ABSOLUTE®

2024 サイバーレジリエンス・リスク・インデックス

多くの企業や団体で、AI がもたらすセキュリティ上の課題への備えができていない；

エンドポイントおよびネットワークセキュリティのアプリケーションで、しばしばエラーが発生

サマリー

サイバーレジリエンスは、従来のサイバーセキュリティよりも大規模かつ重要なパラダイムです。効果的なサイバーレジリエンス機能を持つ企業や団体は、サイバー攻撃、技術的な不具合、または意図的な改ざんの試みに耐え、迅速に通常の業務に回復できるデジタルオペレーションを備えています。今年のレポート「Absolute Security サイバーレジリエンス・リスク・インデックス 2024」の目的は、今日のグローバル企業のサイバーレジリエンスの状況を評価するとともに、サイバーレジリエンス能力が軽減できるセキュリティリスク要因を特定し、明らかにすることです。

調査は、企業のセキュリティにとって最も高いリスクの種類を判断することを目的として、当社のファームウェア組み込みソリューションを実行する Windows 10 および 11 が稼動している 507万44台の PC およびスマートデバイスからの匿名化されたテレメトリを収集して行われました。主な調査結果は以下の通りです。

- PC で自動修復機能がサポートされていない場合、EPP とネットワーク・アクセス・セキュリティ・アプリケーションは、24%の確率でセキュリティポリシーへのコンプライアンスを維持できない
- AI 技術をサポートするためには、企業や団体の PC の 92% を更新または交換する必要があり、大規模なセキュリティ上の課題につながる可能性がある
- 多くの企業や団体で、脆弱性のパッチ適用が数週間から数カ月遅れており、リスクギャップが拡大している

Absolute Security はこのデータから、セキュリティとコンプライアンスに悪影響を及ぼす 3つの重大なリスク要因を特定しました。

- リスク要因 1: エンドポイントおよびネットワーク・アクセス・セキュリティ アプリケーションの障害
- リスク要因 2: AI エンドポイント導入の波
- リスク要因 3: 重要なパッチ適用が遅れ続ける企業や団体

このレポートは、これらの重要な発見と詳細な分析を共有し、CISO やその他のセキュリティおよびリスクの専門家へのガイダンスを提供します。

- 特定されたリスク要因の存在を確認する方法
- サイバーレジリエンスの定義、サイバーレジリエンスをリスク要因の低減に役立てる方法
- サイバーレジリエンス体制を改善する方法

エンタープライズのトップ・セキュリティ・リスク

管理対象PCのEPPとネットワーク・アクセス・セキュリティ・アプリケーションは、24%の確率でセキュリティポリシーのコンプライアンスを維持できません。

24%

エンタープライズ向けデバイス 92%は AI に対応できておらず、十分なRAMなどの基本要件が不足しています。

92%

74

Windows 10 デバイスの平均パッチ適用期間 (日数)

45

Windows 11 デバイスの平均パッチ適用期間 (日数)

Absolute Security のファームウェア組込み型ソリューションが動作する 500万台以上の Windows 10 および 11 の PC の匿名化されたテレメトリを分析した結果、企業や団体のセキュリティに対するトップリスクが明らかになりました。

イントロダクション

PC の販売数は急増しています。IDC によると、世界の PC の出荷台数は **2028**年までに 2億9,200万台まで増加する可能性があるといいます。パンデミック時に発行された旧式のデバイスを交換する必要性、企業向けAI対応アプリケーションの実行に必要なレベルに処理能力が向上したノートPCへの需要、Windows 11、ハイブリッドワークやリモートワークの本格化など、いくつかの要因がこのトレンドを後押ししています。

企業や団体における Windows のシェアは 68パーセントを占めており、PCは今後も数十年にわたってビジネスツールとして使われ続けるでしょう。CISOをはじめとするセキュリティやリスクの専門家にとって、PCのユビキタス化は、サイバー犯罪者や脅威行為者が悪用する新たな脆弱性をデバイスにもたらすことにつながり、あらゆる業界で攻撃対象領域が拡大されることになります。規制もまた、PCエコノミーにさらなる圧力をかけるでしょう。たとえば、EUでは、環境規制を順守する企業は、新たに安全なPCを導入するだけでなく、すでに使用されている数百万台のデバイスを改修・更新する方法を見つけなければなりません。

