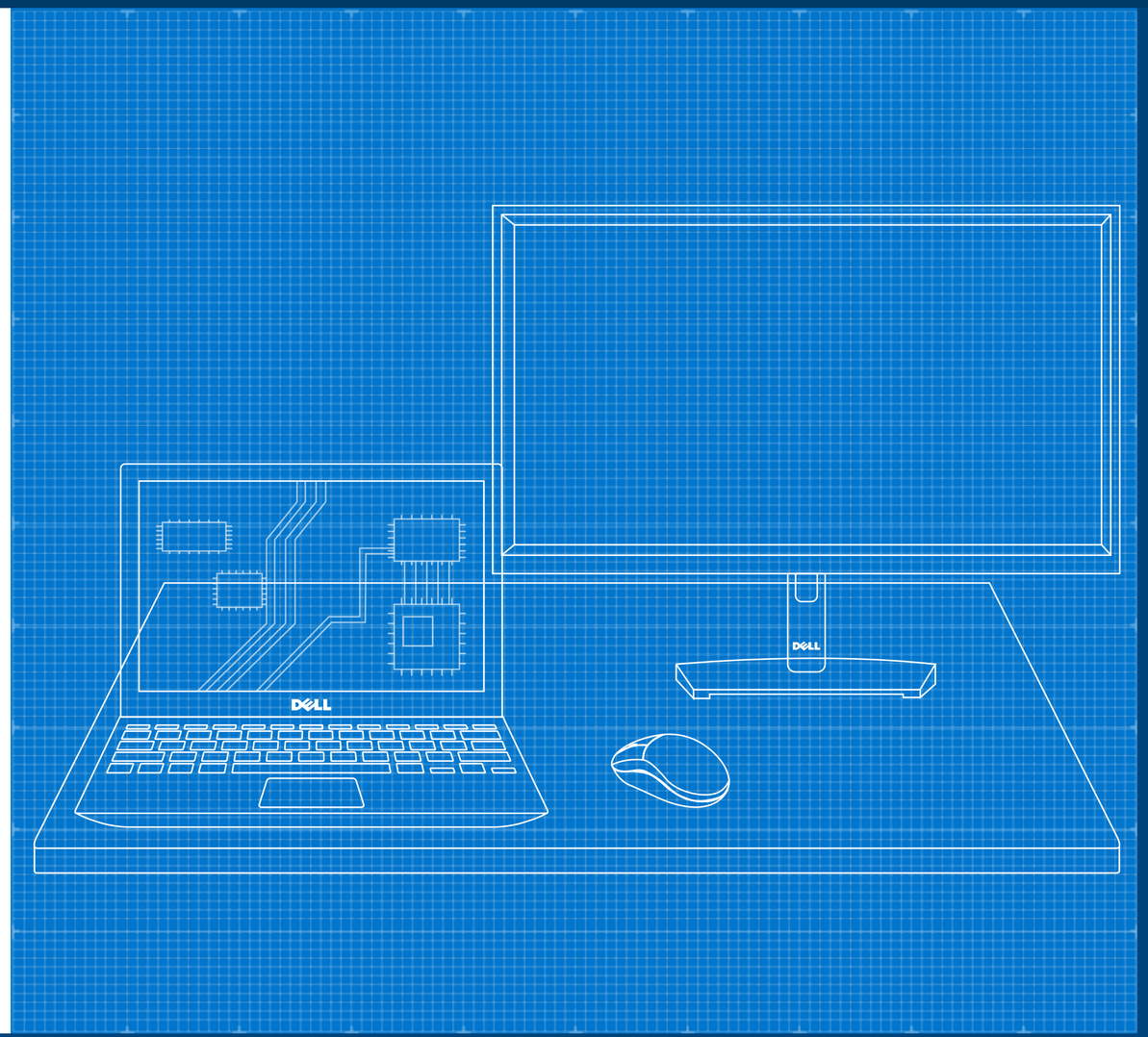
DELL Technologies

徹底解剖：信頼できるワークスペース

多層防御で組織全体のセキュリティを向上



概要

今日、サイバー攻撃の発生は不可避であり、攻撃はより大規模かつ巧妙になっています。主な標的とされるようになったのは、エンドポイント デバイス、ネットワーク、クラウド環境です。

