ABSOLUTE®

2023 RESILIENCE INDEX

デジタルエンタープライズのセキュリティ認識と現実とのギャップ

サマリー

Absolute は、エンドポイントレジリエンスのトレンドに関する定期調査として、北米、欧州、APAC の顧客組織で活動する 1,400 万台の Absolute 対応デバイスの匿名化データ、および信頼できる第三者からのデータおよび情報を分析しました。今回の調査は、4 年目となります。

このレポートでは、組織の複雑性・継続性・コンプライアンス態勢を評価することで、リモートワーク・モデルにおけるレジリエンスの状態を調査しています。一般に、より多くのセキュリティソリューションを導入すれば、脅威に対する保護が強化されると長年信じられてきましたが、それは真実であるとは言えないことが、調査結果から明らかになっています。

そのため、多くの組織は従業員を企業のネットワークやリソースに安全に接続する方法を探すようになりました。その中で、セキュリティとサイバーレジリエンスを両立させ、従業員がリスクにさらされても安心して仕事に取り組めるようにする、新しい Comply to Connect (安心できるように接続する) の流れが生まれつつあります。

Resilience Index 2023 では、以下を目的としています。

1. 環境の複雑さを評価し、サイバーレジリエンス態勢を評価する
2. 今日必要とされるコネクティビティとコンプライアンス慣行を理解する
3. Absolute が既存のセキュリティをどのように機能させるかを把握する

リモート / ハイブリッド ワーク環境の セキュリティを確保

組織や従業員がパンデミック後の規範に適応していく中で、あることが明らかになりました。ハイブリッドワークは今後も続くものであり、一部の従業員に与えられる特典ではなく、従業員の期待に応える働き方であるということです。Gartner によると [1]、2023 年末には、ナレッジワーカーの 48% がハイブリッドまたは完全リモートで働くようになり (2019 年の 27% から増加)、そのうちの 39% はハイブリッドワークである (2020 年の 12% から増加) と言われています。

1. Gartner; Forecast Analysis: Knowledge Employees, Hybrid, Fully Remote and On-Site Work Styles, Worldwide, 2023 年 1 月

WINDOWS 10
エンタープライズデバイスの多くを占める

800+
ビルド/パッチ

14
バージョン

OSバージョン&パッチ

煩雑な環境

「どこでも仕事できる」新しいモデルは、IT 担当者やセキュリティチームに負担をかけ、かつてない複雑さを生み出しています。従業員が組織内外のネットワークを行き来することで、可視性と制御の問題が生じています。そのことが、エンドユーザーの問題を診断・解決し、サイバーセキュリティのリスクを最小限に抑制するための IT/ セキュリティチームの能力に影響を及ぼしています。加えて、ネットワーク、ハードウェア、OS のバージョン、パッチなど、さまざまなものに対応する必要があります。

一例として、80%以上の端末がマイクロソフト社の OS「Windows(R)」を採用しており、その大多数が「Windows 10」であることを考えてみましょう。一見、管理は簡単そうに思えます。しかし現実には、IT 担当者は、14 種類の異なるバージョンと 800 種類以上のビルドとパッチが存在する従業員・エンドポイントを最新の状態に保つことに苦労しています。

デバイス

> 80% WINDOWS DEVICES
大規模組織

< 20% CHROMEBOOKS
大規模組織

出展：Absolute デバイス・テレメトリ・データ

デバイスモビリティの向上が、新たな脆弱性を生む

4

エンタープライズデバイスが組織リソースにアクセスする場所の数

遠隔地の従業員や複数の拠点が、さらにこの複雑なレベルに拍車をかけています。リモートの従業員は、組織が所有または管理していないネットワーク上で重要な作業を行っており、組織のリスクエクスポージャーを劇的に増加させています。また、ユーザーが同じ場所にいても、デバイスやネットワークを頻繁に切り替わることがあります。たとえば、お気に入りのコーヒーショップの Wi-Fi に接続したノート PC から、通信事業者の携帯電話ネットワークに接続したモバイルデバイスに切り替え、帰宅するまでの間にオンラインミーティングを行うなど、ユーザーはライフサイクルに合わせて生産性を向上させる行動をとることがあります。そのことを考えると、Absolute ユーザーのエンタープライズ向けデバイスの平均ロケーション数が前年比で 15%増加し、2023 年 2 月にはデバイス 1 台あたり平均 4 箇所に上ったことは驚くべきことではありません。

