

Absolute の インテリジェントな 自己復活ソリューション

「消えない」「切れない」
セキュリティ



コロナ禍でリモートワークやハイブリッドワークが推進されました。分散した職場環境は今後も続くことでしょう。その中でセキュリティにおいては、エンドポイントとアクセスアセスメントを完全に統合し、ゼロトラストの原則を完全に適用するセキュリティアプローチが求められています。Absolute は、エンドポイントからネットワークエッジまでの可視化と自己修復を可能にするユニークな機能を提供し、エンドユーザーの生産性とネットワークパフォーマンスに妥協することなく、セキュリティを最大化するソリューションを提供します。

68%

68%の組織が過去 12カ月以内にエンドポイント攻撃を受け、実際に被害にあっています。

Ponemon Institute, 2020 State of Endpoint Security Risk

25%

25%のデバイスで、セキュリティ対策が不健全な状態になっています。

Absolute, 2021 Endpoint Risk Report

51%

51%の組織が、侵害されたエンドポイントが会社のデータへのアクセスに使用された痕跡を確認しています。

HP Wolff Security, 2021 Blurred Lines and Blindspots Report

信頼性が高く生産性の高い「どこでも仕事できる」環境の基礎となるのは、従業員のエンドポイントをカバーし、アクセスする場所に関係なく情報交換や組織リソースへのアクセスを可能にする安全で信頼できるネットワーク接続性です。

エンドポイントが組織ネットワークへの主要なアクセスポイントであることを考慮すると、エンドポイントのセキュリティギャップは多くの脅威者に狙われており、そのためにエンドポイント上で確立されたセキュリティ制御の有効性が阻害されることがよくあります。これは、崩壊、ソフトウェアの衝突、またはサイバー犯罪者が混乱や検出のリスクを回避するためにセキュリティ機能をオフにするために発生します。

リモートアクセス機器には脆弱性がひそんでいます。身近な物理的環境がセキュリティで保護されておらず、エンドユーザーは使用する従業員が操作時の警戒や行動の際にカジュアルになりがちです。そのため、多くの組織で、侵害されたエンドポイントが組織ネットワークへのアクセスに利用されることもめずらしくはありません。組織を守るためには、エンドポイントとリモートアクセス制御の両方を保護して、レジリエントなゼロトラスト原則を確立できるようにすることが不可欠です。

すべてをカバー： ファームウェアのブートからネットワークアクセスまで

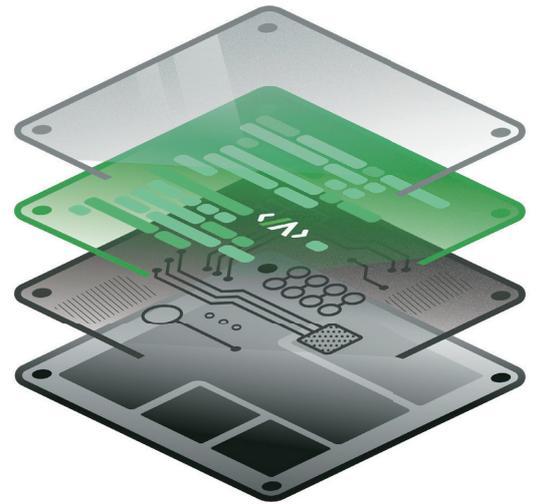
ここで、Absolute® の出番です。Absolute は 6 億台以上のデバイスに組み込まれており、エンドポイント、アプリケーション、ネットワーク接続に可視性と制御機能を提供する唯一のインテリジェント・セキュリティ・ソリューション・プロバイダです。Absolute 独自の自己復活機能を Absolute Secure Endpoint と Absolute Secure Access のパワーと組み合わせることで、最適なりモートおよびモバイルのユーザーエクスペリエンスを維持すると同時に、デバイス、データ、ユーザーを保護し、重要なセキュリティ制御が最大の効果を発揮するようにすることができます。

