DELL Technologies

エンドポイント セキュリティはゼロトラスト戦略の導入に不可欠な要素

ゼロトラストの準備に向けた 3 つの推奨事項

DELL Technologies

概要

ゼロトラストは長期にわたる取り組みです。このセキュリティ対策は、組織に導入する製品やソリューションとは違い、時間をかけて構築する、セキュリティ管理のための戦略的フレームワークです。この e-book では、IT 導入決定者がゼロトラスト トランスフォーメーションを導くための実用的なガイダンスを提供します。また、場所を問わずに仕事を進められる世界に向けて、現代的かつ真に安全な基盤を作り上げる上で、エンドポイント デバイスのセキュリティが果たす役割について重点的に説明します。

目次

サイバー攻撃に関する概要 3
..... 4
..... 5
..... 6
..... 7
3 8
..... 11
..... 11

サイバー攻撃に関する概要

テレワーク、ハイブリッド ワーク、クラウドの就業形態が増えるにつれ、セキュリティに対する脅威も高まっています。

組織のデータ資産の保護は、ここ数年で大きく複雑さを増しています。テレワークやハイブリッド ワークなどの就労形態が増えるにつれ、クラウドが業務の生産性に大変革をもたらしましたが、同時にコストも発生しました。オンプレミスのインフラストラクチャのみの管理からクラウドへと移行することにより、攻撃を受ける対象が拡大し、その影響も大きくなっています。例えば、攻撃を受けた場合、1 人のお客様のみではなく、そのクラウド サービスを利用するすべてのお客様、またサプライ チェーン全体の利用者に影響が及ぶ可能性があります。国家による攻撃でも、一般的な犯罪者による攻撃の場合でも、攻撃者は多額の支払を要求できる可能性があります。その結果、犯罪者たちは、新たな脆弱性を常に探し続けています。

世界中のサイバー犯罪による損害額は、**2025 年までに 10 兆 5 千億ドル**にのぼると予想されています [i]

Verizon が実施した 2022 年の調査によると、確認されたデータ侵害の件数は **5,200** 件に達しています。**これは前年比の 1.3 倍です** [ii]

場所を問わずに仕事ができる世界が意味するもの

組織は、進化する脅威のランドスケープに対して準備する方法を見つける必要があります。

では、リモート ワークが増大する世界が意味するものとは何でしょうか？大まかに言うと、2 つあります。

あらゆる組織には脆弱性があり、...

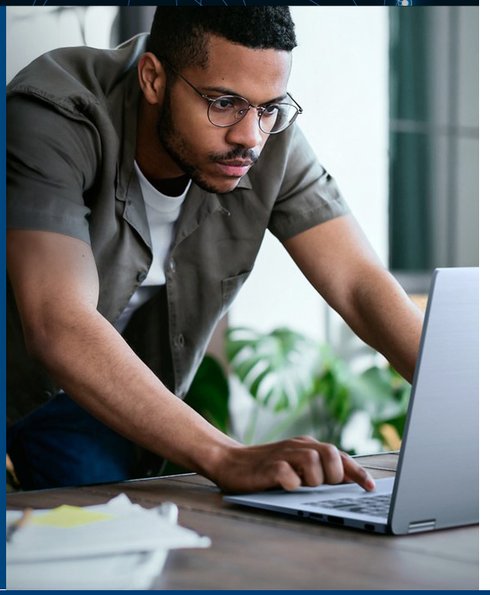
> 「組織のシステムに本気で侵入しようと思う者がいたなら、成功する可能性はかなり高いのです」
>
> *— 元国家安全保障局長官、元米国サイバー軍司令官 Michael Rogers 提督* [iii]

... 対応を誤ると莫大な被害を受ける。

> 「2024 年のデータ侵害の被害額は、過去最悪を記録し、平均 488 万米ドルでした」[iv]

攻撃の経路は増え、攻撃対象領域も拡大しているため、完全にセキュリティを確保できているという企業はありません。組織は最悪のシナリオを想定し、回避できない攻撃に備えて防御を固める必要があります。

69% の組織が、インターネットに接続している資産の管理が不十分だったため、何らかのサイバー攻撃を受けています。[v]



