DELL Technologies

Dell SafeData

Absoluteプラットフォーム

データとデバイスを確認して保護

エンドポイントのインテリジェンスと耐障害性を高める唯一のファームウェア組み込みソリューション

あらゆる適切な戦略を実装していても、従来型のエンドポイント管理ツールとセキュリティ ツールには制限と死角があります。これらのツールはエンドユーザーによって無効化されたり、デバイス リソースの競合が発生したりして、不注意から意図したとおりに機能しなくなります。

その結果、エンドポイントの確認、制御、保護が困難になります。これにより、不正確さ、運用上の非効率、セキュリティのギャップが発生して、問題を確実に検出し、自信を持って脅威に対応することができなくなっています。避けられない結果として、監査が不確実になり、リソースの無駄、データ侵害、コンプライアンス違反が発生します。

Dellはデバイスが工場から出荷される前に、Absoluteが特許を取得したPersistence®テクノロジーをファームウェアに組み込んでいます。Persistence®は、デバイスが再イメージ化された場合やハード ドライブが交換された場合でも、ブート シーケンスごとにAbsoluteエージェントを自動的に修復して再インストールします。

Absoluteがアクティブになると、強固なデジタル テザーを通じて必要な耐障害性が提供されます。そのため、何が起きても常にデバイスを確認して制御し、セキュリティのギャップに対処できます。

詳細については、DellEMC.com/endpointsecurityをご覧ください

ABSOLUTE®

資産インテリジェンス

持続的なエンドポイント可視性：ネットワークの内外を問わず機能

Absoluteは各デバイスへのデジタル テザーの完全性を確保し、お客様の企業ネットワークの内外を問わず、すべてのエンドポイントで信頼性の高いインテリジェンスを提供します。

ハードウェアとソフトウェアのインベントリーを常に最新状態に保ち、デバイスのライフサイクル管理を合理化して、監査と毎日の運用を高速化できます。また、デバイスの移動時にアラートを受け取ることや、使用率の低いリソースを検出して無駄を防ぐことや、そのような情報を使用してコスト パフォーマンスに優れた意思決定を行うことができます。

お客様の成功基準：

組み込み型＆自己修復：デバイスのファームウェアに組み込まれた自己修復テクノロジーを搭載した唯一のプラットフォームにより、プラットフォームやネットワークを問わず1つのダッシュボードからフリート全体を確認、制御できます

ハードウェア分析：すべてのエンドポイントを見守り、あらゆるエンドポイントが記載された常に最新状態の完全なインベントリーを構築します。デバイスごとに数百のデータ ポイントを表示します

地理的な位置情報：ネットワークの内外を問わず、任意の対象デバイスの物理的な位置をいつでも正確に追跡します。追跡内容には履歴ログも含まれます

リモート 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、再割り当て、廃棄を合理化します。例えば、定期的なメンテナンスの自動化、デバイスの問題への対処、認定済みのライフサイクル終了消去の実行ができます

ソフトウェア レポートとアラート：ソフトウェア インベントリーを最新状態に維持し、シャドーITを根絶して、必要なアプリケーションが見つからない場合を検出します

デバイス使用率：デバイスがどのように使用されているかを理解し、非アクティブな資産を特定して、再割り当てすべき資産と停止が必要な資産を決定します

耐障害性を備えたエンドポイント セキュリティ

セキュリティ体制を評価してセキュリティ制御を適用

単一のクラウドベースのコンソールから、標準または規制へのコンプライアンスに関するレポートを作成し、その情報を組織内のステークホルダーと共有します。構成の逸脱と脆弱性を検出し、セキュリティ アプリケーションを自動的に適用します。また、コマンドとワークフローをリモートで導入してセキュリティのギャップに対処し、それらの「必須」タスクを自動化します。