このe-bookは、ITおよびセキュリティ部門の意思決定者向けのガイドであり、進化を続ける脅威ランドスケープにおいて効果的にエンドポイントを保護するために必要となる要素について解説します。

目次

今日の脅威ランドスケープ

ハイブリッド型の業務体制への移行が進むことで、複雑な状況と新しい攻撃ベクターによる侵害が発生しています。それに伴い、**エンドポイント、ネットワーク、クラウドにおいて攻撃対象領域が拡大しています**。

さらに、昨今の攻撃者は、コンピューティング スタックのさまざまなレイヤーを標的とする巧妙な手法を利用し、正常なシステム プロセスに攻撃を潜ませるようになっています。一部の攻撃者は、特権的なアクセス権限を取得する方法により、検出を完全に回避しつつソフトウェア保護の機能を無効化する場合さえあります。

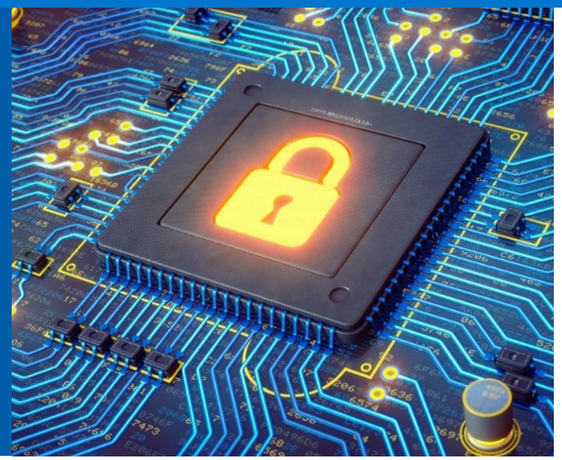
このような脅威に対抗するために、多くの組織がゼロトラストの導入に取り組むようになりました。しかし、ゼロトラストの原則を有効にするには、デバイスを信頼できる状態に維持しなければなりません。

攻撃がより頻繁になり、高度なテクノロジーによって新たな攻撃経路が次々に生まれるなか、**デバイスの信頼性をどのように維持できるでしょうか？**

[1] 『CrowdStrike 2024 Global Threat Report』
[2] 『Dell Innovation Index』、2023年

ご存じでしょうか...

2023年に発生した攻撃の75%が、マルウェアをベースとしないタイプの攻撃[1]



「自社のテクノロジーやアプリケーションにはセキュリティが組み込まれている」と極めて強い自信を持って回答したのは、調査対象組織の41%のみ[2]

サイバーセキュリティの成熟度を高めるゼロトラストの詳細にご興味のある方は、当社のe-book *『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』*をぜひお読みください。

課題

効果的なエンドポイント セキュリティを実装するには、攻撃者とその活動を理解することが重要です。

侵害により得られる可能性のある多額の利益を念頭に、**攻撃者は成功の確率を高めるためにさまざまな手法やエントリー ポイントを利用しながら、同じ組織への侵害を何度も試みます。**たとえば、攻撃者は1つのデバイスのライフサイクル全体を通して、多数の攻撃経路で脆弱性を利用しようとする可能性があります。

従来の防御方法は、エンドポイントの安全を維持するうえで十分に機能していません。組織が1つの攻撃対象領域の保護を強化しても、脅威アクターはより脆弱な別の領域に標的を移すだけです。世界中でハイブリッド型の業務体制が普及したことで、脅威アクターはエンドポイントという新たな攻撃経路を特定し、その結果として深刻な被害が生じています。

右側の攻撃の例を参照してください

サプライ チェーン攻撃：標的とされるのはサプライヤーです。サプライヤーの（さらに、その延長として顧客の）システム、データ、ネットワークへのアクセス権限を取得しようとします。**例としては、コンポーネントの改ざんから始まる、下記のようなハードウェア サプライ チェーンへの攻撃が挙げられます。**

攻撃者はPCの出荷時に侵害し、ハード ドライブを改ざんします。

組織のIT部門は、侵害されたデバイスを組織全体に導入します。

攻撃者はマルウェアをインストールし、ユーザーがログインした際に資格情報を窃取します。

ソーシャル エンジニアリング攻撃：標的はエンド ユーザーです。攻撃者はエンド ユーザーを騙して機密情報を提供させ、デバイスやネットワークへのアクセス権限の取得に利用します。**例としては、以下のようなフィッシング メールから始まるスプーフィング攻撃が挙げられます。**

