス、エンドユーザーのオーディオとビデオの最適化、エンドユーザーの信頼性の高いネットワークアプリケーションへのアクセス、最も不安定なネットワーク条件でも回復力のある接続とアプリケーションを提供することができます。
- ✔ **ネットワーク利用状況を把握** ネットワーク接続状況の把握、アプリケーションメトリクスとジオロケーションへのアクセス、設定状況の評価、ネットワーク接続の健全性全体への影響、さらに利用パターンの分析と ROI の証明を実現します。
- ✔ **コスト管理** データ使用量の把握、データバックホールの削減、コストのかかるインフラのオーバーホールなしに VPN から ZTNA への移行、ネットワークパフォーマンスの分析により、より多くの情報に基づいた購入の意思決定を行うことができます。
- ✔ **ヘルプデスクの効率化** 接続問題の根本原因分析の実施、問題の迅速な特定によるダウンタイムの最小化、帯域幅および接続診断の自動発動、ZTNA ポリシーの実施効果の可視化を実現します。



ゴール
リスクを軽減し
コンプライアンス態勢
を強化

- ✔ **リソースの保護** SaaS、オンプレミス、プライベートクラウドのリソースを侵入者や攻撃から保護し、リソースのホスティング先に関係なく平等に扱い、アプリケーション間の横移動をブロックし、継続的なリスク評価を実施します。
- ✔ **ユーザーの保護** オンラインの脅威や不適切なコンテンツへのユーザーのアクセスを制限し、ファイアウォールの内側と外側で完全に制御できるようにし、自動的にフィッシングやスミッシング攻撃をブロックし、エンドポイントでのきめ細かいポリシー実施により摩擦のないセキュリティを提供します。

ゴール
ビジネスを強化

- ✔ **継続的なサービス提供を保証** 現場作業員の信頼できる接続性を確保し、地理的な位置情報に基づいて適切なサービス料金が適用されるようにし、障害や停電を迅速に特定して解決し、サービス SLA を実施する。



お客様のビジネスニーズに対応するふたつのフレーバー

Absolute Secure Access では、Absolute Core™ Plus と、Absolute Edge™ のふたつのフレーバーを提供しています。

上位製品

Absolute Core Plus

Absolute VPN + ポリシーエンジン

モビリティとモダンエッジのためにゼロから開発

含まれている機能

- ✔ 従業員体験の積極的な改善
- ✔ トンネルとセッションレジリエンスを利用した常時接続性
- ✔ ビデオとオーディオの最適化
- ✔ モバイルファーストのエンタープライズ VPN でのセキュアなアプリケーションアクセス
- ✔ ポリシーエンジン

Absolute Edge

すべてのコア機能 + 以下の機能

Absolute ZTNA

SDP に最適なユーザーエクスペリエンス

- ✔ 組織境界の外側で完全な可視性を実現
- ✔ 複数のデータポイントを利用した継続的なリスクアセスメントにより、アクセスポリシーを強化
- ✔ どこでホストされているかに関係なく組織リソースへのアクセスを制限

Absolute Insights for Network

デジタルエクスペリエンス監視のための最適な診断と改善策

- ✔ 特許取得済み、デバイスとネットワークをプロアクティブに診断
- ✔ 携帯電話から公衆無線 LAN まで、組織境界の外側にあるネットワークのパフォーマンスを分析
- ✔ リアルタイムのジオロケーションダッシュボード
- ✔ リモートワーカーが訪問するドメインの脅威分類を実施



Technical Specifications

暗号化と証明書

- ✓ FIPS 140-2 認証の暗号化技術
- ✓ NSA Suite B 暗号
- ✓ Common Criteria EAL 4+ および SOC2 認証済

IPv6 サポート

- ✓ IPv6 アプリケーション、サーバー、インフラをフルサポート、シングルスタック、デュアルスタックに対応

Active Directory Group サポート

- ✓ Active Directory のグループやグループメンバーシップの変更に基づき、構成設定やポリシーを更新

Absolute Console Access

- ✓ ロールベースのアクセス管理
- ✓ ロールベースのテンプレート提供 (クライアントアドミン、ヘルプデスクユーザーなど)
- ✓ コンソールユーザーによるすべての変更を監査可能なロギング