15%

エンタープライズ向けデバイスのロケーションが前年比で 15% 増加

出展：Absolute デバイス・テレメトリ・データ

組織のデバイスにインストールされているアプリの数（平均値）

67 種類

生産性向上、セキュリティ、業務に関係ないアプリ等を含む

組織のデバイスの **10%** が

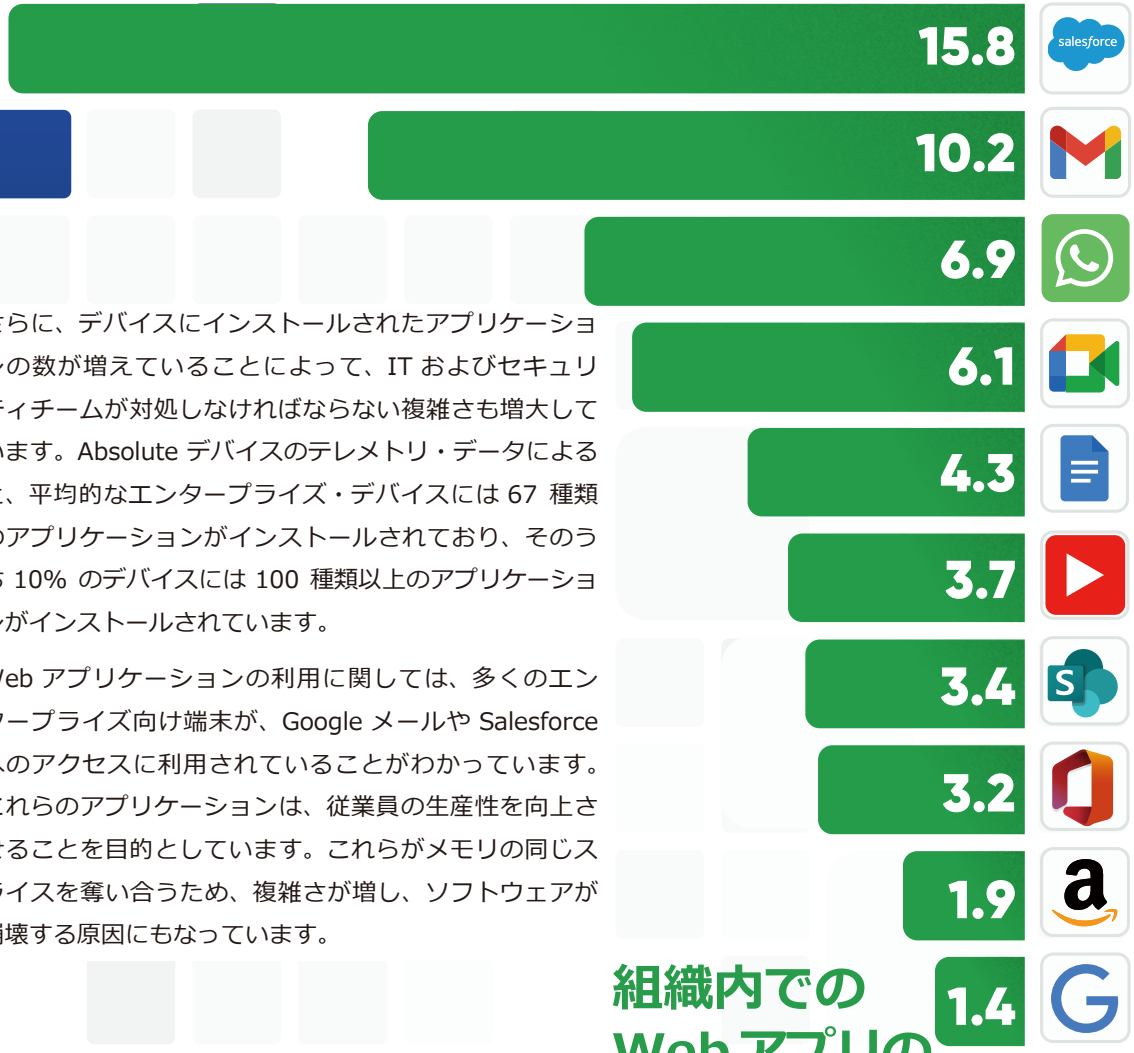
100 種類

以上のアプリをインストール

さらに、デバイスにインストールされたアプリケーションの数が増えていることによって、IT およびセキュリティチームが対処しなければならない複雑さも増大しています。Absolute デバイスのテレメトリ・データによると、平均的なエンタープライズ・デバイスには 67 種類のアプリケーションがインストールされており、そのうち 10% のデバイスには 100 種類以上のアプリケーションがインストールされています。