進化が求められているセキュリティ戦略

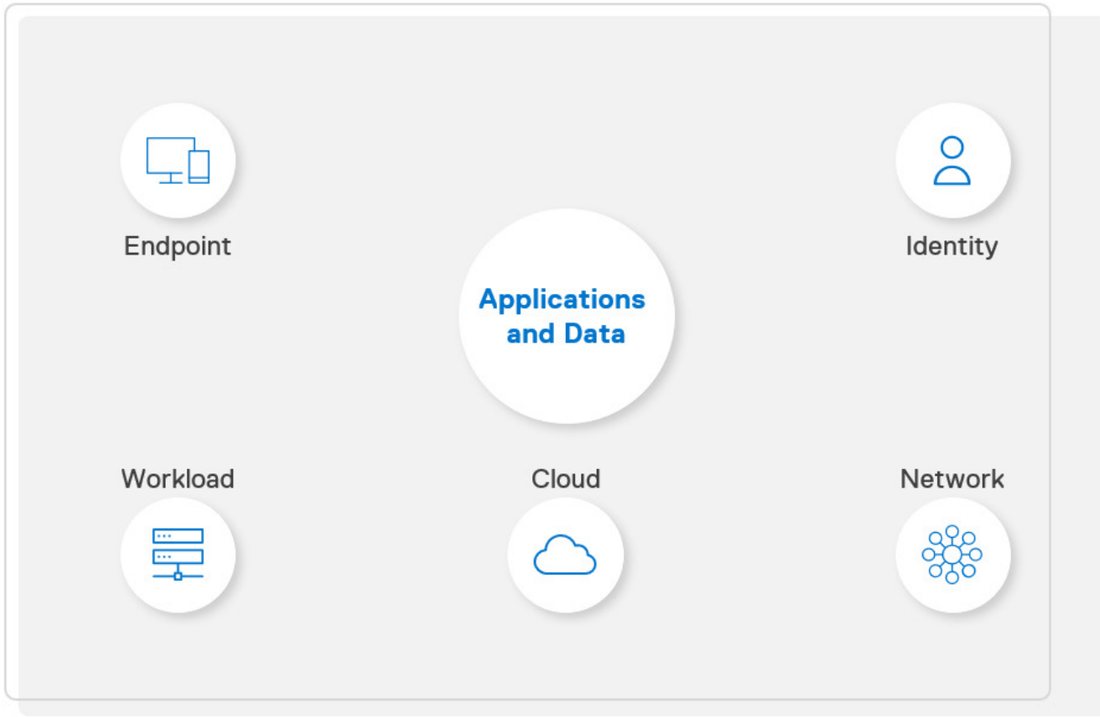
クラウドベースの環境を活用する必要があります。これが、ゼロトラストという考え方が生まれた背景です。

従来のセキュリティ モデルはもはや通用しません。ここでは、その理由を説明します。

組織が効果的なセキュリティ体制を備えるためには、5 つの管理ポイントに注意する必要があります。つまり、エンドポイント、ワークロード、ID、ネットワーク、クラウドです。目標は、アプリケーションとデータを保護することです。

従来のアプローチでは、サイロ化が進みやすくなります。そのため、このようなアプローチをとる組織が攻撃を受ける可能性は高くなります。

次へ ...

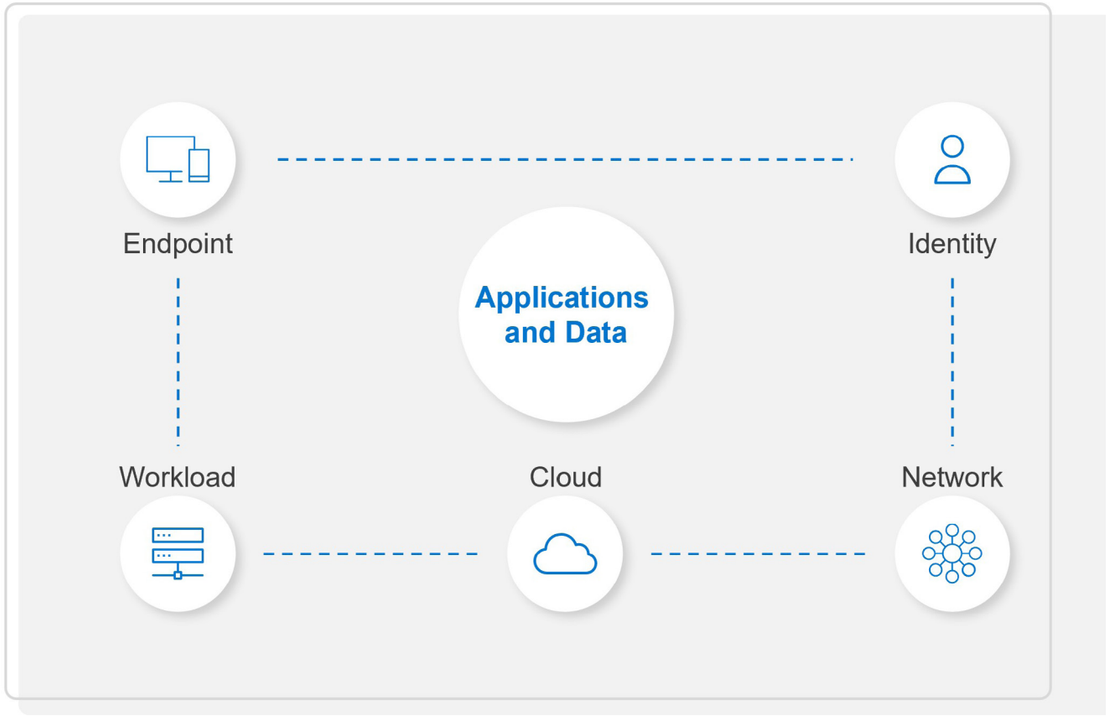


進化が求められているセキュリティ戦略

クラウドベースの環境を活用する必要があります。これが、ゼロトラストという考え方が生まれた背景です。

最新のアプローチでは、管理体制の強化を目指し、管理ポイント間の通信を改善する方向に進んでいます。ただし、テレワークやハイブリッド ワークの環境を採用することが増えているため、境界をさらに強化する必要があります。

次へ ...