エンド ユーザーがフィッシング メールに騙され、偽造されたWebページに誘導されて資格情報を提供します。

攻撃者はこの正当な資格情報を使用して、ネットワークに遠隔でアクセスします。

攻撃者はWebサービス経由でデータを引き出し、窃取したデータを暗号化して身代金の要求に利用します。

モダン ワークスペースの保護

エンドポイントの保護では、デバイスのライフサイクル全体のさまざまな状況において、防御、検出と対応、リカバリーと修復が必要になります。ライフサイクル全体には、PCの部品調達から製造、出荷、導入、業務使用の期間、廃棄までが含まれます。その攻撃対象領域の大きさを想像してみてください。

最も効果的なサイバーセキュリティ戦略は、最悪のシナリオに備えた計画を組み入れた戦略です。そうした戦略では、侵害は起こり得るものだと想定し、攻撃を可能な限り迅速かつ数多く阻止できるよう、多層防御を戦略に組み込みます。また、攻撃の再発リスクを最小限に抑えるための修復機能も導入します。

防御

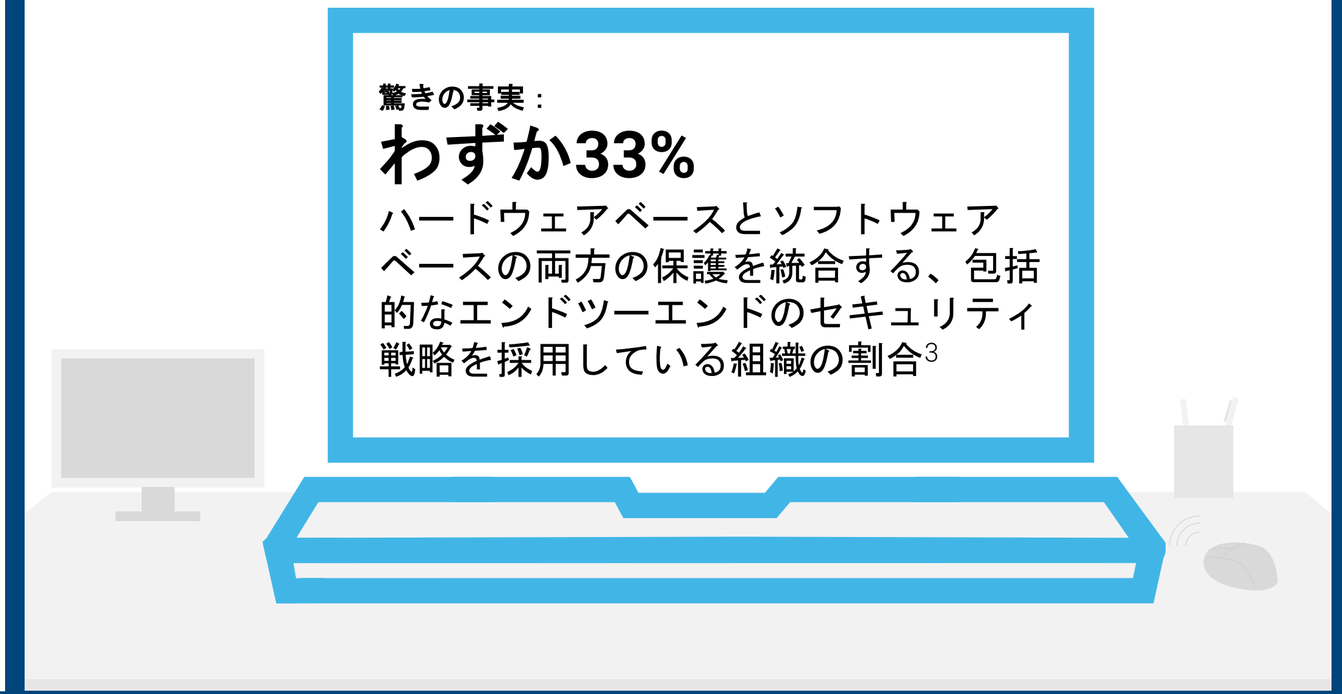
攻撃をブロックするために設計された防御機能で、攻撃の標的となる領域を縮小。

検出と対応

侵害は常時発生し得ると想定し、警戒を維持。

リカバリーと修復

攻撃による影響を緩和し、通常の業務へと復帰。



[3]『Dell Innovation Index』、2023年

徹底解剖：信頼できるワークスペース

最新のエンドポイント セキュリティは、3つの要素を必要とします。

1. **ソフトウェア セキュリティ**：今日では、かつてないほどにユーザー、デバイス、データが企業ネットワークの外部に存在するようになっています。ソフトウェア セキュリティでは、デバイスを保護するだけでなく、悪意ある活動の起点となることの多いネットワークやクラウドの環境にも保護の範囲を拡張します。

2. **ハードウェア セキュリティ**：デバイスにはセキュリティ機能を組み込む必要があります。これには、使用中のデバイスを保護するハードウェアおよびファームウェアのセキュリティが関連します。ワークスペースを保護するためには、デバイスの可視化と制御を可能にする組み込み型の機能が必要です。

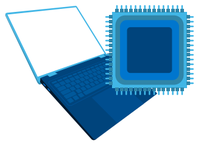
3. **サプライ チェーン セキュリティ**：デバイスはセキュアな方法で製造する必要があります。これは、a)最新の脅威ランドスケープを理解しており、b)その知識をランドスケープの進化に合わせて適切に活用できるサプライヤーと提携することを意味します。PCの設計、開発、テストをセキュアな方法で実施すれば、製品の脆弱性によるリスクを最小化できます。また、サプライ チェーンでの統御により、製品改ざんのリスクを低減できます。