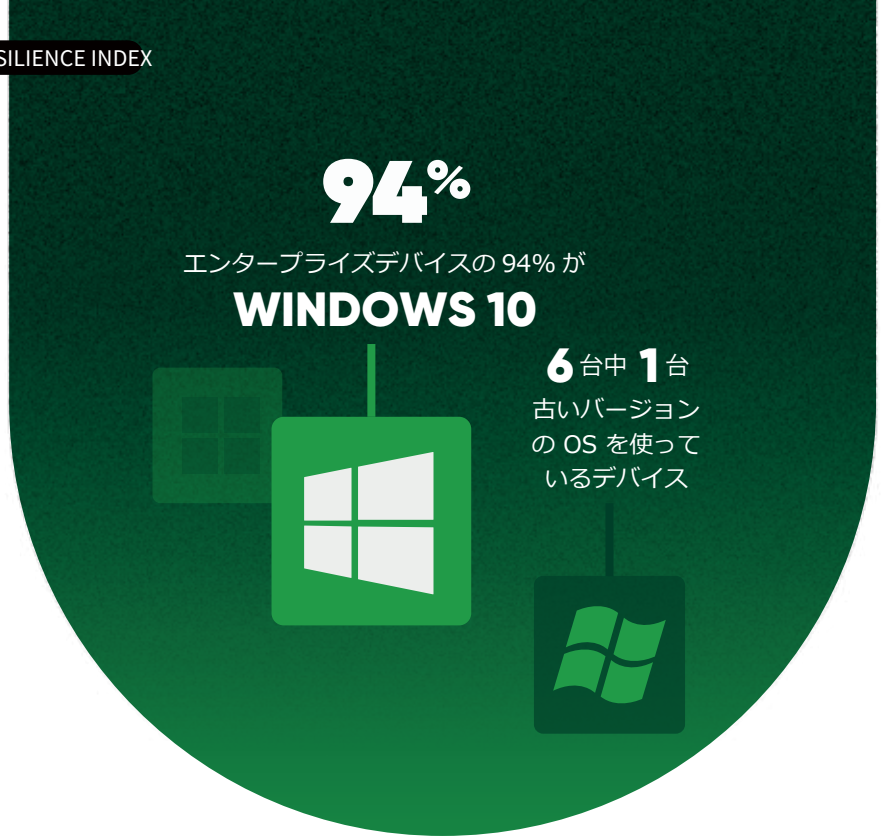
Web アプリケーションの利用に関しては、多くのエンタープライズ向け端末が、Google メールや Salesforce へのアクセスに利用されていることがわかっています。これらのアプリケーションは、従業員の生産性を向上させることを目的としています。これらがメモリの同じスライスを奪い合うため、複雑さが増し、ソフトウェアが崩壊する原因にもなっています。

組織内での Web アプリの使用状況



出展：
Absolute デバイス・テレメトリ・データ

エンタープライズデバイスが抱える「複雑性」を象徴



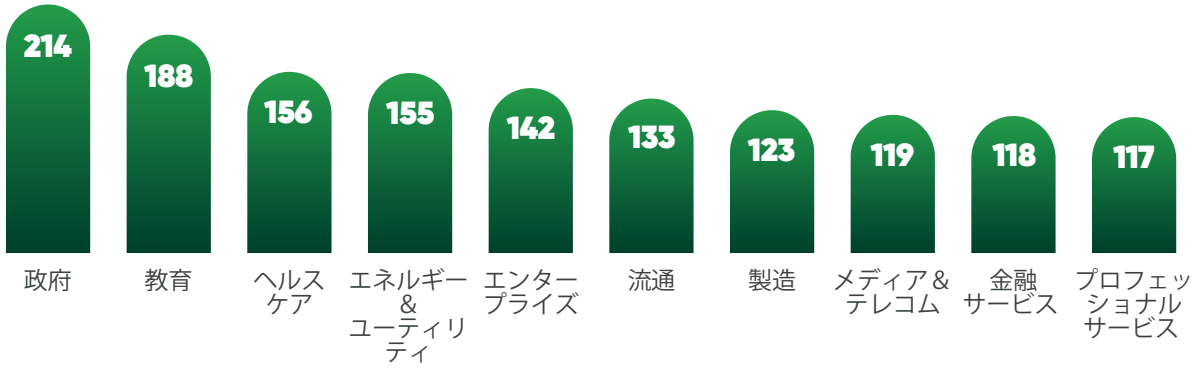
エンタープライズ向けデバイスにインストールされているアプリケーションの数は非常に多く、OS のバージョンやビルドもさまざまです。そのため、IT チームやセキュリティチームがこれらのアプリケーションを保守したり、パッチを当てたりする作業は非常に煩雑になります。このような状況は、既知の脆弱性への曝露を抑制する能力に悪影響を及ぼします。

これは、IT 部門が 50 種類から 100 種類ものアプリケーションをプロアクティブに管理しようとしていることを想定しています。もっと可能性が高いのは、管理しているのはもっと小さなサブセットです。ほかにも、実際には管理もパッチも適用されていないが、バックグラウンドでまだ動いている可能性のある「シャドーアプリケーション」も存在します。このため、組織はさらなるリスクにさらされ、システムリソースはさらに消費されることになります。