Absoluteは、任意の他のセキュリティ制御を持続できる最初で唯一のエンドポイント可視性および制御ソリューションです。Absoluteの耐障害性を他のアプリケーションに拡張することで、セキュリティ スタック全体が自動修復できるようになります。これにより、デバイスを持ち込むことなく、その強固なセキュリティをフリート全体に拡張できます。エンドポイントが望ましいイメージから逸脱すると、Absoluteは破壊的なデータ侵害を回避してビジネス継続性を確保するために、強制的に調整を行います。

お客様の成功基準：

標準ベンチマーキング：サイバーセキュリティ標準またはデータ プライバシー規制へのコンプライアンスに関するレポートを作成し、暗号化またはマルウェア対策がなされていないデバイスにフラグを付け、コンプライアンス ギャップを解消します

構成の強化：望ましいエンドポイント構成を基に弱点と逸脱を検出し、大規模に調整を行います

詳細については、DellEMC.com/endpointsecurityをご覧ください

ABSOLUTE®

アプリケーションの継続性：アプリケーションが自動修復するので、ユーザーの生産性とビジネス継続性は妨げられません

データ保護の保証：暗号化、マルウェア対策、VPN、エンドポイント管理などのセキュリティ制御を持続させて、データ保護を強化します。その際、人手は必要ありません

脆弱性の検出と解決：企業ネットワークの内外を問わず、脆弱なOSバージョンを実行しているエンドポイントを特定し、緊急のアップデートをプッシュするか保護対策を実装します

自動ワークフロー：コマンドと自動ワークフローをリモートで導入して、セキュリティのギャップに迅速かつ大規模に対応します

確実なリスク対応

セキュリティ インシデントを検出し、対応を行って正常に復旧

Absoluteを使用すると、デバイスの深部にアクセスしてリスクのある機密データを検出し、未使用デバイスや疑わしい動作を特定できます。前兆、脆弱性、侵害、リカバリーなど、インシデントのあらゆる段階を通じて、Absoluteは確実な対応とリカバリーを行うための持続的なツール スイートを提供します。

未使用デバイスの脆弱性、漏洩、または新しいアクティビティに対して即座にアラートを受け取ります。それらのデバイスをロック ダウンして、保存されているデータを消去します。インシデントの発生中にデータが常に保護されていたことを規制当局に証明します。履歴ログを利用して侵害通知を回避し、根本原因について学習して、同様のインシデントがさらに発生するのを防止します。

お客様の成功基準：

エンドポイント データの検出：HIPAA、GDPR（一般データ保護規則）、CJIS、CCPAといったプライバシー規制に違反するリスクや恐れがある機密データ（IP、PII、PHI、PFIなど）を特定します

早期インシデント検出: 無効になっている制御とデバイス改ざんの証拠に関するアラートを受け取り、データを搭載したデバイスが誤った場所に置かれてしまった場合に把握します

未使用デバイスのレポート：一定期間オフラインになっているデバイスを検出し、それらのデバイスがインターネットに接続するとすぐにアラートが出されるように「未使用」のフラグを付けます

緊急データ保護：侵害されたデバイスをリモートでフリーズまたは削除してサニタイズの証明書を取得し、データ転送を防止するほか、その他多くの修復処置を大規模に実行します

調査エキスパート：経験豊富な調査員で構成されるAbsoluteチームを活用できます。Absoluteチームは法執行機関と緊密に協働し、起訴、盗まれたデバイスの回収、またはフォレンジック ツールによるユーザーの特定を行います

コンプライアンスの証明：履歴ログを利用して、インシデント発生中にデータ保護が有効であったことを確認します。また、根本原因について学習し、セキュリティ ポリシーを反復処理します