多層的なセキュリティ レイヤーの具体的内容

（セキュリティ施策の代表的な例を記載）

ソフトウェア セキュリティ

- 次世代アンチウイルス(NGAV)
- エンドポイントでの検出および対応(EDR)
- Extended Detection and Response (XDR)
- クラウド データ保護
- ネットワーク保護
- 自動化された自己修復



ハードウェア/ファームウェア セキュリティ

- 起動時間の検証
- ランタイムの検証
- ユーザー認証
- セキュリティに関する通知とアラート/テレメトリー

サプライ チェーン セキュリティ

- セキュアな開発プラクティス
- セキュアなサプライ チェーン プラクティス
- コンポーネントの検証
- 改ざん防止措置を施した梱包

当社のアプローチ：Dell Trusted Workspace

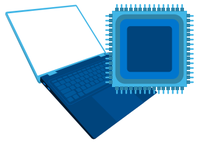
Dellは、全世界の組織が信頼するセキュリティおよびIT分野のパートナーです。Dellはポイント ソリューション ベンダーとは異なり、セキュリティにおける総合的な成果の達成を重視しており、キル チェーンを遮断してサイバー攻撃に対するレジリエンスを強化するためのソリューション スイートを構築しています。**Dell Trusted Workspaceは以下の要素で構成されます。**

- 世界最高レベルの安全性を誇るDellのビジネス向けPC[4]の基盤となっている、独自の**ハードウェア/ファームウェア保護機能**（組み込み型、内蔵型のセキュリティ）
- デバイスに加えてネットワークとクラウドも対象として、高度な脅威に対する保護機能を提供する、**業界をリードするソフトウェア** パートナーのエコシステム*（追加型のセキュリティ）*

[4]Dellの社内分析（2024年10月）に基づきます。インテル プロセッサー搭載のPCに対する評価です。すべてのPCで全機能を使用できるわけではありません。一部の機能では追加購入が必要です。Principled Technologiesによる検証『A comparison of security features』（2024年4月）

パートナー エコシステムに支えられた*追加型*のソフトウェア セキュリティ

- **Dell SafeGuard and Response**：**CrowdStrike**と**Secureworks**が脅威に対する検出、対応、修復の機能を提供。
- **Dell SafeData**：**Netskope**が、クラウドベースのアプリケーションを可視化およびモニタリングし、データ ロスを防止する機能を提供。**Absolute**が、アプリケーションとネットワークの自己修復の機能を提供。



