DATA SHEET

Absolute Resilience

エンドポイントやミッションクリティカルなアプリケーションをサイバーレジリエントに。自動復活で安全を保護

Absolute Secure Endpoint の最上位モデル

多くの組織は、サイバー脅威を防ぐために、セキュリティコントロール (アンチウイルス、アンチマルウェア、エンドポイント保護プラットフォーム、統合エンドポイント管理など) の実装を積極的に行っています。残念ながら、多くは、一度セキュリティ対策を施せば、その効果はいつまでも続くと思い込んでいます。その結果、確立されたセキュリティ管理が意図したとおりに機能しているかどうかの検証が行われないことが多いのです。このアプローチは、サイバー敵の攻撃チェーンの盲点を突くことになり、組織のサイバーリスク露出を不必要に増加させることになります。各エンドポイントを崩壊、ソフトウェアの衝突、人為的ミス、悪意のある行為に強いものにすることは、防衛とインシデント対応戦略を成功させるために最も重要なことです。

Absolute は、エンドポイント・レジリエンスのパイオニアであり、エンドポイントやインストール済みのミッションクリティカルなアプリケーションに対する悪条件、ストレス、攻撃、侵害を予測し、耐え、回復し、適応することを可能にします。

25%

セキュリティ管理 (アンチウイルス、アンチマルウェア、エンドポイント保護プラットフォーム、統合エンドポイント管理) が常時不健全なデバイスの割合

6 億台以上

Absolute Persistence® を搭載した大手システムメーカー製デバイスの数

Absolute Platform のパワーを活用する

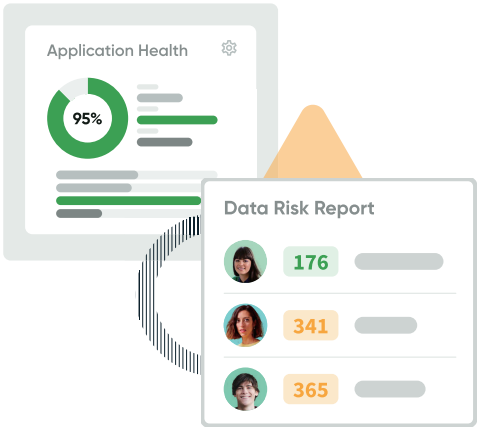
Absolute Resilience™ は、セキュリティ体制の強化、コンプライアンス体制の強化、IT およびエンドユーザーの生産性の向上を実現します。Absolute Visibility™ と Absolute Control™ のすべての機能に加え、脅威や脆弱性からエンドポイントを保護し、セキュリティ侵害やインシデントに対応する重要なレジリエンス機能を備え、Absolute Application Resilience により不健康なアプリケーションを自動的に監視・検出し、自律的に自己復活させます。

IT 管理者は、Absolute Platform を構成するクラウドベースの Absolute® Console または Absolute Mobile App から、デバイス・フリート全体を確認することができます。Absolute Persistence® テクノロジは、主要なシステム・メーカーの 6 億台以上のデバイスに組み込まれています。Absolute Persistence が提供する常時接続を活用することで、自己復活機能をミッションクリティカルなアプリケーション (エンドポイント管理やセキュリティ・ツールなど) に拡張し、無効化、変更、アンインストールされたときに自己復活して再インストールする力が与えられます。Absolute Data Science チームの調査によると、25% のデバイス上のセキュリティ制御 (アンチウイルス、アンチマルウェア、エンドポイント保護プラットフォーム、統合エンドポイント管理など) が常時不健全になっていることが明らかになっています。

信頼できるリスク対応

Absolute Resilience は、エンドポイントやミッションクリティカルなアプリケーションに強力な復活力をもたらし、大規模な修復を迅速に行うことを可能にします。

- **デバイスの機密情報を特定**　金融情報、社会保障番号、PII、PHI、知的財産などの機密データをエンドポイントでスキャンし、リスク露出を最小限に抑え、コンプライアンス態勢を強化
- **ミッションクリティカルなアプリを自己復活**　ミッションクリティカルなアプリを偶発的または意図的な削除から保護し、セキュリティコントロールと重要な回復ツールが意図したとおりに機能していることを確認し、不健康なアプリを修正することで最適なユーザーエクスペリエンスを提供
- **リモートでデバイスを照会し、修復**　設定から廃止までのリモートライフサイクル管理を合理化し、解決までの時間を短縮し、リスク露出を最小化
- **Web アプリのの利用状況を把握**　Web サブスクリプションの利用状況を把握、Web プリケーションの利用パターンを分析、投資対効果を証明、不正またはリスクのある Web アプリケーションの利用状況を把握
- **紛失または盗難デバイスの調査・回収**　経験豊富な調査チームを活用し、警察棟と連携して盗難デバイスを回収し、デバイス回収コストを削減



ABSOLUTE®

エンドポイントの安全性を保証

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死角があります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、うっかりすると意図したとお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。

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。

お客様のビジネスニーズに対応する 3 つのフレーバー

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

Absolute Visibility

デバイスとアプリケーションの健全性の実情を正確に表示

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

- 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表示
- リモートでのファームウェア保護

最上位製品

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

- Web Application Usage
- エンドポイント・データ・ディスカバリ
- Application Resilience
- 修復スクリプト・ライブラリ
- 紛失・盗難デバイスの調査と追跡レポート

Absolute Resilience Add-On

- **Absolute Insights for Endpoint** 管理者がデバイスやセキュリティの傾向を把握可能
- **Absolute 紛失デバイス追跡レポート** Absolute Reclamation の専門家チームが、デバイスを追跡、発見、保護し、デバイスを取り戻すためにユーザーと連絡を取るなどにより、デバイスを調査し、トラッキングレポートを作成
- **Absolute Ransomware Response for レジリエンス** Absolute レジリエンス を強化し、デバイス群全体のランサムウェアへの備えと復旧を優位に促進

関連製品パッケージ

- **Absolute Resilience for Chromebooks** Chromebook ユーザーに特化されたパッケージ
- **Absolute Resilience for Education** 教育機関のユーザーに特化されたパッケージ
- **Absolute Resilience for Student Devices** 学生、生徒向けデバイスに特化されたパッケージ

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。