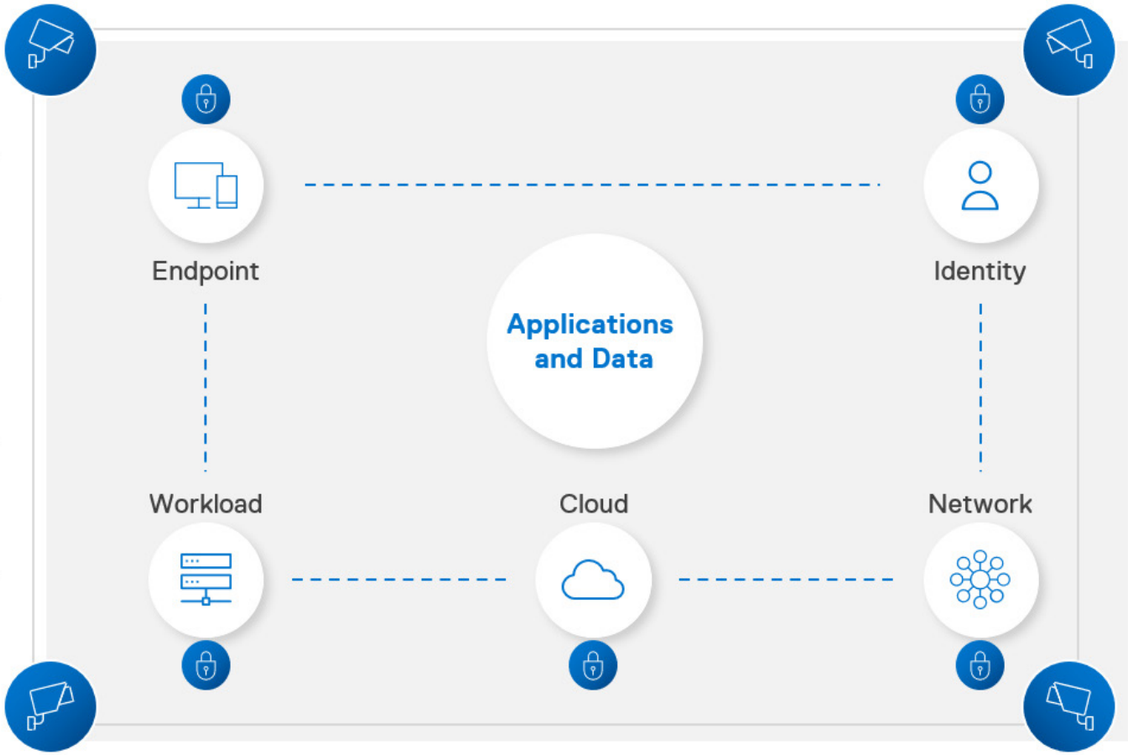


進化が求められているセキュリティ戦略

クラウドベースの環境を活用する必要があります。これが、ゼロトラストという考え方が生まれた背景です。

現在、従業員は自宅、カフェ、ホテルなどあらゆる場所で仕事をしていますが、セキュリティ保護されていない Wi-Fi を使用しているため、ファイアウォールで保護されたオフィスやデータ センターへの接続が制限されたり、まったく接続できなかったりすることがよくあります。標準的な状況では、デバイスからインターネットに直接接続し、クラウドのファイル サーバーやソフトウェア アズ ア サービス (SaaS) アプリケーションに接続して、企業のデータで作業を進めます。

攻撃がますます先鋭化し、攻撃の経路も増加しているため、暗黙の信頼を前提に構築された従来のセキュリティ戦略は、もはや通用しません。これが、ゼロトラストという考え方が生まれた背景です。



ゼロトラストの基本を理解する

ゼロトラストとは、セキュリティの新しい考え方です。これは、*暗黙*の信頼（一度認証されると、ユーザーはネットワーク内を自由に動き回ることができる）に取って代わるアプローチです。ゼロトラストは、このパラダイムを覆して、組織が IT 環境を明示的にコントロールできるようにします。

ゼロトラストを、よく知られた概念で説明してみましょう。ここでは建物のセキュリティ対策にたとえてみます。

あなたは企業のオフィスで働いています。採用時に社員証を渡され、セキュリティ対策についての説明を受けました。毎日この建物の中に入ります。カメラがいたる所に設置されており、数か所で社員証を提示します。自分の席に座り、コンピューターのロックをパスワードで解除します。

An employee arrives at their office building and gets their badge out to gain entry.

次へ ...

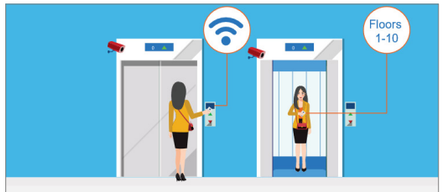
ゼロトラストの基本を理解する

ゼロトラストとは、セキュリティの新しい考え方です。これは、*暗黙*の信頼（一度認証されると、ユーザーはネットワーク内を自由に動き回ることができる）に取って代わるアプローチです。ゼロトラストは、このパラダイムを覆して、組織が IT 環境を明示的にコントロールできるようにします。

ゼロトラストを、よく知られた概念で説明してみましょう。ここでは建物のセキュリティ対策にたとえてみます。

あなたは企業のオフィスで働いています。採用時に社員証を渡され、セキュリティ対策についての説明を受けました。毎日この建物の中に入ります。カメラがいたる所に設置されており、数か所で社員証を提示します。自分の席に座り、コンピューターのロックをパスワードで解除します。

An employee arrives at their office building and gets their badge out to gain entry.