世界最高レベルの安全性を誇るビジネス向けPC[4]ならではの、*内蔵型*のハードウェア/ファームウェア セキュリティ

使用中のデバイスを保護する機能の例：

- **Dell SafeBIOS**のオフホストのBIOS verification*、 Indicators of Attack* 、CVE検出*が、悪意ある活動をパソコンへの侵害が発生する前に検出できるよう支援。
- **Dell SafeID**が、専用のセキュリティ チップにユーザー資格情報を安全に保管。*
- **オフホストのファームウェア検証**が、高い特権があるファームウェアの整合性を保護。*
- **Dell Trusted Deviceアプリケーション**を使用して、デバイスのテレメトリーを業界をリードするソフトウェアに統合し、環境全体のセキュリティを向上。*

初回起動時からPCの安全性を保証するうえで役立つ、*組み込み型*のサプライ チェーン セキュリティ

- Dell Secured Component Verification* (SCV)などの**Dell SafeSupply Chain**のアドオンが、製品の整合性をより確実に保証。

** Dell独自の機能*

すべての対策を統合するDellのソリューション

ハードウェアとソフトウェアの両方を保護する対策を実装すれば、一般的な攻撃を阻止するうえで役立つ防御機能により、攻撃対象領域を縮小できます。

検出と対応の機能は、見逃される可能性があるステルス攻撃への対処を可能にします。

4ページで紹介したサプライ チェーン攻撃の場合、Dellの支援を活用することで、**セキュアなサプライ チェーン プラクティス**などの防御策を利用して、キル チェーンの早期段階で攻撃を阻止できます。攻撃が見逃されてしまった場合も、**SCV**などの追加の防御策によって対処されます。

ソーシャル エンジニアリング攻撃の場合、ユーザーが攻撃者に騙されて有効な資格情報を提供したとしても、**SafeIDなどのハードウェアベースのユーザー検証**により、攻撃者を阻止して、より広範な領域へのアクセスができないようにします。**次世代型セキュアWebゲートウェイ**などのセキュリティ ソフトウェアは、モニタリングおよび保護の追加のレイヤーを提供します。

コンポーネントの改ざんから開始される**ハードウェア サプライ チェーンへの攻撃に対する対策**

攻撃者はPCの出荷時に侵害し、ハード ドライブを改ざんします。

- **セキュアなサプライ チェーン プラクティス**
- 改ざん防止措置を施した梱包
- ドア ロック

組織のIT部門は、侵害されたデバイスを組織全体に導入します。

- Secured Component Verification (SCV)
- ランタイムの検証

攻撃者はマルウェアをインストールし、ユーザーがログインした際に資格情報を窃取します。

- クラウド アクセス セキュリティ ブローカー
- 次世代型セキュアWebゲートウェイ

フィッシング メールから開始される**ソーシャル エンジニアリング攻撃に対する対策**

エンド ユーザーがフィッシング メールに騙され、偽造されたWebページに誘導されて資格情報を提供します。

- NGAV
- EDR
- XDR

攻撃者はこの正当な資格情報を使用して、ネットワークに遠隔でアクセスします。

- **SafeIDによる多要素認証**
- ゼロトラスト ネットワーク アクセス

攻撃者はWebサービス経由でデータを引き出し、窃取したデータを暗号化して身代金の要求に利用します。

- Next-Gen Secure Web Gateway + ユーザーとエンティティの行動分析

重要ポイント

侵害は避けられない現実です。効果的なエンドポイント セキュリティでは、最悪のシナリオを常に想定し、デバイス、ネットワーク、クラウドのどの場所で発生するかにかかわらずキル チェーンの遮断に注力します。

単独のソリューションでは、攻撃を100%ブロックできません。ハードウェア保護策とソフトウェア保護策を組み合わせることが、最善の防御方法です。

セキュリティはサプライヤーに大きく左右されます。自社が提携するサプライヤーに、各自のセキュリティ施策の概要を提示するよう求めましょう。

Latitude
ノートPCおよび
2-in-1 PC

詳細はこちら：

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

Dellをフォロー：LinkedIn @DellTechnologies | X @DellTech

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。**豊富な経験を持つセキュリティ/テクノロジー パートナーと提携すれば、エンドポイント セキュリティをモダナイズできます。**

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が独自に提供する、ハードウェアおよびソフトウェア保護の包括的なポートフォリオで、攻撃対象領域を縮小しましょう。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継続的な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ビ環境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。