現在のPC主導のデジタル・ビジネス・エコシステムで成功を収め、ビジネスや脅威の状況が急速に変化する中でリスクを低減するためには、企業や団体は従来のサイバーセキュリティ戦略からサイバーレジリエンスの推進に移行する必要があります。

2028年までに
PCの出荷台数が
2億9,200万台
に増加する可能性がある

需要促進要因

- パンデミック対応で購入された機器の交換
- AI に必要な処理能力
- WINDOWS 11
- ハイブリッドおよびリモートワーカーの継続的ニーズ

エンタープライズにおける
WINDOWSの
シェアは
68%

セキュリティリスク要因 1

エンドポイントとネットワーク・アクセス・セキュリティ アプリケーションの障害

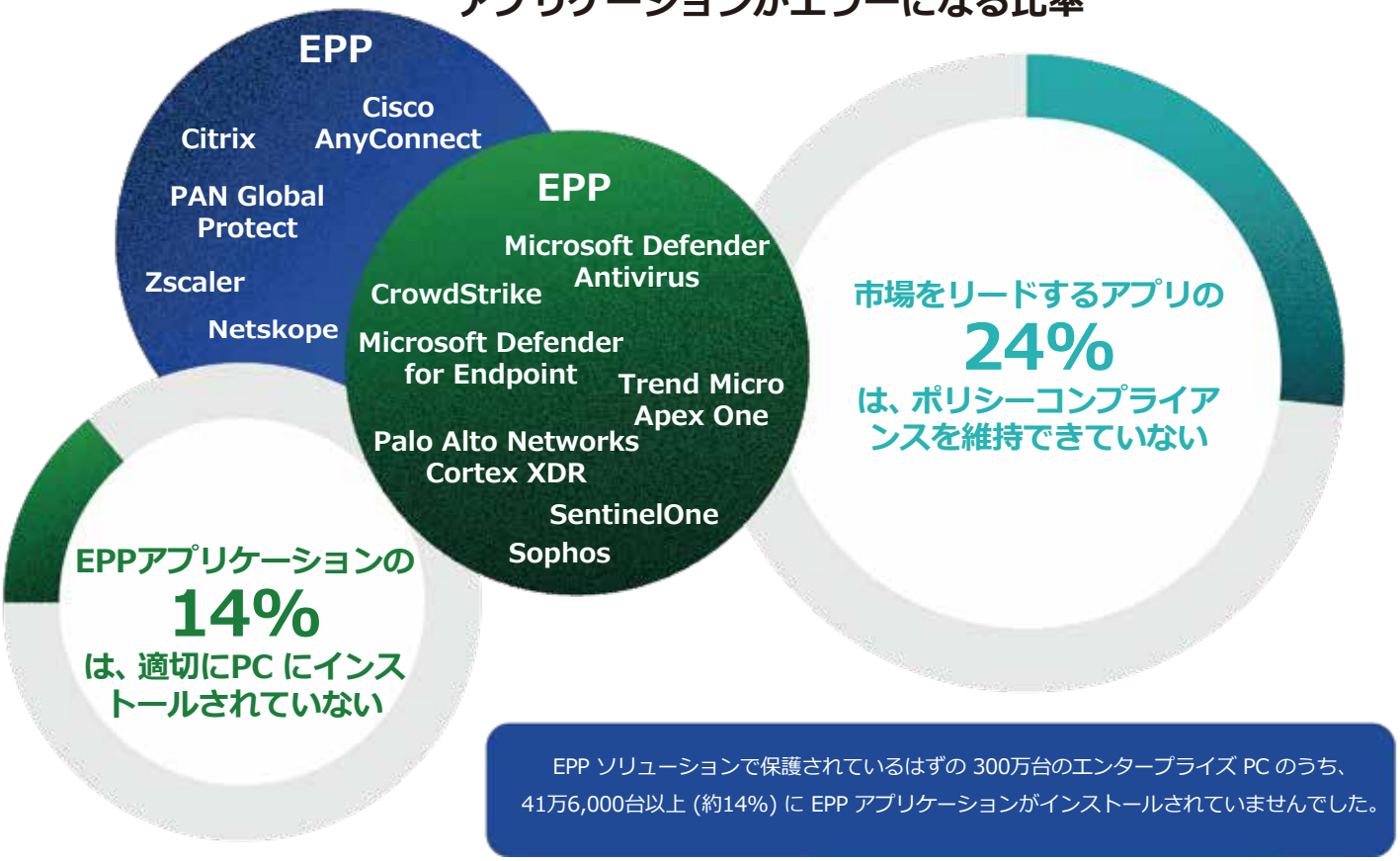
分析結果：デバイスが自動修復技術でサポートされていない場合、EPPとネットワーク・アクセス・セキュリティ・アプリケーションは、管理対象 PC 全体で 24 パーセントの確率でセキュリティポリシーへの準拠を維持できない (EPP には主要な XDR、ネットワーク・アクセス・セキュリティ・アプリケーションには ZTNA が含まれます）。