WINDOWS 10 パッチの適用時期

業種別 パッチが適用されるまでの日数

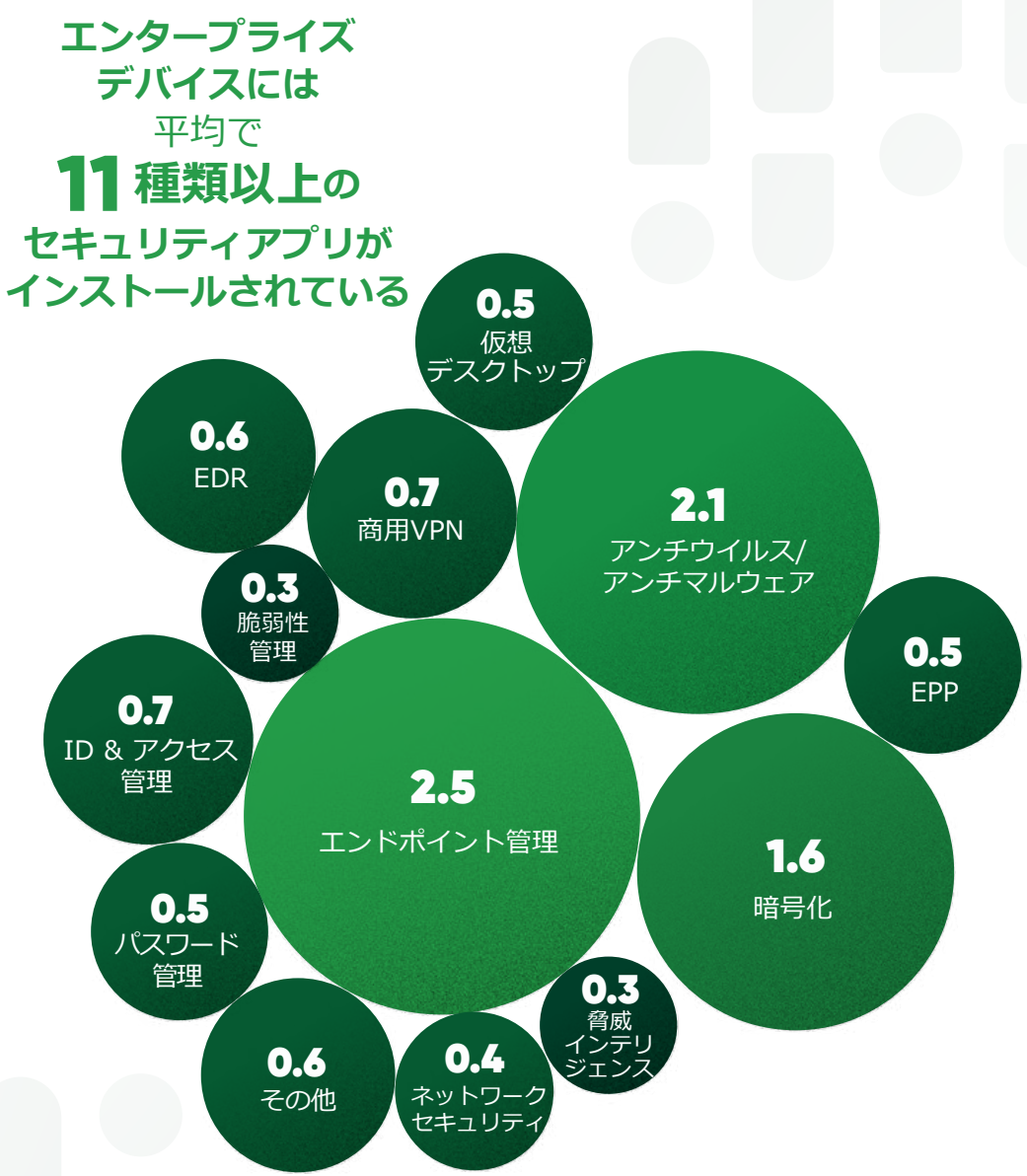
最も期間が長いのは 政府と教育



組織規模別 パッチが適用されるまでの日数

最も期間が長いのは 超大規模組織

出展：Absolute デバイス・テレメトリ・データ



セキュリティに対する誤った考え方

一般に、IT やセキュリティ技術に費用をかければかけるほど、セキュリティ態勢が強化されるという考えが蔓延しがちです。その考えに基づいて、多くの組織は、新たな課題や脅威に対応するために、より多くのソリューションを購入します。エンドポイントセキュリティだけで年間数百億円も費やしているのです。その結果、平均的な業務用ノートパソコンにインストールされているセキュリティアプリケーションが、11 種類以上に上っているのも当然といえます。

注目すべきは、多くの業界標準 (ISO/IEC 27001、NIST CSF、PCI DSS、GDPR など) や政府規制 (HIPAA、HITECH、FISMA など) で必須のセキュリティ管理とされているエンドポイント管理、アンチウイルス、アンチマルウェア、暗号化に対応するために、エンタープライズ向けデバイスには平均して複数のセキュリティアプリケーションがインストールされていることです。このことは、多くの組織が、デバイス群全体のソフトウェア資産に対するインサイト (洞察) が不足していること、必要以上のソフトウェアを実行していること、あるいは単に多くのツールを導入すればするほど安全であると信じていることを示しています。

