妥協のない可視性の確立と侵害があった場合にリアルタイムに元の正常な状態に修正。Absoluteの自己回復型エンドポイントセキュリティなら可能です。

セキュリティ戦略を強化するAbsolute® Data & Device Security。すべてを可視化し、侵害に対してリアルタイムに対処する適応型エンドポイント・セキュリティ・ソリューションです。Absoluteは、エンドポイントおよびそれらに含まれるデータに対して、永続的な接続を実現します。これは、デバイスが企業ネットワークからオフラインになっている場合でも、また紛失したり、盗まれたりした場合でも、常に制御できることを意味します。

Absolute Data & Device Security（旧Computrace®）をセキュリティラインナップに組み込むことにより、セキュリティスタックを強化し、コンプライアンスを確立し、欠陥を瞬時に修正できます。

ネットワーク接続がオンラインであるかオフラインであるかに関係なくデータやデバイスを監視し、セキュリティで保護

監視できないものはセキュリティで保護できません。Absoluteを使用すれば、各デバイスと信頼性の高い双方向接続を維持して、エンドポイントの妥協のない可視性を確立できます。この永続的な接続により、リスクを評価するために必要な情報を入手でき、リモートからセキュリティ対策を適用できます。これらの機能は、クラウドベースのコンソールを介して実現され、ITインフラストラクチャを追加する必要はありません。

Absoluteが有効になっているエンドポイントはクラウドベースのモニタリングセンターに定期的にチェックインし（デフォルトでは24時間ごと）、正常性とセキュリティを判断するうえで必要な情報を配信します。

Absoluteを使用すると、リモートから監査とコンパライアンス違反の修正を行うことができます。また、ケース固有のコンプライアンスと詳細なセキュリティ対応計画を使用して、セキュリティ上の問題を素早く解決できます。インターネットアクセスのないオフラインデバイスについてはどうでしょう。オフラインポリシーを使用することにより、あらかじめ設定されている時間を経過してもインターネット接続のないデバイスを、自動的にフリーズできます。

紛失または侵害の可能性がある場合は即座に対応します。システムの最後の既知の状態を検証し、リスクが存在すると判断された場合は、リモートからアクションを実行します。このようなアクションには、NIST準拠のハード・ドライブ・ワイプの実行や、ユーザーにメッセージを送信してシステムをフリーズすることがあります。また、Absoluteの専門調査担当者に支援を依頼して、リモートからフォレンジック調査を行い、紛失または盗まれたデバイスを回復することもできます（ただし、一定の条件が必要です）。

持続技術のメリット

Absoluteの特許取得済み持続®技術により、エンドポイントおよびそれらに含まれるデータとの間に、自己回復機能のある双方向接続を実現できます。この技術は、デル製PCやその他のほとんどのコンピュータ、タブレット、スマートフォンのコアに組み込まれているため、ほとんどすべての既存のデバイスで有効化できます。

Absoluteクライアントをデバイスにインストールすると、デバイスのコアに存在するファームウェアエージェントが有効化され、自己回復機能のあるエンドポイントセキュリティが有効になります。双方向接続は、ファームウェアやアプリケーションの改ざん、ハードドライブの除去、OSの再インストールに耐えられるように設計されています。

既存のIT投資のコンプライアンスと価値の検証

Absoluteを使用すると、ネットワーク接続がオンラインであるかオフラインであるかに関係なくデバイスを監視および制御できるだけでなく、既存のセキュリティスタックを実質的に強化できます。Absoluteでは、レポート作成、アラート、およびSIEM統合を介して、インストールされている他のセキュリティアプリケーションのステータスを検証し、セキュリティで保護されているデバイスのコンプライアンス準拠を証明できます。さらに、AbsoluteにはSCCM回復機能が備わっ

ており、クライアントを一貫性のある手順で管理できます。

Absoluteの自己回復技術を、他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、エンドポイント管理アプリケーション、およびVPNアプリケーションと統合して、エンタープライズクラスの耐障害性を実現することもできます。