PC は、現在最もユビキタスなビジネス・コンピューティング・ツールとなっており、Windows デバイスがその 68パーセントを占めています。テレメトリ分析結果によると、デバイスごとに平均して12種類以上のセキュリティ・アプリケーションが使用されており、4種類の基本的なセキュリティポリシーで管理されています。

1. アプリケーションがデバイス上に存在していることを確認
2. アプリケーションが正しいバージョンであることを確認
3. アプリケーションが期待通りに動作していることを確認
4. 申請書が適切に署名され、改ざんされていないことを確認

Absolute Security は、企業や団体がポリシーへのコンプライアンスが維持されている頻度を把握するため、500 万台以上の Windows PCにおいて、主要なエンドポイントおよびネットワーク・アクセス・セキュリティ・コントロールのソリューションを評価しました。

エンドポイントとネットワーク・アクセス・セキュリティ アプリケーションがエラーになる比率



EPP ソリューションで保護されているはずの 300万台のエンタープライズ PC のうち、41万6,000台以上 (約14%) に EPP アプリケーションがインストールされていませんでした。

データによると、これらのアプリケーションは平均して、4種類のセキュリティポリシーに 24%の割合で準拠していません。EPP とネットワーク・セキュリティ・アプリケーション (ZTNA を含む) がモバイルおよびハイブリッド・ネットワーク・エッジにおける防御の第一線であることを考えると、この結果は注目に値します。

セキュリティへのインパクト

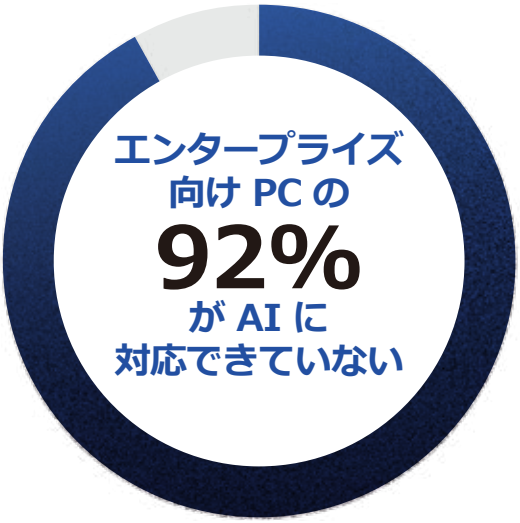
PCのEPPとネットワーク・アクセス・セキュリティ・アプリケーションは、24%の確率でセキュリティ・ポリシーへのコンプライアンスを維持できていません。このギャップにより、PCは障害や侵害、ランサムウェア、その他の脅威にさらされる可能性があります。

対策：CISOをはじめとするセキュリティおよびリスクの専門家は、エンドポイントおよびネットワーク・アクセス・セキュリティ・アプリケーションを可能な限りリアルタイムで監視、レポート、修復できるソリューションを導入する必要があります。アプリケーションに標準装備されている「フェイルセーフ」では、誤動作や侵害されたソフトウェアが自己修復して有効な状態に戻ることができないため、十分でない場合があります。サイバー攻撃、技術的な誤動作、または意図的な改ざんの試行後、アプリケーションの修復と有効な状態への復元を自動化する技術によって、エンドポイントおよびネットワーク・アクセス・セキュリティの制御が強化されます。