出展：Absolute デバイス・テレメトリ・データ

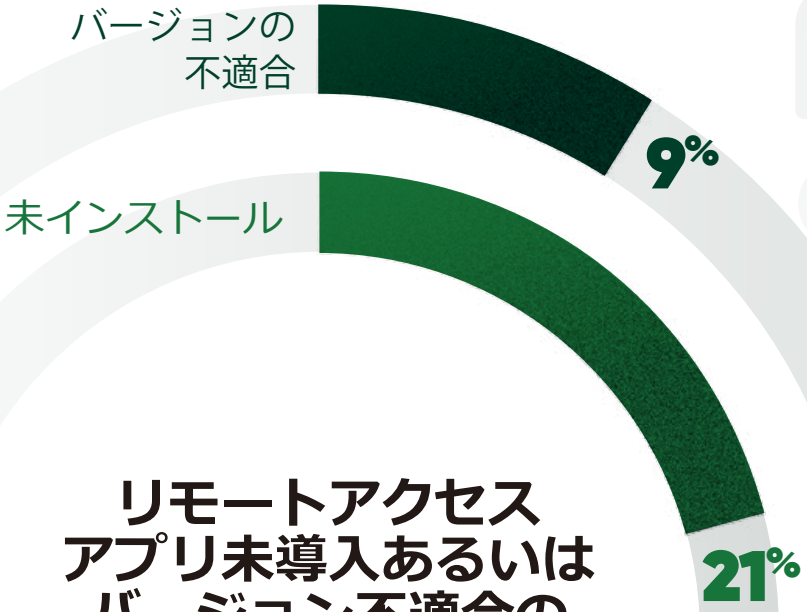
セキュリティアプリケーションの有効性は千差万別

残念ながら、目に見えないものを確保し、その有効性を確保することはできません。組織のセキュリティ態勢は、それを支えるセキュリティ管理によってのみ強化されます。エンドポイントに配置されたすべてのセキュリティコントロールは、着実に実行されてその役割を果たすことができていない限り、潜在的な脆弱性になってしまいます。一般的な腐敗、意図しない削除、悪意のある行為はすべて、セキュリティアプリケーションやエンドポイント管理ツールの完全性と有効性に影響を与えます。

アプリケーションの共存を保証するのは、ソリューションプロバイダー自身が担うべきだという意見もあるかもしれません。しかし、ツールの数、それぞれのバージョンやビルドの数、OS のバージョンやビルドの数などに基づく順列の数を考えると、どのソリューションプロバイダーでも無理があるのが現実です。また、エンドユーザーを保護するために、悪意のある者による脅威を常に把握する必要があることも事実です。

エンドポイントプロテクションプラットフォーム (EPP)、エンドポイント検知応答 (EDR)、アンチウイルスなどのセキュリティツールは、攻撃を防御するために不可欠であり、したがって常に稼働し、最新の状態に保つべきであるというのが、IT 管理者やセキュリティ実務者の意見です。Absolute のデータでは、25 ～ 30%のデバイスにおいて、セキュリティ制御が不健全であることがわかっています。