認証とログイン

- ✓ 認証メソッドはユーザー、デバイス、グループで設定可能
- ✓ 管理者は、セキュリティ要件、ワークフロー、フォームファクターに最も適した方法を使用することができ、指定された認証方法をユーザーに透過的に提示することが可能
- ✓ サポートされている認証メソッド：
 - NTLM
 - RADIUS (PEAP, EAP-GTC, EAP-NTLM)
 - Active Directory
 - PKI x.509 v3 certificates
 - RSA
 - その他、業界標準の 2 要素認証ソリューション
既存の ID プロバイダーソリューション (Microsoft Azure AD、Active Directory Federation Services、Okta、Cisco Duo など) との統合を可能にする、SAML によるフェデレート認証

データの収集とプライバシーを管理

- ✓ セキュリティイベント、ビジネスニーズ、またはプライバシー基準に基づく

サードパーティとの連携

- ✓ リアルタイムで Absolute コンソールの主要メトリクスを確認できる API アクセス

エンドポイントでのポリシー実施

- ✓ モバイルフレンドリーなアプローチ
- ✓ すべてのトラフィックをヘアピンする必要がなく、高いスケーラビリティを保証

サポートされているアプリケーション

- ✓ IP ネットワーク用に書かれたあらゆるアプリケーションをサポート (例: FirstNet、AT&T ADTM、Verizon Business Services などの 3GPP QoS 標準)

Absolute Software は、約 20,000 社のお客様から信頼いただいている、自己復活型のインテリジェント・セキュリティ・ソリューションの唯一のプロバイダです。6 億台以上のデバイスに組み込まれている Absolute は、エンドポイント、アプリケーション、ネットワーク接続にインテリジェントかつ動的に可視化、制御、自己復活機能を適用する永久デジタルテザーを提供する唯一のプラットフォームで、ランサムウェアや悪意のある攻撃の脅威が高まる中、お客様のサイバー耐性の強化に貢献しています。

© 2023 Absolute Software Corporation. All rights reserved. ABSOLUTE、ABSOLUTE ロゴ、NETMOTION は Absolute Software Corporation またはその子会社の登録商標です。ここに記載されているその他の名称やロゴは、アブソリュート社またはそれぞれの所有者の商標である場合があります。本書において、各商標に ™ および ® が記載されていないことは関連商標の所有権を放棄するものではありません。その他のすべての商標は、それぞれの所有者に帰属します。ABT-SecureAccess-DS-JP-030723



Absolute Secure Access Agents

- ✓ Apple® iPad および iPhone devices (iOS 11 以降)
- ✓ Apple Mac OS (10.13 以降)
- ✓ Android デバイス (Android 5.0 以降で動作)
- ✓ Android for Work
- ✓ Samsung KNOX
- ✓ Windows Pro タブレット、ノート PC、その他 Windows 8、10、11 が動作するデバイス
- ✓ ARM プロセッサで動作する Windows および macOS デバイス
- ✓ 自己修復、Windows 向けレジリエントエージェント
- ✓ 英語、日本語、フランス語、イタリア語、ドイツ語、スペイン語のクライアントが利用可能

キャパシティとスケーラビリティ

- ✓ 最大 60,000 人の同時接続可能
- ✓ 高可用性、水平方向のスケーラアウト、ゼロダウンタイムのアップグレードを可能にする、ハイパーレジリエントなデプロイメントアーキテクチャ

サーバー (オンプレミスのみ適用可能)

- ✓ Windows Server 2016、2019、2022 の Standard 版と Data Center 版のみ。Windows Server Essentials はサポート対象外です
- ✓ サーバーの仕様は、導入規模によって異なります
- ✓ サーバーは英語と日本語で利用可能

展開オプション

- ✓ セキュアアクセスクラウド
 - ハードウェアやインフラのコストが不要
 - プロビジョニング、パッチ、メンテナンスのオーバーヘッドなし
 - レイテンシーを低減し、成長に合わせた柔軟なスケーラビリティを実現
 - モバイルファースト、クラウドファーストに最適化
 - 高可用性、水平方向のスケーラアウト、ゼロダウンタイムのアップグレードを実現する、レジリエントなデプロイメントアーキテクチャ
 - Microsoft® Azure が提供する制御と冗長性、99.999% のアップタイム SLA を保証
- ✓ オンプレミス (お客様のリクエストベースで対応)
 - エンド to エンドのセキュリティシステムとインフラをトータルに制御
 - オンプレミスのデータセンターまたは独自の仮想プライベートクラウドインスタンス内にソフトウェアを展開
 - すべてのデータとシステムをオンプレミスに置くことを要求する法律や規制の義務に対応
 - 高可用性、水平方向のスケーラアウト、ゼロダウンタイムのアップグレードを実現する、レジリエントな展開アーキテクチャを利用可能