セキュリティリスク要因 2
AI エンドポイント導入の波

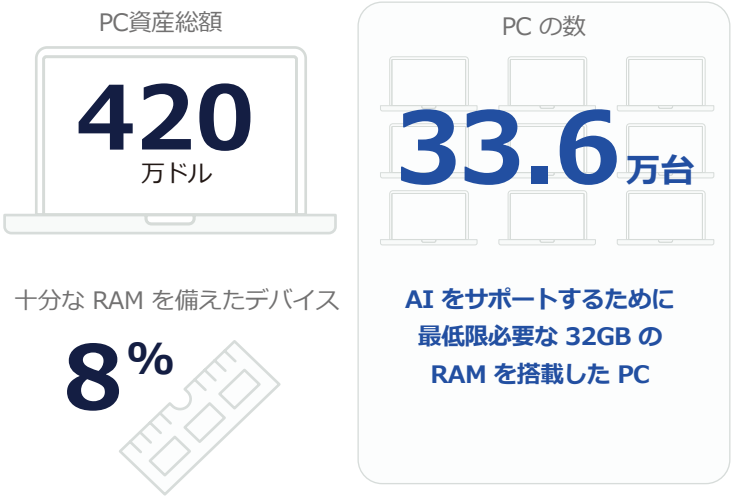
分析結果：エンタープライズ向け PC の 92%はAI に対応できていない。

エンタープライズ向け PC で AI アプリケーションやプロセスを効果的に実行するには、最低 32GBの RAM とスタンドアロン GPU または統合 NPU を搭載する必要があり、世界トップクラスのアナリスト企業はこの基準を標準化するよう顧客にアドバイスしています。現在のエンタープライズ・デバイスのAIベースの準備状況を評価するために、Absolute Security は 400万台以上の Windows マシンを分析しました。その結果、ほとんどのデバイスがAIをサポートするために必要な基本要件を満たしていないことが明らかになりました。IDC が、AI の新機軸をサポートする PC の需要が 5,000万台から 2027年までに 1億6,700万台へと 60%急増すると予測しているのも不思議ではありません。



AI 対応の遅れ

- デバイスの 92% (420万台) で、AI に必要な RAM の容量が不足している



セキュリティへのインパクト

大規模な導入は複雑でリソースを必要とします。AI 対応のデバイスへの巨額の投資は、重要な IT やセキュリティの優先事項から予算や人的リソースを流用する可能性があり、セキュリティやリスクポリシーにギャップを生じさせます。新しいソフトウェアを搭載したデバイスは複雑さを増すだけでなく、パフォーマンスやセキュリティにも影響をおよぼします。前述したとおり、今回の分析で、エンドポイント・セキュリティ・アプリケーションが頻繁に失敗することが判明しています。さらに、重要なエンドポイント脆弱性へのパッチ適用が遅れていることも明らかになっています。
これらの要因やその他の要因を考慮すると、来るべき大規模な AI への対応の波が、膨大なセキュリティとリスクへの取り組みを必要とする理由が容易に理解できます。

対策：AI に対応する PC の大規模な導入に投資する企業や団体は、IT、セキュリティ、リスクの各手順を最大限に効率化するための対策を講じる必要があります。CISO をはじめとするセキュリティとリスクの専門家は、ロールアウトと管理プロセスだけでなく、セキュリティ・アプリケーションの修復と有効な状態への復元も自動化し、脅威に対する最大限の防御を可能にするテクノロジーを備えた AI 対応デバイスの投資を組織に提言すべきです。