出展：Absolute デバイス・テレメトリ・データ

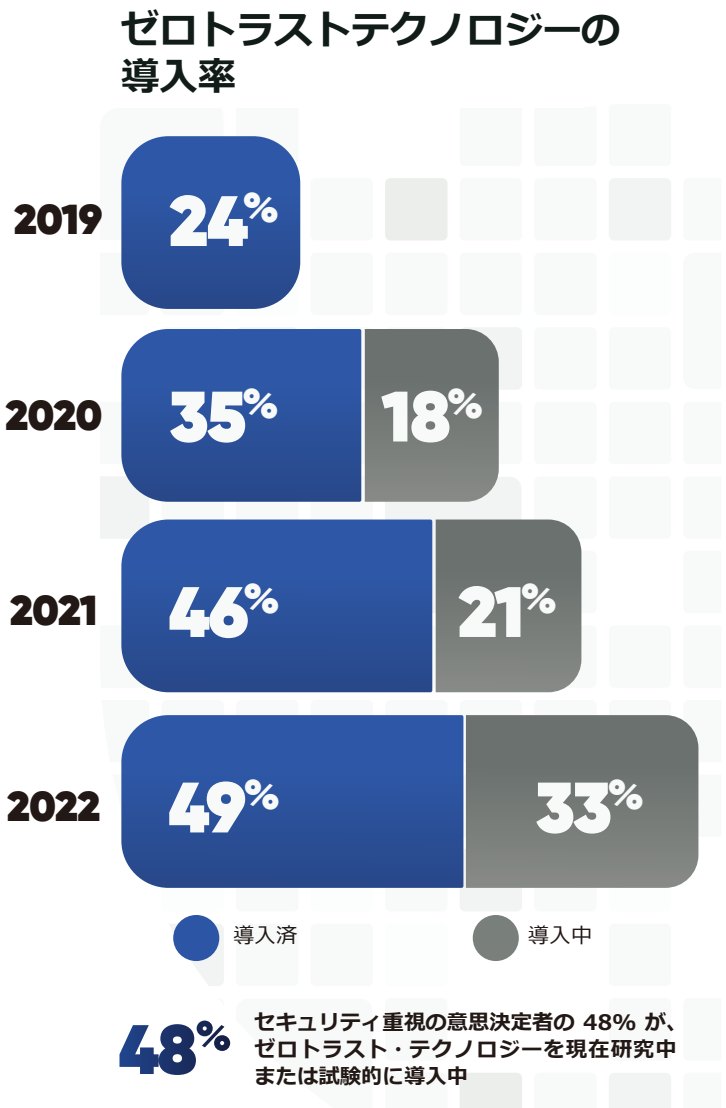


リモートアクセスアプリ未導入あるいはバージョン不適合の問題があるデバイスの比率

出展：Absolute デバイス・テレメトリ・データ

リモートアクセスや ZTNA (Zero Trust Network Access) アプリケーションは、組織にとって生命線となるもので、忘れてはならない存在です。モバイルワーカーは、常に安全であると同時に、必要なときに組織のリソースに摩擦なくアクセスできなければなりません。それが、これらのテクノロジーがエンドポイントと組織ネットワークの接点となっている理由であり、組織による採用が進んでいる理由です。つまり、これらのツールの整合性が改ざんされないようにすることが不可欠なのです。

しかし、Absolute のデータによると、これらの重要なツールは、30% 以上のデバイスで、インストールされていないか、必要なバージョンに達していないため、組織は不必要なリスクにさらされています。



サイバーレジリエンス：増大する脅威に対処するための新たな戦略

前述の調査結果の意味を考慮すると、組織が侵害に遭うのはもはや「もし侵害に遭ったら」ではなく「いつ侵害に遭うか」の問題であることがわかります。つまり、攻撃を防ぐことだけに注力するのではなく、攻撃が成功して侵害されてしまった場合の影響を軽減するための計画を立てることが重要なのです。そのため、多くの先進的な組織は、サイバーレジリエンスと呼ばれる、今日のサイバー脅威の増大に対処するための新しい戦略を採用しています。

最初のステップは「誰も信用しない」こと

クラウドの導入が加速し、どこでも仕事ができるようになったことで、一般的な境界の防御力が低下し、組織はかつてないほど脆弱な状態になっています。組織を守るための最初のステップは、サイバーレジリエンスと同時に、ゼロトラスト原則を適用することです。

Forrester は、ゼロトラストを、アプリケーションやデータへのアクセスをデフォルトで拒否する情報セキュリティモデルとして定義しています。脅威は、ユーザーとそのデバイスにまたがる継続的でコンテキストに基づいたリスクベースの検証によって知らされたポリシーに基づいて、ネットワークとワークロードへのアクセスのみを許可することによって阻止されます。ゼロトラストは、「すべてのエンティティはデフォルトで信頼されない」「最小限の特権アクセスを強制する」「包括的なセキュリティ監視を実施する」という 3 つの基本原則を提唱しています。

ゼロトラストのアーキテクチャとテクノロジーは、組織のセキュリティに着実に浸透しており、旧来の境界線中心のアプローチに取って代わろうとしています。Foundry (旧 IDG Communications 社) の 2022 年セキュリティ優先度調査では、回答者の 32%がゼロトラスト技術を研究していると答え、16%が「試験的に導入している」と答えています。[2]

2. 出展：Foundry (旧 IDG Communications)、Security Priority Study、2020 ～ 2022 年

今日の環境では、攻撃者は既にネットワーク内に存在していると想定すべきです...

ZTNA、ゼロトラストへの論理的出発点

ゼロトラストの導入を、どこから始めるかを決めるのは難しいことですが、サイバー敵対者を理解し、その搾取の戦術、技術、手順 (TTP) を評価することが指針になるはずです。このコンテキストでは、現代のゼロトラストの柱の定義は、ネットワークを超えて、今日の拡大し続ける攻撃表面を包含するということを理解することが重要です。

攻撃者が機密データにアクセスするための最も簡単な方法は、ユーザーの ID を侵害することです。実際、IDSA (Identity Defined Security Alliance) の調査によると、クレデンシャルに基づくデータ漏洩はどこにでもあり (調査回答者の 94%が ID 関連の攻撃を経験)、かつ非常に予防しやすい (99%)[3] ことが明らかにされています。このような背景から、ZTNA は、組織リソースへのアクセスを許可する前に、ユーザー名 / パスワードに依存するのではなく、時間帯、地理的位置、デバイスのセキュリティ姿勢などのコンテキスト要因を重視します。

しかし、人為的なミスや悪意ある行為、腐敗した安全でないソフトウェアが、ゼロトラスト技術の有効性を阻害することも少なくありません。そのため、NIST (米国国立標準技術研究所) は、自己修復型あるいはレジリエントなサイバーセキュリティ・システムの利用を推奨しています。

