DATA SHEET

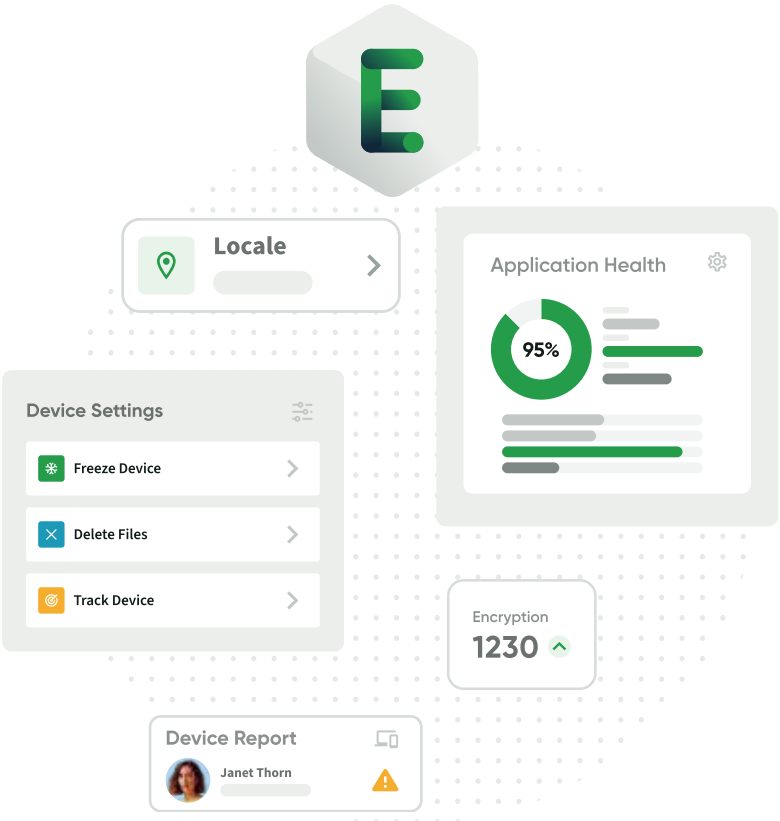
# Absolute Secure Endpoint

## ハイブリッドワーク時代の高信頼、レジリエントなエンドポイント管理

今日のリモートワークまたはハイブリッドワーク環境の従業員の主要な仕事道具として機能しているエンドポイントを管理しセキュリティを確保するために、ほとんどの IT チームは、専用のソフトウェアを使用しています。IT チームにとっては、エンドポイント管理は、エンタープライズ・インフラストラクチャー戦略の基本的な要素であるといえます。

「どこでも働ける」業務環境への急速な移行は、組織ネットワークへの接続に依存する従来型のアプローチを採用していた組織にとって、大きな課題となりました。エンドポイントの可視化とセキュリティ制御を確立する場合、IT 担当者やセキュリティ担当者は、防御に踏み込んだアプローチを確立する必要があります。ネットワークに接続するエンドポイントが、セキュリティ管理の不備のために安全でない可能性がある場合、ネットワークのセキュリティだけに注力しても有効ではありません。防衛戦略を成功させるためには、各エンドポイントの耐障害性を高めることが重要です。

同時に、ユーザーはどこにいても一貫した良質なエクスペリエンスを期待しています。一般にユーザーは、採用されているテクノロジーが機能することを望んでおり、必要なリソースに確実かつ一貫してアクセスできるのであれば、バックエンドで何が起ころうとも気にはとめません。つまり、ユーザーがリモートで仕事をする場合、IT 部門はより高いレベルの可視性を確保し、場所に関係なく一貫したエクスペリエンスを提供することが求められるのです。




### パーシステンスの成果

そこで Absolute® Secure Endpoint の出番です。Dell、HP、Microsoft、Lenovo などの大手メーカーの PC には、デバイスが工場を出る前にファームウェアに **Absolute Persistence®** 技術が組み込まれています。Absolute Persistence は、デバイスの再インメージ、ハードディスクの交換、ファームウェアの更新があっても、起動シーケンスごとに Absolute Agent を自動的に修復して再インストールします。一度 Absolute Secure Endpoint が起動されると、常時接続のデジタルテザーによって必要な耐性が提供されます。これにより、何が起きても、常にデバイスを確認、制御し、セキュリティギャップに対処することができるようになります。

Absolute Secure Endpoint™ 製品ポートフォリオは、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、エンドポイント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。

## IT とセキュリティを強化

Absolute Secure Endpoint の製品群は、汎用性を持ち、組織内のさまざまなステークホルダーを対象とした多数のユースケースに活用することが可能です。エンドポイント管理やエンドポイントセキュリティのソリューションを導入済みであっても、それらのツールには限界や盲点があり、エンドユーザーによって無効化されたり、デバイスのリソースを奪い合ったりして、意図した通りに機能しないことがよくあります。