They use their badge to gain access to the elevator assigned to their floor.

次へ ...

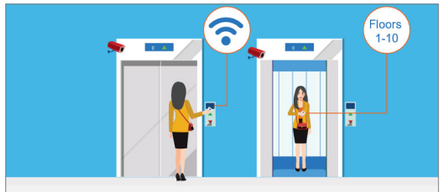
ゼロトラストの基本を理解する

ゼロトラストとは、セキュリティの新しい考え方です。これは、*暗黙*の信頼（一度認証されると、ユーザーはネットワーク内を自由に動き回ることができる）に取って代わるアプローチです。ゼロトラストは、このパラダイムを覆して、組織が IT 環境を明示的にコントロールできるようにします。

ゼロトラストを、よく知られた概念で説明してみましょう。ここでは建物のセキュリティ対策にたとえてみます。

あなたは企業のオフィスで働いています。採用時に社員証を渡され、セキュリティ対策についての説明を受けました。毎日この建物の中に入ります。カメラがいたる所に設置されており、数か所で社員証を提示します。自分の席に座り、コンピューターのロックをパスワードで解除します。

An employee arrives at their office building and gets their badge out to gain entry.



They use their badge to gain access to the elevator assigned to their floor.

The employee uses their badge again to activate their floor selection in the elevator.

次へ ...

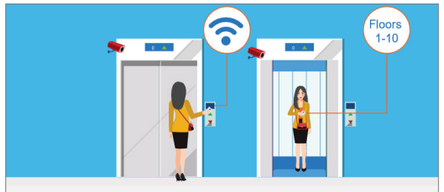
ゼロトラストの基本を理解する

ゼロトラストとは、セキュリティの新しい考え方です。これは、*暗黙*の信頼（一度認証されると、ユーザーはネットワーク内を自由に動き回ることができる）に取って代わるアプローチです。ゼロトラストは、このパラダイムを覆して、組織が IT 環境を明示的にコントロールできるようにします。

ゼロトラストを、よく知られた概念で説明してみましょう。ここでは建物のセキュリティ対策にたとえてみます。

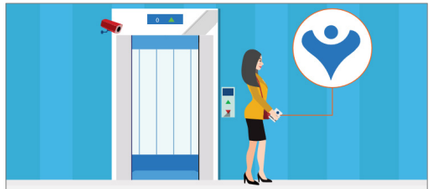
あなたは企業のオフィスで働いています。採用時に社員証を渡され、セキュリティ対策についての説明を受けました。毎日この建物の中に入ります。カメラがいたる所に設置されており、数か所で社員証を提示します。自分の席に座り、コンピューターのロックをパスワードで解除します。

An employee arrives at their office building and gets their badge out to gain entry.



They use their badge to gain access to the elevator assigned to their floor.

The employee uses their badge again to activate their floor selection in the elevator.



Once they arrive on their floor, the employee walks to their office suite.

次へ ...

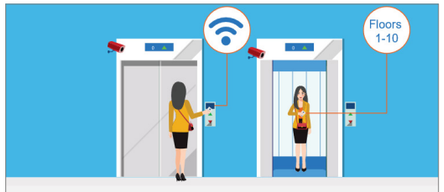
ゼロトラストの基本を理解する

ゼロトラストとは、セキュリティの新しい考え方です。これは、*暗黙*の信頼（一度認証されると、ユーザーはネットワーク内を自由に動き回ることができる）に取って代わるアプローチです。ゼロトラストは、このパラダイムを覆して、組織が IT 環境を明示的にコントロールできるようにします。

ゼロトラストを、よく知られた概念で説明してみましょう。ここでは建物のセキュリティ対策にたとえてみます。

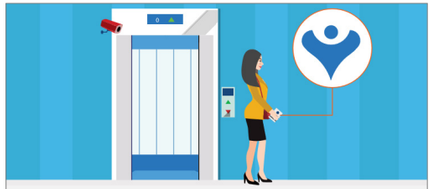
あなたは企業のオフィスで働いています。採用時に社員証を渡され、セキュリティ対策についての説明を受けました。毎日この建物の中に入ります。カメラがいたる所に設置されており、数か所で社員証を提示します。自分の席に座り、コンピューターのロックをパスワードで解除します。

An employee arrives at their office building and gets their badge out to gain entry.



They use their badge to gain access to the elevator assigned to their floor.

The employee uses their badge again to activate their floor selection in the elevator.



Once they arrive on their floor, the employee walks to their office suite.

They swipe their ID card to gain entry to their suite.

次へ ...

ゼロトラストの基本を理解する

ゼロトラストとは、セキュリティの新しい考え方です。これは、*暗黙*の信頼（一度認証されると、ユーザーはネットワーク内を自由に動き回ることができる）に取って代わるアプローチです。ゼロトラストは、このパラダイムを覆して、組織が IT 環境を明示的にコントロールできるようにします。

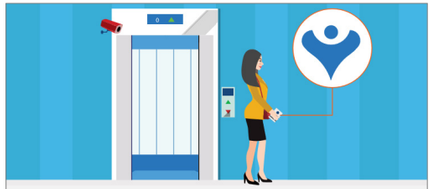
ゼロトラストを、よく知られた概念で説明してみましょう。ここでは建物のセキュリティ対策にたとえてみます。

あなたは企業のオフィスで働いています。採用時に社員証を渡され、セキュリティ対策についての説明を受けました。毎日この建物の中に入ります。カメラがいたる所に設置されており、数か所で社員証を提示します。自分の席に座り、コンピューターのロックをパスワードで解除します。

An employee arrives at their office building and gets their badge out to gain entry.