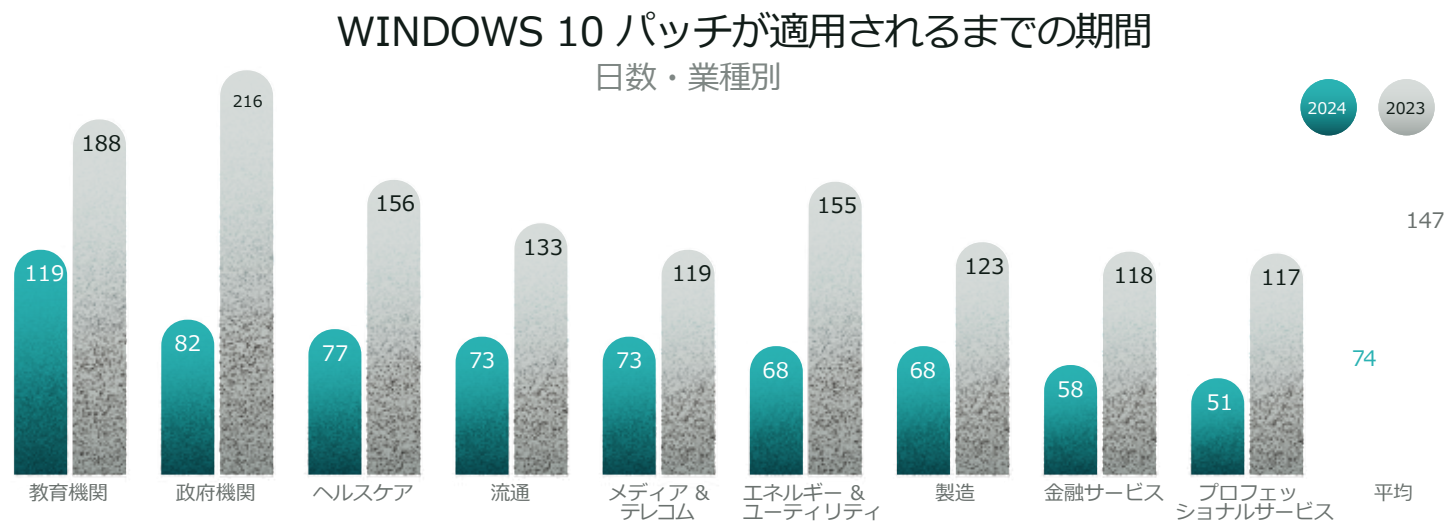
AI データセキュリティの利点

AI がサイバーセキュリティ機能を強化することは間違いありません。同時に、脆弱性や AI を利用した脅威が発生するため、リスクも増大します。データセキュリティに関して言えば、大規模なデータセットと言語モデル処理をローカルで処理できるデバイスは、データをサードパーティのクラウドホストに保存して処理するのではなく、企業や団体が所有する資産に保存するという利点があります。データをより局所的に管理することで、企業や団体はデータの窃取や漏洩のリスクを全体的に低減することができますが、これはデバイスに導入されたセキュリティとリスク管理が適切に機能している場合に限られます。

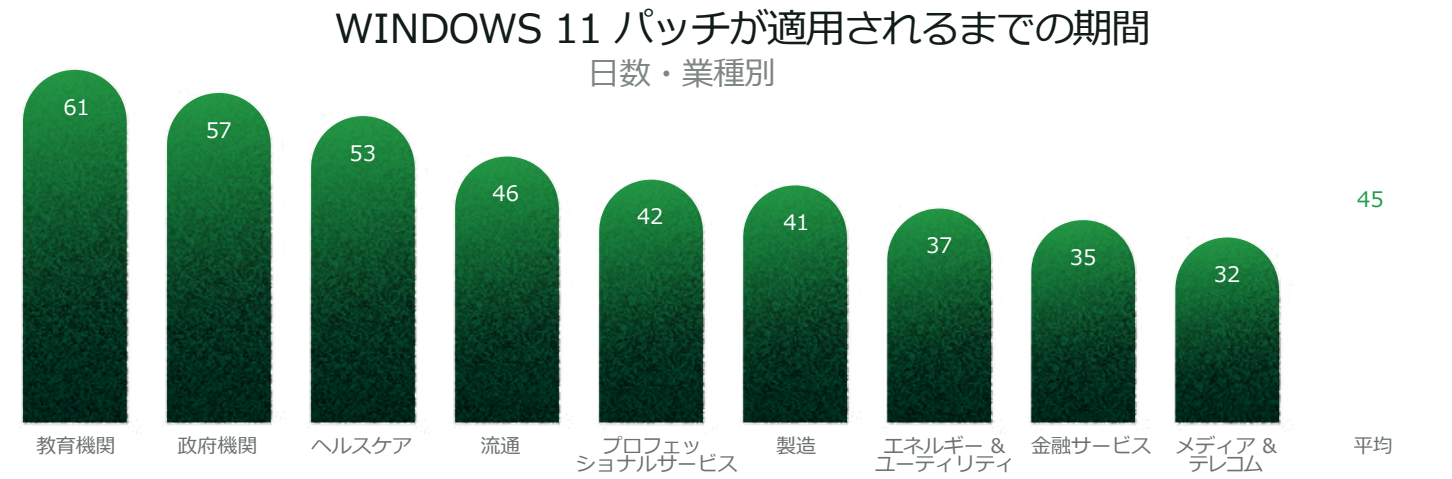
セキュリティリスク要因３
重大な脆弱性へのパッチ適用の遅延

分析結果：多くの企業や団体では重要なパッチの適用が遅延している。

Google の脅威分析グループ (TAG) は、2023年に 97件のゼロデイ脆弱性のエクスプロイトを報告しました。2022年の 62件から 35件増加しています。CVEdetails.comは、2023年に 29,065件の CVE を記録し、2024年には 4月中旬までに既に 8,395件を記録しています。脆弱性が増加しているにもかかわらず、バージョン 10 と 11 を実行している Windows PC のテレメトリ分析によると、Windows 10 環境へのパッチ適用は Windows 11 への適用状況を下回っていることが確認されています。