自己修復型サイバーセキュリティ・システムを最終的に差別化するのは、ヒューマンエラー、腐敗、ソフトウェアの衝突、悪意ある行為といった、保護するために構築されたのと同じ要因を防ぐ能力が相対的に高いかどうかです。結局は、単なるソフトウェアのひとつに過ぎないのです。そのため、敵対的な外的要因に直面しても耐えうるソリューションを選択することが重要です。

このようなハードニングの状態を実現するためには、自己修復機能をエンドポイントのファームウェアに組み込み、意図的または非意図的な操作から保護する必要があります。

3 Identity Defined Security Alliance (IDSA), Identity Security: A Work In Progress

ハイブリッド人材を確保するための サイバーレジリエンスとは？

ゼロトラストの原則が確立された後でも、組織は最悪のシナリオに備える必要があるため、防御的な対策とサイバーレジリエンスのバランスをとる必要があります。これは、MITRE[4]、NIST、世界的なアナリスト企業である Gartner、そして野心的な国家サイバーセキュリティ戦略でサイバーレジリエンスを求める米国ホワイトハウスの多くの提言に反映されています。ホワイトハウスの戦略は、市場原理がサイバー犯罪や国家による攻撃から国家の安全を守ることに失敗したという、米国政府内で広く信じられている信念を反映しています。

米国のサイバーセキュリティおよびインフラストラクチャ・セキュリティ庁の長官が、先日以下の情報を引用していました。「今日、既知の脆弱性にパッチを当てなかったためにセキュリティ侵害を起こした組織はたびたび非難されますがが、そもそも多くのパッチを必要とする技術を製造したメーカーはどうなのでしょうか。」[5] 多くの人は、サイバーレジリエンスを維持するための責任は、チャレンジに踏み出す必要のあるベンダーに転嫁されるべきだという意味だと受け止めていました。

MITRE によると、サイバーレジリエンス (またはサイバー回復力) とは、サイバーリソースに対する悪条件、ストレス、攻撃、侵害を予測し、それに耐え、回復し、適応する能力のことを示します。サイバーレジリエンスの必要性は、システム、データ、ネットワークを侵害から守るためには従来のセキュリティ対策ではもはや不十分である、という認識の高まりから生じています。サイバーレジリエンスの目的は、サイバー上の有害な事象を確実に回避することです。意図的か否かにかかわらず、組織の業務運営の機密性、完全性、可用性に悪影響をおよぼしません。

4 MITRE, Cyber Resiliency Overview, 2020 年 1 月

5 Cyberscoop; CISA director urges tech sector to stop shipping unsafe products, 2023 年 2 月 27 日

> より良いコンプライアンスと、
> 複雑な状況下でのより優れた
> 継続性を提供します。

Christy Wyatt
Absolute Software　社長 兼 CEO

Absolute Software: セキュリティ機能の着実な動作を支援

Absolute は、エンドポイントおよびネットワークのレジリエンスのパイオニアとして知られており、その Persistence® 技術は、長年にわたり世界の主要なシステムメーカー (Dell、Lenovo、HP、Microsoft など) に採用され、数百万人のユーザーにサイバーレジリエンスを提供しています。

Absolute は 6 億台以上のデバイスのファームウェアに組み込まれており、エンドポイント、アプリケーション、ネットワーク接続の可視化と制御を可能にします。独自の自己復活機能を活用することで、デバイス、データ、ユーザーを保護し、重要なセキュリティコントロールが最大の効果を発揮することを保証すると同時に、最適なリモートおよびモバイルユーザー・エクスペリエンスを実現することができます。

このレポートの冒頭でお伝えしたように、何百万台ものアクティブなデバイスのファームウェアにおける Absolute 独自のポジションは、「Absolute Application Resilience」がいかにアプリケーションの健全性を監視する能力を提供するかを示しています。Absolute Application Resilience カタログに掲載されているサードパーティ製アプリケーションが不健全になっている場合の修復や再インストールを自動的に行い、健全な動作に回復させることができます。

最終的には、組織のコンプライアンス態勢を強化し、安全で信頼性の高いネットワークアクセスを保証し、従業員がリスクにさらされても自信を持って仕事に取り掛かることができ、仕事を続けることができるようにすることが重要です。

Absolute Application Resilience を採用すれば、IT 担当者が介在しなくても、アプリケーションの健全性スコアが 50% 未満から 100% 近くにまで上昇することが確認されています。セキュリティのアップタイムを改善することは、サイバーリスクとサイバーレジリエンスのギャップを埋めることを意味します。

Absolute Application Resilience を使用すると、IT 部門が関与しなくても自動的に、初期アプリの健全性スコア 50% 未満から、100% 近くにまで飛躍的に向上させることができます。