They use their badge to gain access to the elevator assigned to their floor.

The employee uses their badge again to activate their floor selection in the elevator.



Once they arrive on their floor, the employee walks to their office suite.

They swipe their ID card to gain entry to their suite.

The employee arrives at their desk and unlocks their computer using a password.

次へ ...

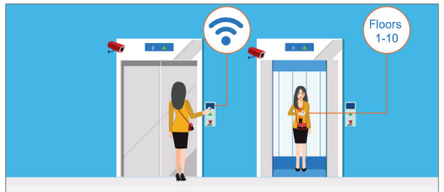
ゼロトラストの基本を理解する

これがゼロトラストの仕組みです。

雇用主は、入社初日から社員を確認できます。それ以降は、組織の資産（ユーザーやデータなど）を保護するため、アクセスを要求するたびに認証が行われます。さらにセキュリティ確保の手段として、警備員が建物内のあらゆる場所の動きをモニターで監視しています。許可されていない部屋への侵入など不審な動きが確認されると、調査の対象になります。

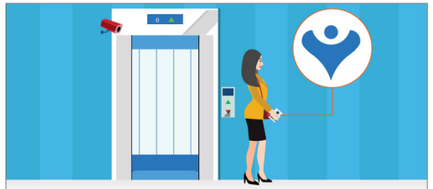
現在、ユーザー、デバイス、アプリケーション、データが、企業のネットワーク外に存在することが、これまでになく多くなっています。その結果、ユーザー ID が盲点となり、多くのセキュリティ侵害では ID 情報の漏えいが主な要因になっています。ゼロトラストを採用すると、これが修正されます。

An employee arrives at their office building and gets their badge out to gain entry.



They use their badge to gain access to the elevator assigned to their floor.

The employee uses their badge again to activate their floor selection in the elevator.



Once they arrive on their floor, the employee walks to their office suite.

They swipe their ID card to gain entry to their suite.

The employee arrives at their desk and unlocks their computer using a password.

ゼロトラストの原則を有効にする

エンドポイント セキュリティは、ゼロトラスト トランスフォーメーションに不可欠な要素です。

ゼロトラスト戦略を効果的に導入するには、セキュアなエンドポイントが不可欠です。

MITRE ATT&CK® のフレームワークによると、攻撃者がネットワークへの侵入に使用する「初期のアクセス技術」が現在 9 種類存在するとされています（*イラストを参照*）[vi]。この調査で示されているように、クラウドベースの世界では、従来の防御策ではエンドポイントのセキュリティを確保できません。攻撃者には、わずか 1 か所の侵入ポイントがあればよいのです。エンドポイントが多数あるために、攻撃者は、デバイスのライフサイクル全体を通じて、いくつもの脆弱性を利用できるのです。

ネットワーク上のデバイス数の増加に伴い、エンドポイントが攻撃ベクトルとして狙われるようになっています。

ゼロトラスト モデルでは、セキュリティ ポリシーによって「既知の正常な」状態が明確かつ詳細に定義され、それ以外はすべてブロックされます。その後、脅威管理機能で既知の正常な状態から逸脱していないか監視し、通常と異なる動作にフラグを設定して、潜在的な脅威を修復するための適切なアクションをトリガーします。

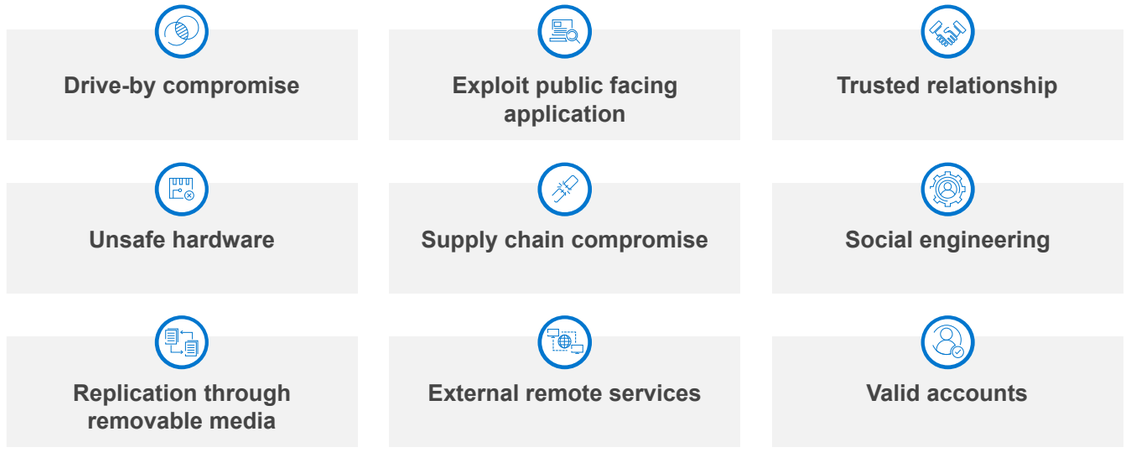


イラスト 1/3

ゼロトラストの原則を有効にする

エンドポイント セキュリティは、ゼロトラスト トランスフォーメーションに不可欠な要素です。

ゼロトラスト戦略を効果的に導入するには、セキュアなエンドポイントが不可欠です。

MITRE ATT&CK® のフレームワークによると、攻撃者がネットワークへの侵入に使用する「初期のアクセス技術」が現在 9 種類存在するとされています（*イラストを参照*）[vi]。この調査で示されているように、クラウドベースの世界では、従来の防御策ではエンドポイントのセキュリティを確保できません。攻撃者には、わずか 1 か所の侵入ポイントがあればよいのです。エンドポイントが多数あるために、攻撃者は、デバイスのライフサイクル全体を通じて、いくつもの脆弱性を利用できるのです。