IT部門およびセキュリティ部門のニーズに応える共通プラットフォーム

Absolute のすべての製品ラインと個々の製品は、Absolute Platform をベースに提供されています。Absolute Platform の重要な構成要素のひとつが、特許取得済みの Persistence® テクノロジーです。このテクノロジーは 6 億台以上のデバイスのファームウェアに組み込まれており、Absolute Platform とエンドポイントとの間に安全で常時接続できる環境を提供します。このテクノロジーは一度起動すると、強い回復力を持ち、デバイスの再イメージング、ハードディスクの交換、ファームウェアの更新を行っても、無効化の試みに耐える唯一のソリューションとなります。

同じことを成しうるテクノロジーは他にありません。

この自己復活機能は、Application Resilience™ カタログに掲載されているミッションクリティカルなアプリケーションに連携されます。一度導入すると、アプリケーションの健全性が監視され、健全性が損なわれていると判断された場合には自動的に修復や再インストールを行うことができます。これにより、一般的なソフトウェアの崩壊、衝突、意図しない削除、悪意のある行為などがあってもアプリケーションは常に意図したとおりに機能することが保証されます。その他、トンネルやネットワーク接続が外的要因に強いことを保証するとともに、オーディオやビデオの伝送を最適化する特許技術 Network Resilience™ を有しています。



Persistence® テクノロジーは、6 億台以上のファームウェアに組み込まれています。

Absolute 製品を支えるコンポーネント

Absolute® Platform を構成する一連の基本コンポーネントは、お客様やエコシステムパートナーがセキュアエンドポイントやセキュアアクセスのあらゆるユースケースに対応できるようにするため構築されています。クラウドベースの安全なマルチテナントアーキテクチャを活用し、グローバルでご利用いただけます。



「消えない」エンドポイント管理 Absolute Secure Endpoint

Absolute Secure Endpoint™ 製品は、Absolute Persistence が提供する常時接続を活用して、IT 担当者およびセキュリティ担当者がエンドポイントの問題を監視して対処できるようにし、ノート PC とそのミッションクリティカルなアプリケーションを自己復活させます。

これによって、IT 資産の管理、組織のセキュリティ態勢の強化、コンプライアンスの維持が強化されます。Persistence テクノロジーは主要 PC メーカーのファームウェアに組み込まれており、削除されても自分自身を自動復活させます。「消えない」ソリューションで、エンドポイントの安全を守ります。

Absolute Secure Endpoint には、機能に応じて 3 つのフレーバーが用意されています。

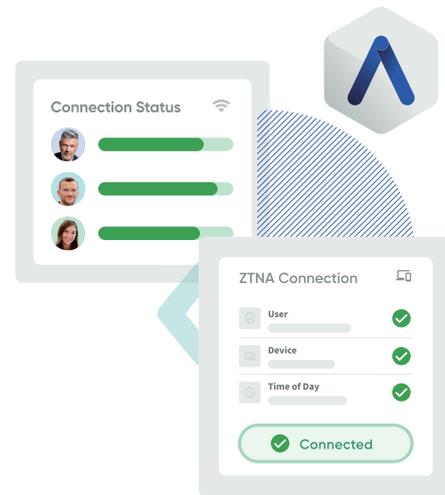
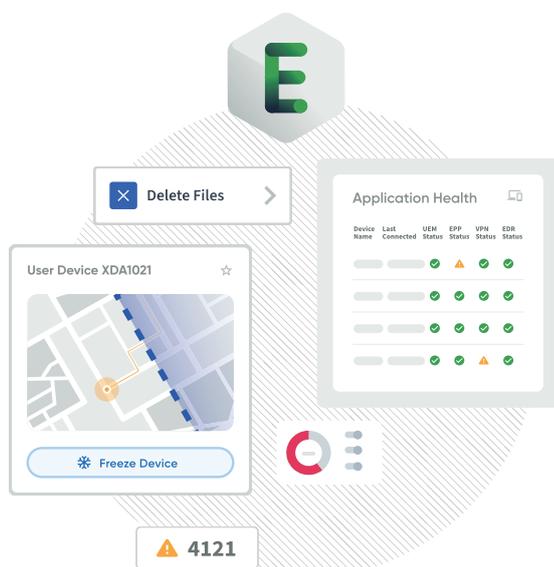
Absolute Visibility は、エンドポイントのロケーション、セキュリティ態勢、ハードウェア / ソフトウェアのインベントリに関するデータを収集します。ソフトウェアやハードウェアの利用状況を分析し、潜在的な障害箇所や疑わしい使用パターンを特定することができます。