Absoluteが提供する可視性と修正能力

導入されているデバイスおよびオペレーティングシステム全体をAbsoluteのクラウドベースのコンソールからプロアクティブに保護できます。Absoluteのグローバル監視センターはエンタープライズクラスの機能を持ち、ISO認定を取得しています。何百万台ものデバイスが毎日、Absolute監視センターと連絡を取り合っています。

レポート作成と分析

履歴データなどの情報を、各デバイスから収集できます。不適格なソフトウェア/ハードウェアのインストール、IPアドレス、ロケーション、ユーザーの変更など、セキュリティインシデントにつながるアクティビティや前兆を識別できます。SIEMと統合することも、Absolute Security Vitals Dashboardを使用することもできます。

地理情報

デバイスの最近および過去の所在地をGoogle Maps™上で追跡できます。企業のポリシーに基づいて、ジオフェンス（仮想的な地理的境界線）および領域外アラートを作成し、不正な場所に移動しているデバイスを調査できます。

リスクの評価

重大度の高いセキュリティリスクに関連するイベントについてポリシーとアラートを設定することにより、セキュリティインシデントを未然に防ぐことができます。不適格なデバイスの識別、ブラックリストに登録されたアプリケーションがインストールされた際のアラート通知、不正な従業員へのフラグ設定が行えます。SCCMなどの重要なアプリケーションのステータスの検証と監視が行えます。

リスクへの対応

適応型セキュリティ対策を有効化できます。オフラインポリシーを設定して、デバイスを自動的に保護できます。データの回復または削除、デバイスのフリーズ、ステータスのやり取り、監査ログの生成、データ削除を認定するワークフローの使用によるデバイスの使用停止が行えます。デバイスがリスクにさらされていたときにエンドポイントデータや企業ネットワークにアクセスされていなかったことを証明できます。

エンドポイントデータの検出

不適格なデータを識別し、修正できます。デバイス上の個人の医療情報や個人を特定できる情報などの機密データを検出し、付随するリスクを評価できます。クラウド・ストレージ・アプリケーションと同期されている機密データを検出できます。

エンドポイントの調査

組織内部の脅威を、阻止し、識別し、排除できます。Absoluteの調査チームを活用して、エンドポイントで発生したセキュリティインシデントの原因を特定できます。紛失した、または盗まれたデバイスを見つけて、必要に応じて回復できます。データ漏洩の通知が必要であるかどうかを判断できます。

Absoluteのエディション

Standard

ネットワーク接続がオンラインであるかオフラインであるかに関係なく資産を管理できる信頼性の高いソリューションをお探しの企業や組織に最適です。ハードウェアとソフトウェアのレポート作成と分析、デバイス所在地のマッピング、ログ記録とレポート作成、通話履歴、制御喪失レポートなどの機能を備えています。

Professional

セキュリティリスクを表示する能力およびデバイスとデータの制御と修正の能力を備えたソリューションをお探しの企業や組織に最適です。デバイスの使用状況、デバイスの所在地（ジオフェンシング）、デバイスにインストールされているセキュリティソフトウェアの正常性、暗号化ステータス、クラウド共用の有無、SCCM自己回復などに関するレポート作成と制御の機能、およびセキュリティダッシュボードを備えています。セキュリティデータをSIEMソリューションに送信するためのコネクタも備えています。

Premium

Professionalのすべての機能に加えて、エンドポイントでの機密データの検出機能を備えています。また、Absoluteの調査チームによる専門サービスを利用できます。調査サービスでは、フォレンジック調査、および地域の司法当局との合同による盗まれたデバイスの調査と回復が行われます（ただし、一定の条件が必要です）。

テクニカル要件

Absolute DDSエージェン

- Windows 7、8、8.1、10（32ビットおよび64ビット）
- Mac OS X 10.6以降
- Android 4.4.2以降
- インターネット接続

Absoluteクラウド・ベース・コンソール

- Windows Internet Explorer
- Microsoft Edge（Windows 10）
- Mozilla Firefox（WindowsおよびMac）
- Google Chrome（WindowsおよびMac）
- Safari（Mac

詳細情報:
http://www.dell.com/ja-jp/work/learn/software-security-data-security