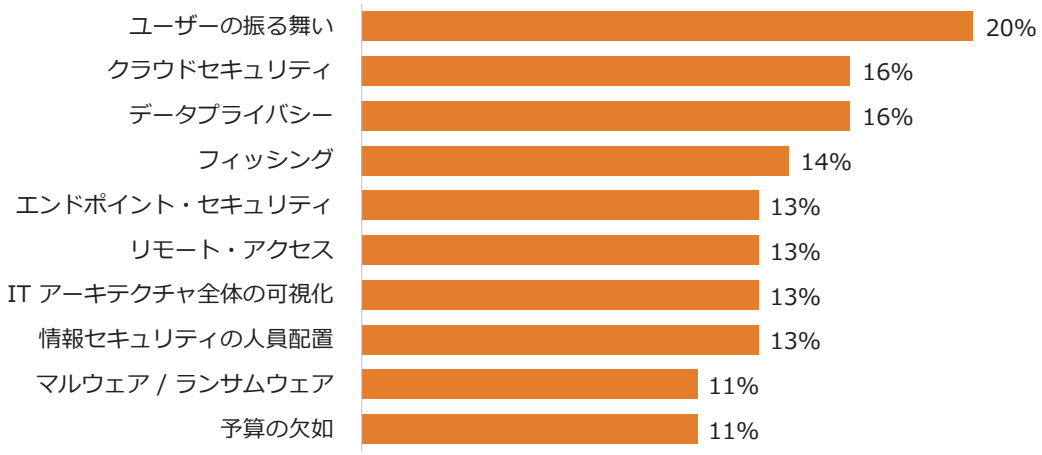
レジリエント・ゼロトラスト機能の構築

451 Research の見解

組織は、今日直面している多くのセキュリティ課題を、ゼロトラストの効果的なアプローチをとり、レジリエンス (回復力) 機能を提供することによって解決することができます。しかし、多くの場合、導入したゼロトラスト環境のレジリエンスが十分に考慮されず、ネットワーク・アクセスとデバイス・セキュリティが独立して処理されています。このような状況は、セキュリティ運用を複雑化させ、従業員の生産性にも影響を及ぼしかねません。ネットワーク・アクセスとデバイス・セキュリティが統合されれば、451 Research が最近行った調査で情報セキュリティの専門家が指摘したセキュリティ課題上位 10 項目のうち 6 項目に対処することができます。

ゼロトラストは広義の用語であり、その意図は明確であっても、詳細はあまり明確ではありません。たとえば、ゼロトラスト・アーキテクチャとゼロトラスト・ネットワークアクセス (ZTNA) は、しばしば混同されます。ZTNA はゼロトラスト・セキュリティのアプローチに必要な要素ですが、ZTNA 単独ではゼロトラストの目標を達成するのに十分ではなく、統合されたアプローチの一部に位置づけられなければなりません。完全なゼロトラスト・アーキテクチャの基盤を構築するには、運用時だけでなく、あらゆるインシデントからの復旧時にも頼りになる弾力性のある機能を構築することが必要です。

セキュリティ課題トップ 10



質問：セキュリティ課題のトップ 3 を選択してください
有効回答数：368 件
出展：451 Research’ s Voice of the Enterprise: Information Security, Workloads & Key Projects 2021

上記の調査データが示すように、組織はセキュリティ上のさまざまな問題に取り組んでいます。ゼロトラスト・アプローチは効果的ですが、それらがうまく統合されていない場合、いくつかの課題が発生する可能性があります。エンドポイント保護は重要ですが、アクセス環境やネットワーク保護とひもづけることができなければ、運用が不必要に複雑になる可能性があります。セキュリティ・チームがそれぞれの側面に個別に対応しなければならない場合、重複して多大な労力が発生するだけでなく、復旧に要する時間も長くなる可能性があります。デバイスを復旧させる前に、セキュリティ・チームがデバイスの接続性を回復させるために別々に作業しなければならないとすると、デバイスのダウンタイムが長くなり、デバイスに依存している従業員の生産性が損なわれます。

デバイス管理がアクセスおよびネットワーク要素に統合されたレジリエントなゼロトラスト・アプローチにより、セキュリティ・チームはセキュリティ態勢の統合的かつ相関的なビューを得ることができます。これにより、アクセスの全体像が可視化され、把握しやすくなります。また、コントロール・ギャップやヒューマン・エラーの可能性を低減することができます。見落とされがちな点として、インシデント発生時に復旧のためのアンカーとして機能する統合された接続性の能力が挙げられます。デバイス保護パッケージの一部であるレジリエントな接続要素があれば、復旧がより迅速に行われ、従業員がより早く生産性を取り戻せるようになります。

ゼロトラスト環境を真にレジリエントなものにするためには、エンドポイント・セキュリティ、セキュアアクセス機能、ネットワークの可視性、管理機能を統合したシステムを構築する必要があります。多くのゼロトラスト・アプローチは、これらの要素をリンクさせることはできても、真の意味で統合することはできません。たとえば、デバイス態勢をアクセス環境に送ることは有効ですが、デバイスの侵害によって管理システムとの接続が断たれると、その効果は失われます。デバイスのアクティビティ情報が、アクセスを管理する同様の統合環境は、デバイス、そのアクティビティ、ネットワーク・トラフィック、ハイレベルな脅威の可視性など、あらゆる側面からの視点を集約することで、状況認識を強化することができます。統合環境は、デバイス、アクティビティ、ネットワーク・トラフィック、ハイレベルな脅威の可視性など、あらゆる側面からの視点を集約することで、状況認識を強化することができます。このようにして、組織は、真にレジリエントなゼロトラストが約束する利点を実現することができるのです。

ビジネスへの影響

従業員が信頼できるコネクティビティ. ゼロトラストのためのレジリエントなアプローチは、従業員が必要とする接続性を、信頼できる保証とともに提供します。接続性とは、ネットワークへのアクセスだけでなく、それを利用するためのデバイスの可用性も意味します。

セキュリティ上の最大の問題点に対処. セキュリティ・チームが直面する最も重要な問題に対処するための機能にアクセスできます。エンドポイント・セキュリティとコネクティビティを融合し、ユーザーの振る舞い、エンドポイント保護、リモート・アクセス、データ保護などの問題に取り組みます。

アクセスの一部としてのエンドポイント保護. エンドポイント保護とインシデントリカバリをアクセスの一部として統合することで、より効果的で効率的なセキュリティ運用が実現されます。

生産性の低下を抑制. インシデントは必ず発生します。組織は、従業員が速やかに生産性を回復できるよう、迅速に復旧できる体制を整えておく必要があります。

今後の展望

セキュリティ戦略で最も重要な要素として、状況の変化に適応する能力があげられます。ゼロトラスト・アプローチが効果的であるためには、現在はもちろん将来に亘って、環境の完全な運用ライフサイクルに対処できるように構築されている必要があります。451 Research は、ハイブリッドな勤務形態が組織の標準になると予想しており、それによってセキュリティ・チームにはさらなる制約が課されることになると考えています。同時に、サイバー犯罪者も、そのスキルと戦術を進化させ続けています。将来、どのような事態が発生しても対応できるように、ゼロトラスト・アーキテクチャは、エンドポイント・セキュリティとアクセスおよびネットワークの可視性を統合した機能を提供するとともに、インシデント発生時の復旧を容易にする回復力を提供する必要があります。未来について分からないことはたくさんありますが、ゼロトラストの強固な基盤は、組織が安全に未来に立ち向かうための準備に役立ちます。