Absolute Control は、Absolute Visibility の機能に加え、インターネット経由でエンドポイントを制御し、リモートでのファイル削除やデータ消去、危険時のオンデマンド凍結、ジオフェンスやアラートの確立を可能にします。

Absolute Resilience は、脅威や脆弱性からエンドポイントを保護し、セキュリティ侵害やインシデントに対応するための機能をさらに強化します。たとえば、ミッションクリティカルなアプリケーションを自己修復することで、デバイスの変化への耐性を確保します。

Secure Endpoint パッケージは簡単にアップグレードが可能で、簡単なライセンスフィーチャーキーで Visibility、Control、Resilience の各サービス階層を移動し、機能やカバーできるユースケースを拡張することができます。お客様のビジネスニーズに合わせて、様々なサービス階層を組み合わせてご利用いただけます。

ランサムウェアの攻撃からデバイス群を回復させる能力に主眼を置くお客様には、**Absolute Ransomware Response** を提供します。マルウェア対策やデバイス管理ツールなどのミッションクリティカルなセキュリティアプリケーションを健全な状態に保ち、自己修復が可能であることを確認し、ランサムウェア攻撃が発生した場合にエンドポイントの隔離と復旧を迅速に行うための機能とサービスを提供します。



「切れない」ネットワークアクセス Absolute Secure Access

Absolute は 2021 年 7 月に NetMotion を統合しました。これにより、ネットワークアクセスを管理する機能が Absolute のポートフォリオに追加されました。Secure Access™ 製品は、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、信頼性と回復性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、ユーザーの生産性や管理制御に影響を与えることなく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。また、信頼性の高いネットワーク接続を可能にするだけでなく、ネットワークのパフォーマンスと最適化を向上させることができます。安定した「切れない」ネットワーク接続で、エンドユーザーのエクスペリエンスを高度に維持します。

Absolute VPN は、暗号化とアクセス制御により、移動中のデータに対してセキュリティと機密性を提供します。また、トンネルやネットワークセッションのレジリエンス、ストリーミングビデオやオーディオの最適化など、エンドユーザーの利便性を向上します。

Absolute ZTNA は、ゼロトラスト・ネットワークアクセスを通じてソフトウェアで定義された境界を提供し、アプリケーションまたはアプリケーションのセットの周囲に、どこでもホストされていても、コンテキストベースの論理的アクセス境界を作成します。インターネットからアプリケーションを遮蔽し、不正なユーザーから見えないようにします。アクセスポリシーはエンドポイントで実施されるため、デバイスのデータを保護し、 choke points をなくすことができます。

Absolute Insights for Network は、エンドポイントおよびネットワーク全体の診断およびエクスペリエンス監視機能を提供し、組織が所有または管理していないネットワーク上でも、エンドユーザーのパフォーマンス問題を迅速かつ大規模にプロアクティブに監視、調査、修復することを可能にします。Secure Access は、Absolute Core Plus (Absolute VPN およびポリシーエンジン) と Absolute Edge (上記 3 製品すべてを含む) の 2 種類のフレーバーで提供されます。

ワンベンダーのメリット

Absolute Secure Endpoint と 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るため、予算管理が効率化され、シンプルなベンダー管理を実現します。