そうなると、エンドポイントの確認、制御、セキュリティ確保が困難になります。そのために、不正確な情報、運用の非効率性、セキュリティギャップが生じ、問題を確実に検知して脅威に自信をもって対応する能力が損なわれてしまいます。

結果として、不確実な監査、リソースの浪費、データ漏洩、コンプライアンス違反が避けられなくなります。


## エンドポイントに対する疑念を払拭し、セキュリティを保つ

今日の分散型組織では、エンドポイントやアプリケーションにインテリジェントかつダイナミックに可視化、制御、自己修復機能を適用し、サイバーレジリエンスの強化を支援する常設のデジタル接続が求められています。

分散した従業員に対応し、サイバーレジリエンスを実現するために、IT 管理者やセキュリティチームは、資産インテリジェンス、レジリエントなエンドポイントセキュリティ、確信に満ちたリスク対応が統合されたソリューションを必要としています。そのような組織では、Absolute Secure Endpoint が威力を発揮します。

## 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**

- **ハードウェアの在庫管理を最適化**　ハードウェアのインベントリを常に正確に把握し、ハードウェアの監査を合理化し、マルチプラットフォームの断片化を回避し、リース管理を最適化します。
- **ソフトウェアの在庫管理を合理化**　ソフトウェアのインベントリを常に正確に把握し、ソフトウェア監査を合理化し、エンドユーザーの生産性を最適化して、シャドー IT を検出し根絶します。
- **使用状況を把握**　ハードウェアの無駄を特定して排除、ソフトウェアの無駄を特定して排除、想定されるユーザー行動を検証し、使用パターンの分析、ROI の証明を行います。
- **リモートデバイスのライフサイクル管理**　リモートデバイスのプロビジョニング、リモートデバイスの設定、デバイスの返却と安全な再配布の実施、リモートデバイスの廃止の合理化を可能にします。
- **ヘルプデスクを効率化**　デバイスの問題を予測し、ヘルプデスクツールを充実させ、効率的かつ大規模に問題を解決し、解決までの時間を短縮します。

ゴール
**リスクを軽減しコンプライアンス態勢を強化**

- **セキュリティ態勢を評価**　エラーになったセキュリティアプリの検出、設定の逸脱の検出、脆弱な OS やアプリの検出、規制や業界標準への準拠をレポートします。
- **セキュリティ標準を実施**　セキュリティアプリを自己修復、標準構成を実施、脆弱な OS やアプリを修復、ファームウェア保護をリモートで有効にします (Lenovo のみ )。
- **セキュリティインシデントを検出**　不審なデバイスの使用や移動を検出、紛失したデバイスを特定、( 工場からの移動中を含めた ) デバイスの改ざんを検出、危険にさらされた機密データを検出します。
- **エンドポイントリスクに対応**　機密データファイルのリモート保護、盗難や疑わしいデバイスの調査、侵害されたデバイスの修復、ゼロデイ攻撃への対応を実施します。
- **インシデントからの回復を成功させる**　ランサムウェアへの戦略的な準備状況を確認、インシデント後の侵害通知を回避、将来の同様のインシデントを防ぐために根本原因を特定、回復作業を支援し迅速化します。( ランサムウェアへの対応など )



ABSOLUTE®

# お客様のビジネスニーズに対応する 3つの製品群

Absollute Secure Endpoint には、機能に応じて 3 タイプの製品があります。

最上位製品

## Absolute Visibility

デバイスとアプリケーションの
健全性の情報を正確に表示

含まれている機能

- ✓ デバイスの健全性
- ✓ セキュリティ態勢
- ✓ アプリケーションの健全性
- ✓ デバイスの使用状況
- ✓ ジオロケーション

## Absolute Control

リスクにさらされたデバイスや
データを保護する防御線

Absolute Visibility に含まれる機能
および以下の機能

- ✓ ジオフェンス
- ✓ デバイスのフリーズ
- ✓ ファイルの削除
- ✓ デバイスのワイプ
- ✓ エンドユーザー向けメッセージ
- ✓ リモートファームウェア保護

## Absolute Resilience

アプリケーションの自己復活と
リスクへの着実な対応を実現

Absolute Control に含まれる機能
および以下の機能

- ✓ Web Application Usage
- ✓ エンドポイント・データ・ディスカバリ
- ✓ アプリケーション・レジリエンス
- ✓ 修復スクリプト・ライブラリ
- ✓ 紛失・盗難デバイスの調査と回収

## Absolute Ransomware Response

ランサムウェアへの対策と感染時の迅速なリカバリ

含まれている機能

- ✓ 戦略的ランサムウェア対策チェック
- ✓ エンドポイント全般にわたるサイバーハイジーン・ベースラインの策定と実施
- ✓ リカバリータスクの推進
- ✓ リモートアシスタンス ( 原則として英語のみ )

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。