ネットワーク上のデバイス数の増加に伴い、エンドポイントが攻撃ベクトルとして狙われるようになっています。

ゼロトラスト モデルでは、セキュリティ ポリシーによって「既知の正常な」状態が明確かつ詳細に定義され、それ以外はすべてブロックされます。その後、脅威管理機能で既知の正常な状態から逸脱していないか監視し、通常と異なる動作にフラグを設定して、潜在的な脅威を修復するための適切なアクションをトリガーします。

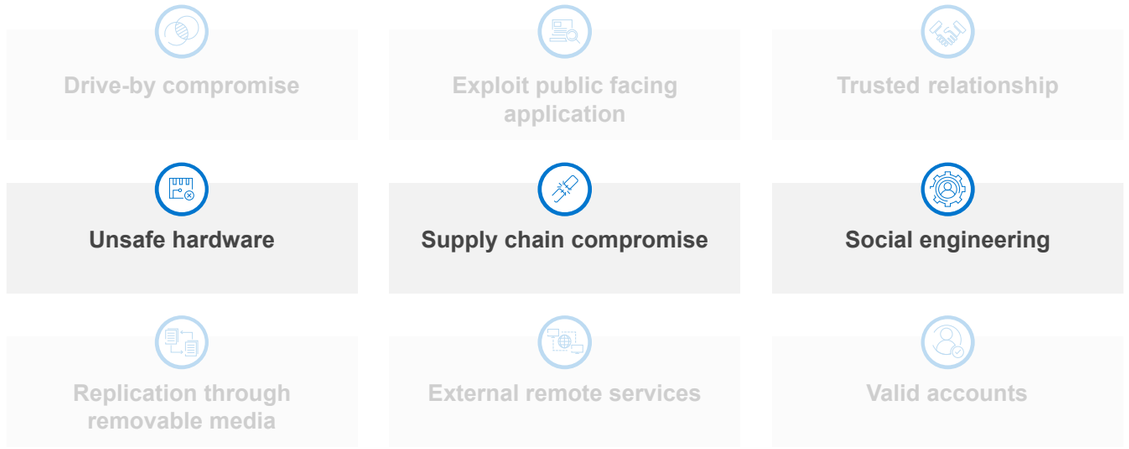


イラスト 2/3

ゼロトラストの原則を有効にする

エンドポイント セキュリティは、ゼロトラスト トランスフォーメーションに不可欠な要素です。

ゼロトラスト戦略を効果的に導入するには、セキュアなエンドポイントが不可欠です。

MITRE ATT&CK® のフレームワークによると、攻撃者がネットワークへの侵入に使用する「初期のアクセス技術」が現在 9 種類存在するとされています（*イラストを参照*）[vi]。この調査で示されているように、クラウドベースの世界では、従来の防御策ではエンドポイントのセキュリティを確保できません。攻撃者には、わずか 1 か所の侵入ポイントがあればよいのです。エンドポイントが多数あるために、攻撃者は、デバイスのライフサイクル全体を通じて、いくつもの脆弱性を利用できるのです。

ネットワーク上のデバイス数の増加に伴い、エンドポイントが攻撃ベクトルとして狙われるようになっています。

ゼロトラスト モデルでは、セキュリティ ポリシーによって「既知の正常な」状態が明確かつ詳細に定義され、それ以外はすべてブロックされます。その後、脅威管理機能で既知の正常な状態から逸脱していないか監視し、通常と異なる動作にフラグを設定して、潜在的な脅威を修復するための適切なアクションをトリガーします。