オペレーションの効率と生産性を向上

- ✓ ハードウェアとソフトウェアの在庫活用を最適化
- ✓ デバイス、アプリケーション、ネットワークの使用状況を把握
- ✓ ネットワーク接続の継続性を確保
- ✓ ネットワークとアプリケーションのパフォーマンスを最適化
- ✓ デバイスの追跡と位置確認により、紛失したデバイスや盗難にあったデバイスの回収を支援
- ✓ リモートデバイスのライフサイクル管理（デバイスの再生や再プロビジョニングなど）を実現
- ✓ アプリケーションを自律的に監視し、自己修復して可用性を確保
- ✓ エンドポイントやネットワークアクセスに関するヘルプデスクの効率を向上

リスクを軽減しコンプライアンス体制を強化

- ✓ デバイスのセキュリティ態勢を評価し、セキュリティインシデントを検出
- ✓ ジオフェンスを設置し、リスクのあるデバイスを特定
- ✓ ミッションクリティカルなアプリケーションを自律的に監視し、自己修復することで、セキュリティ標準を強化
- ✓ デバイス群から機密データを検出
- ✓ 監査に必要な証拠や報告を提供
- ✓ 脆弱性への露出を最小限に抑制
- ✓ エンドポイントリスクに対応し、インシデントから復旧
- ✓ パスワードの依存性を排除し、ユーザー / 組織リソースを保護
- ✓ 最新のセキュリティフレームワークを採用

ビジネスを強化

- ✓ 「どこでも働ける」環境でのワークフォースを実現
- ✓ ユーザーエクスペリエンスを最適化
- ✓ ファーストレスポンスやフィールドワーカーなどに対するサービス提供の継続を保証



お客様が Absolute を評価する理由

G2.com ユーザーレビューでの評価

Secure Endpoint と Secure Access
両製品の平均スコア：5 点満点中 4.7 点

★★★★★

セキュリティチームに安心をもたらします。

紛失したコンピューターに何が入っていたのか、いつ紛失したのか、どこで紛失したのか、どのマネージャーから聞かれても答えられます。暗号化されていたかどうか、最後に使ったのは誰なのかもわかります。HIPAA を順守するためには、Absolute で得られる情報と制御が必須です。

IT セキュリティエンジニア / 従業員数 1,000 人以上

★★★★★

まさに求めていたものです。

これまで使ってきたデバイス管理ソリューションの中で、最も優れているもののひとつです。Absolute は意図した通りの働きをしてくれるので、すべてのデバイスを管理するのに役立っています。当社では、すべてのデバイスを最新の状態に保たなければなりません。Absolute は、ネットワーク外のデバイスも管理する能力を与えてくれました。

企業顧客 / 従業員数：1,000 人未満

★★★★★

盗難対策だけではありません。

資産回復において威力を発揮するソリューションです。それだけでなく、エンドポイントでもデバイスやアプリケーションを管理できることに真価があります。コロナ禍においては Absolute を使えるのはありがたいことでした。

CIO / 従業員数：1,000 人未満

Gartner Peer Insights での評価

Secure Endpoint と Secure Access
両製品の平均スコア：5 点満点中 4.7 点

★★★★★

Absolute Software は、ビジネス・ソフトウェアの保守に加えてセキュリティ制御の開発を支援してくれます。

情報セキュリティ脅威アナリスト
銀行 / 従業員数：年商 5,000 万ドル未満

★★★★★

Absolute は、組織内外のネットワークで組織の資産をトラッキングできる素晴らしい製品です。

セキュリティ・オペレーション部門責任者
金融 / 年商 2,500 ~ 5,000 万ドル

★★★★★

Absolute によって、コンプライアンスを維持し、正確性を期することができます。

ネットワーク管理者
ヘルスケア / 年商 5 億 ~ 10 億ドル

Absolute Software は、18,000 社以上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。