セキュリティのアップタイムを改善することは、サイバーリスクとサイバーレジリエンスの間のギャップを埋めることを意味します。

サイバーレジリエンスとアプリケーションレジリエンスの力

IT 担当者やセキュリティの専門家には周知のことですが、サイバー攻撃の連鎖のフロントエンドでリスク・エクスポージャーを最小化するために必要なツールは多くはありません。EPP、EDR、そして、リモートアクセスソリューションです。これらのツールの助けを借りなければ、組織は本来の機能性と運用性を維持することはできません。また、単に防御力を確保するだけでなく、攻撃された場合の復旧作業においても同じツールを活用することが重要です。これらの活動は後回しにされ、見過ごされがちです。しかし、ここではセキュリティの効能が大きな役割を果たします。

Application Resilience の有効性を示すために、Absolute は、業界レポートでリーダーとして挙げられ、Absolute のお客様も使用している EPP/EDR とリモートアクセスのトップセキュリティベンダーのアプリケーションヘルスを評価しました。対象となったのは、Cisco、Citrix、CrowdStrike、Microsoft、Netskope、Palo Alto Networks、SentinelOne、Sophos、Trend Micro、および Zscaler です。そして、Application Resilience ポリシーを適用した後のアプリケーションの健全性を比較しました。以下の結果は、匿名化されており、ランダムに表示されています。

	レジリエンスのないアプリ 健全なデバイスの比率*	レジリエンスのあるアプリ 健全なデバイスの比率*	改善値 パーセンテージのアップ値
EPP / EDR			
A 社	95%	**96%**	1%
B 社	70%	**94%**	24%
C 社	47%	**99%**	52%
D 社	49%	**100%**	51%
E 社	89%	**93%**	4%
リモートアクセス			
F 社	75%	**90%**	15%
G 社	73%	**93%**	20%
H 社	85%	**97%**	12%
I 社	53%	**98%**	45%
J 社	76%	**99%**	23%

* アプリの健全性とは、アプリがまったくインストールされていないか、組織が望むバージョンレベルでインストールされているか、アプリが意図したとおりに機能するために必要なサービスが実行されているか、その他多くの条件を表すものです。

Absolute で、IT とセキュリティの複雑化に直面するサイバーレジリエンスを強化

Absolute は、コラボレーション、テクノロジー、セキュリティの各リソースをファームウェアから独自に防御・保護し、先進の組織が求めるパフォーマンスの俊敏性と運用継続性を実現します。デバイスに組み込まれた Absolute Persistence テクノロジーを活用し、Absolute Application Resilience による自己復活機能を拡張することで、組織とセキュリティベンダーは、アプリケーションの有効性を最適化し、セキュリティとコンプライアンスの態勢を強化できます。Absolute は、デジタルの混乱に対処し、モバイルのユーザーエクスペリエンスを変革します。Absolute に守られた従業員はリスクにさらされようとも自信を持って仕事に取り組み、仕事を続けることができます。

レポートメソドロジー

北米、欧州、APAC の顧客組織において、2023 年 2 月から 4 月までの期間にアクティブだった 1,400 万台のアブソルート対応デバイスの匿名化データ、および信頼できる第三者ソースからのデータおよび情報を分析。

Enterprise Resilience インデックス

組織は、複雑性・コンプライアンス・継続性という 3 つのレンズを通して、自身のサイバーレジリエンスを評価することができます。

複雑性

アプリケーションの健全性に焦点を当て、エンドポイントコントロールの数、デバイスとユーザーの数、OS プラットフォームの数などを含む

以下の質問をすることで、複雑性の状態をより詳しく知ることができます。

1. パッチ適用が遅れている OS 別端末の割合は？
2. 機器 1 台あたりのセキュリティコントロールの数は？
3. アンチウイルス / アンチマルウェアと暗号化アプリの最適な組み合わせでテスト / 使用しているか？

コンプライアンス

リスクと暗号化を重視したスコアカード

以下の質問をすることで、コンプライアンス状態をより詳しく知ることができます。

1. 機密データは、転送中や移動中を含むすべてのエンドポイントにおいて暗号化されているか？
2. セキュリティ管理の有効性について、いつでもインサイトを把握できるようになっているか？
3. 組織が支給したすべてのデバイスがどこにあり、機密データが含まれているかどうか、いつでも把握できているか？

継続性

モビリティ、アプリの健全性、可用性を含む

以下の質問をすることで、継続の状態をより詳しく知ることができます。

1. SLA を実施できるような、ネットワークのカバレッジギャップや接続品質に関する知見はあるか？
2. メールシステムに頼らず、エンドユーザーとコミュニケーションをとる方法はあるか？
3. ミッションクリティカルなアプリケーションの修復や再インストールを自動化して攻撃を防いだり、復旧作業を支援したりする方法はあるか？

ABSOLUTE®

Absolute Software は、自動復活するインテリジェントなセキュリティソリューションを提供する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。

G2 は、約 2 万社の顧客から信頼を得ている Absolute を、2023 年春の Grid® Report においてエンドポイント管理部門で 13 四半期連続、Zero Trust Networking 部門で 3 四半期連続で「リーダー」として認定しています。

お問合せまたは
デモのお申込みはこちら

Nasdaq | ABST　TSX | ABST

ABST-ResilienceIndex-042123-B-JP