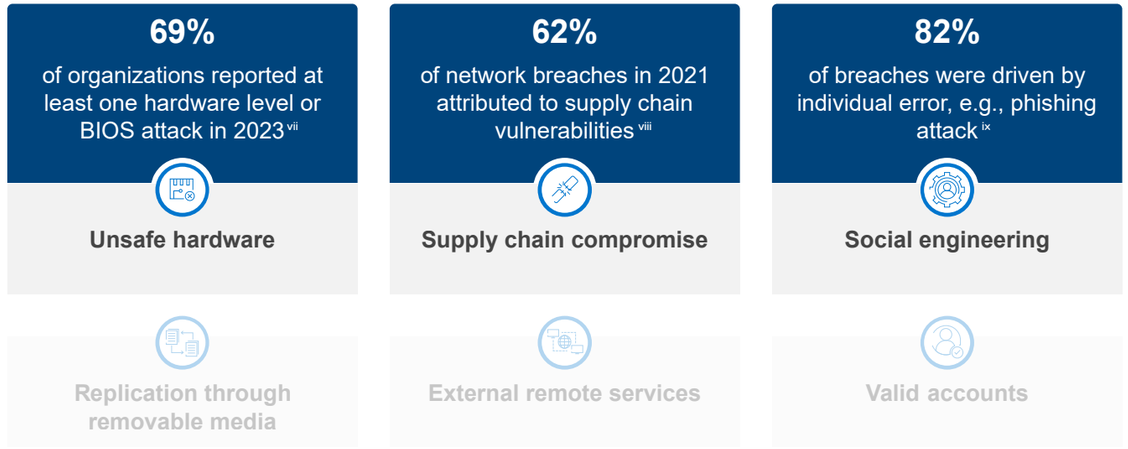


イラスト 3/3

ゼロトラストの準備に向けた 3 つの推奨事項

ゼロトラスト トランスフォーメーションの成功に向けて組織の体制を整えましょう。

1

ビジネスの優先事項をサポートする適切なポリシーと管理体制を確立しましょう。

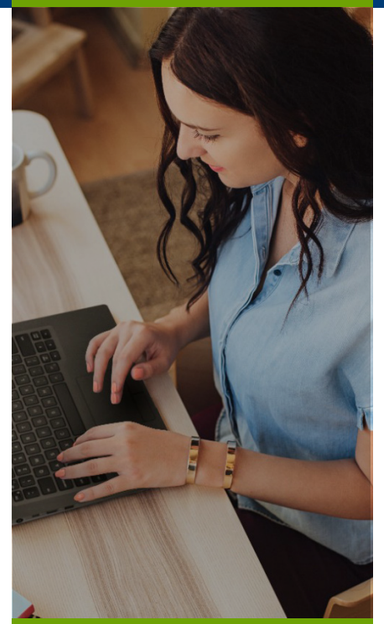
ポリシー エンジンとポリシー管理は、効果的なゼロトラストの実装に不可欠です。ただし、セキュリティ予算を無制限に確保できる組織はありません。したがって、まずはビジネスの優先事項を決定します。保護すべき対象の中で、最も重要な資産と IP を検討してください。その際に、攻撃対象領域と、組織で許容できるリスクとを比較して考慮します。

次に、現在策定されているポリシーと管理体制を見直します。現在のリスクは、私たちが活動するクラウドベースの世界から発生するものです。お使いのポリシー エンジンがこの点について考慮されていることを確認してください。

最も重要な資産へのアクセスを管理するためのポリシーを策定することで、範囲を拡大できるようになります。

詳細

詳しい情報については、*こちらの動画をご覧ください*。Dell のサイバー専門家が、組織が現在直面している主なセキュリティ リスクについて説明します。



企業ネットワークの外部にかつてないほど多くのユーザー、アプリ、データ、デバイスが存在する状況により、IT セキュリティ意思決定者の **82%** は、セキュリティ ポリシーの評価をやり直す必要があると回答しています。[x]

ゼロトラストの準備に向けた 3 つの推奨事項

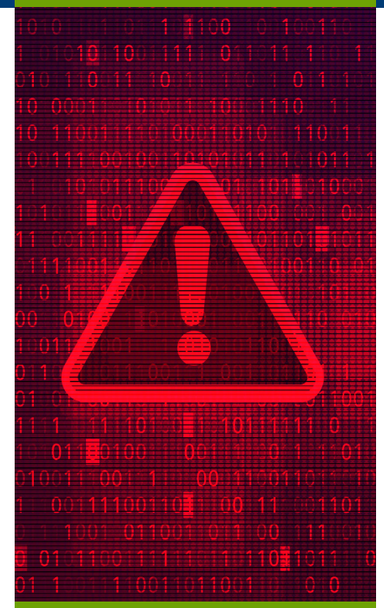
ゼロトラスト トランスフォーメーションの成功に向けて組織の体制を整えましょう。

2 安全なデバイスから始めましょう。

ゼロトラストの計画には、確固とした基盤が必要です。セキュリティを考慮して設計および開発されたデバイスで、防御体制を強化します。以下はその例です。

A. **ハードウェアベースおよびファームウェアベースの保護**：エンドポイント スタックのセキュリティを確保し、可視化します（BIOS の侵害を検知し、IT 部門にアラートを通知するなど）。新規のアクセス要求があるたびに ID を検証して、社員の生産性への影響を最小限にするテクノロジーを組織に導入しましょう。

B. **サプライ チェーンの保護と整合性の管理**：パソコンのライフサイクルの各段階でセキュリティを確保します。近年見られるように、サプライ チェーンへの攻撃による被害は莫大です。真のゼロトラストのアーキテクチャ、認証、検証、モニタリングは、サプライ チェーンから始まります。1）安全なビジネス慣行を採用しており、2）調達から製造や配送に至るまで、デバイスの整合性を検証できるベンダーと取引しましょう。



2021 年に、ある IT 管理企業が受けたランサムウェア攻撃によって、**1,500** 以上のお客様に影響が及びました。[xi]

詳細

デバイス セキュリティのベスト プラクティスに関する詳しい情報は、**Dell** およびインテルのホワイトペーパー、「*Achieving Pervasive Security Above and Below the OS*」をお読みください。