パッチの適用スケジュールやポリシーは各組織によって設定されており、適用状況は業種によって異なります。Absolute Security の調査によると、パッチの適用に最も長い日数を要しているのは教育機関、次いで政府機関です。パッチ適用に要する日数で他の組織をリードしているのは、金融サービス機関です。



Absolute Security がレジリエンス・インデックスのために Windows 11 デバイスを評価したのは今年が初めてです。Windows 11 にアップグレードされた企業や団体は、Windows 10を現在も管理している組織と比較して改善が見られ、パッチ適用にかかる時間がほぼ半分に短縮されています。私たちは、このトレンドが継続するかどうかを確認するため、Absolute Security は今後数カ月間、この傾向の追跡と報告を続けます。

セキュリティへのインパクト

Service Now が Ponemon Institute に委託したレポートでは、侵害の　60パーセントがパッチ未適用の脆弱性に起因していることが明らかになりました。2023年の共同調査では、ランサムウェア感染を可能にする数十のソフトウェア脆弱性が特定されました。どちらがより正確な見解であるかにかかわらず、未修正の CVE がもたらす結果は、データ漏洩、ランサムウェア攻撃、望ましくないサイバー妨害など、否定できないものです。

対策：CISOをはじめとするセキュリティおよびリスクの専門家は、企業や団体内で影響を受けるすべての資産を特定し、配備されたソフトウェアに影響を及ぼす脆弱性に優先順位をづけ、できるだけ多くのパッチ適用タスクを自動化プラットフォームに割り当てることができるソリューションを導入する必要があります。標準的な脆弱性管理プラットフォームでは、たとえパッチが完全に適用されていたとしても、資産がセキュリティポリシーに準拠しているかどうか、または期待どおりに機能しているかどうかを検証できない場合があります。このようなソリューションが追跡できないエラーを回避するには、ソフトウェアとハードウェア資産の可視性を拡大するレイヤーを追加し、それらが必要に応じて動作していることを確認する必要があります。調査によると、評価対象となった 300 万台の PC のうち、41 万 6,000 台以上 (約 14%) に EPP アプリケーションがインストールされていませんでした。

結論

サイバーレジリエンスは比較的新しい概念です。これを主流に押し上げつつある要因はいくつかあります。たとえば、ホワイトハウスがソフトウェアのサプライチェーンにサイバーレジリエンスを組み込むよう指示したこと、高度な脅威を防御するには従来の検知・防御戦略では不十分であることが認識されたこと、主要な業界団体がサイバーレジリエンスを新たなトレンドであると認識したことなどです。

企業や団体のセキュリティとリスクに影響を及ぼす要因は無数にありますが、サイバーレジリエンス機能によってそれを軽減することができます。本レポートでは、実データを活用して、企業や団体全体に共通するいくつかの要因を特定しました。この調査結果は、セキュリティ管理者に、自社のサイバーレジリエンス戦略の実施に着手するための指針を提供するものです。

Absolute Security サイバーレジリエンス・リスク・インデックス 2024 調査方法

このレポートは、当社のお客様のデバイスのうち、Windows 10および11が動作する507万44台のPCの匿名化されたテレメトリを分析したものです。

Absolute Security は、永続的なネットワーク接続を実現するためのソリューション (「切れない」ネットワーク) およびエンドポイントのセキュリティを強固にするソリューション (リモートロック／データ削除) を提供しています。不健全な状態にあるセキュリティアプリやビジネスアプリを自動で回復させるレジリエンス機能 (「消えない」エンドポイント管理) を持つAbsoluteの製品は、世界中の 28社以上の主要メーカーのデバイスに工場出荷時より組み込まれています (累計6億台以上)。Absolute Security 製品をお使いのお客様は世界中で約21,000社を超え、ユーザー数は1,400万以上になります。Absolute Security のサイバーレジリエンス・プラットフォームを適用することで、世界のどこからでも安全かつシームレスに企業や団体のネットワークに接続できるようになります。万が一、悪意のある第三者から攻撃を受けた場合でも、迅速に復旧することができます。Absolute Security は、ZTNA、エンドポイントセキュリティ、SSE、ファームウェア組み込み型パーシステンス、ASCA、ゼロトラストプラットフォームなど、複数のテクノロジーカテゴリーで受賞歴を持ちます。

デモおよびお問い合わせはこちら

ABT-Resilience-Index-Report-JP-041724_CW