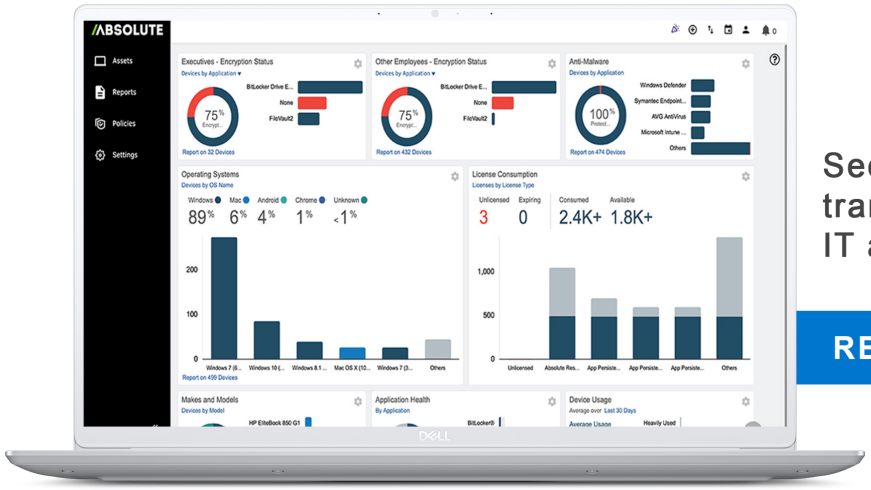
詳細については、DellEMC.com/endpointsecurityをご覧ください

ABSOLUTE®

エンドポイントの安全性に関する不安を払拭

今日の分散型組織には、エンドポイントを持続的に可視化して制御することが必要です。モバイル ワーカーに対応し、組織で耐障害性を高めるために、ITチームとセキュリティ チームは、資産インテリジェンス、耐障害性を備えたエンドポイント セキュリティ、確実なリスク対応が高度な融合したプラットフォームを頼りにします。すなわち、Absoluteプラットフォームを頼りにします。

Absoluteがどのように役立つかの詳細については、absolute.com/platformを参照してください



See how Absolute can transform your organization's IT and Security

REQUEST A DEMO

Absolute Resilienceさえあれば、アプリケーションとセキュリティ ツールは破壊不能

Absolute Resilienceには、持続的なデータ ストリーム、自動インベントリー、リスクのあるデバイスのデータ消去またはロックダウン機能など、可視性と制御性を向上させる機能がすべて備わっています。

アプリケーションのデータ保全

無効化、削除、再構成を試行した後に自己修復と再インストールを行う機能を ミッションクリティカルなアプリケーションに追加します。

エンドポイントデータの検出

ネットワークの内外を問わず、WindowsデバイスとMacデバイス、またはリスクのある機密データ（PII、PHI、PFI、SSN、GDPR（一般データ保護規則）など）と知的財産をスキャンするポリシーを設定し、漏洩のコストを見積もります。

絶対的なリーチ

事前に構築およびカスタマイズされたスクリプトのライブラリを使用し、WindowsデバイスとMacデバイスをもれなく評価して修復処置を実行します。

調査

元法執行機関の専門家で構成されるAbsoluteチームが、紛失または盗難にあったデバイスを追跡し、地域の機関と協力してそれらのデバイスをリカバリーします。

詳細については、DellEMC.com/endpointsecurityをご覧ください

ABSOLUTE®

	Absolute Visibility	Absolute Control	Absolute Resilience
Absolute Console	●	●	●
ハードウェアの追跡	●	●	●
デバイス使用状況の測定	●	●	●
インストール済みソフトウェアのモニタリング	●	●	●
セキュリティ体制の評価	●	●	●
重要なアプリケーションの正常性のモニタリング	●	●	●
サードパーティー統合	●	●	●
不正なデバイス移動の検出		●	●
デバイスのリモート フリーズ		●	●
データのリモート削除		●	●
ファームウェア保護の有効化		●	●
重要なアプリケーションの自己修復			●
デバイスの機密情報の特定			●
リモートによるデバイスの大規模なクエリ＆修復			●
盗難デバイスの調査とリカバリー			●

サポート プラットフォーム：

セキュリティ体制を向上できるDell SafeData製品については、担当のDellエンドポイント セキュリティ スペシャリスト(endpointsecurity@dell.com)までお問い合わせください

詳細については、DellEMC.com/endpointsecurityをご覧ください

ABSOLUTE®

DELL Technologies