ゼロトラストの準備に向けた 3 つの推奨事項

ゼロトラスト トランスフォーメーションの成功に向けて組織の体制を整えましょう。

3

シームレスな統合と、エコシステム全体の相互運用性を目指しましょう。

高レベルかつ効果的なセキュリティ体制を実現するために、不可欠なことが 3 つあります。

A. IT エコシステムにおける、あらゆる保護機能の統合。

B. リアルタイムの可視性。

C. 必要なときに対策を講じることができる能力。

クラウドベースの世界では、ほんのわずかな脆弱性の確認を怠っただけでも、悪夢のような事態が引き起こされる可能性があります。そのため、すべてのシステムで脅威の可能性を認識し、さらに必要な対策を講じることが重要です。

お使いのシステムは統合されているでしょうか？サイロ化した状態で運用されてはいないでしょうか？ポリシー エンジンは、ネットワーク上の BIOS の侵害アラートを IT 管理者に通知する際、特定のワークフローを起動できますか？統合された環境では、オートメーションによって直ちに問題の BIOS を隔離し、以降のアクセスを制限して、修正作業を実行する必要があります。

すべてのエンドポイントを可視化できますか？サプライ チェーン（荷物の搬入口など）からファームウェア（BIOS レベルの改ざんアラートなど）まで、あらゆる階層から取得される充実したテレメトリーがあることが理想的です。

ただし、そのテレメトリーも、統合と同程度の効果しかありません。自社のデータに対応できますか？問題に対処するデータとプログラムのワークフローを把握するため、スキルの高いサイバーセキュリティ人材など、適切なリソースを配置することが重要です。

41% の組織が、ゼロトラストを導入しています [xii]

DELL Technologies

重要ポイント

セキュリティの未来を担うのはゼロトラストです。

- 未来の働き方を取り入れることで、攻撃ベクトルも急激に増加します。
- 侵害行為を避けることはできません。最悪のシナリオに備えた防御体制で、攻撃対象領域を最小限に抑えましょう。
- ゼロトラストは、セキュリティに対する新しい考え方で、組織が IT 環境を明示的にコントロールできるようにします。
- ゼロトラストの原則を有効にするエンドポイントの保護が、セキュリティ保護された現代の基盤を維持する鍵となります。
- ゼロトラスト アーキテクチャを優先的に構築するため、最も重要な資産をピンポイントで特定します。
- 組み込み型の保護を提供するベンダーからデバイスを調達し、サプライ チェーン管理にしっかり投資します。
- セキュリティと IT の相互運用性を評価します。継続的にワークフローを埋め込み、セキュリティ体制を強化します。

次のステップへ

セキュリティは、あらゆる規模の組織にとっての難題です。セキュリティおよびテクノロジーに関する経験豊富なパートナーと提携することで、ゼロトラスト トランスフォーメーションを合理化できます。

Dell Trusted Workspace は、エンドポイントのセキュリティ確保を支援し、ゼロトラスト対応のモダンな IT 環境の構築を促進します。Dell 独自のハードウェアおよびソフトウェア保護の包括的ポートフォリオで、攻撃対象領域を削減しましょう。当社のきめ細かい防御ベースのアプローチでは、組み込み型の保護と常時警戒を組み合わせることで脅威を回避します。エンド ユーザーの生産性を維持しつつ、IT 部門は、現代のクラウドベースの世界向けに構築されたセキュリティ ソリューションにより、自信を持って業務を遂行できます。

お問い合わせ先： global.security.sales@dell.com
ソリューションの詳細： Dell.com/Endpoint-Security
SNS でフォローする： LinkedIn @DellTechnologies | Twitter @DellTech

DELL Technologies

[i] Cybersecurity Almanac 2nd Edition.Cybersecurity Ventures, 2022 https://cybersecurityventures.com/cybersecurity-almanac-2022/

[ii] Ponemon Institute and IBM, Cost of a Data Breach Report, 2024 https://www.ibm.com/security/data-breach

[iii] American College of Cardiology, You Will Be Hacked.Plan Now: Cybersecurity in Health Care, 2021 https://www.acc.org/Latest-in-Cardiology/Articles/2021/11/01/01/42/Feature-You-Will-Be-Hacked-Plan-Now-Cybersecurity-in-Health-Care

[iv] Ponemon Institute and IBM, Cost of a Data Breach Report, 2024 https://www.ibm.com/security/data-breach

[v] ESG Complete Survey Results, Security Hygiene and Posture Management, 2022 https://www.esg-global.com/research/esg-complete-survey-results-security-hygiene-and-posture-management

[vi] MITRE ATT&CK https://attack.mitre.org/tactics/TA0001/

[vii] Futurum Group, Endpoint Security Trends, 2023. https://www.delltechnologies.com/asset/en-us/solutions/business-solutions/industry-market/futurum-group-endpoint-security-trends-research-report.pdf

[viii] Verizon Data Breach Investigations Report, 2022 https://www.verizon.com/business/resources/reports/dbir/2022/summary-of-findings/

[ix] Verizon Data Breach Investigations Report, 2022 https://www.verizon.com/business/resources/reports/dbir/2022/summary-of-findings/

[x] Absolute Endpoint Risk Report, 2021 https://www.absolute.com/go/reports/endpoint-risk-report/

[xi] TechTarget, 2021 https://www.techtarget.com/searchsecurity/news/252503605/Kaseya-1500-organizations-affected-by-REvil-attacks

[xii] Ponemon Institute and IBM, Cost of a Data Breach Report, 2022 https://www.ibm.com/security/data-breach