Dell NativeEdge

保護：ゼロトラスト セキュリティで安心の運用

表目次

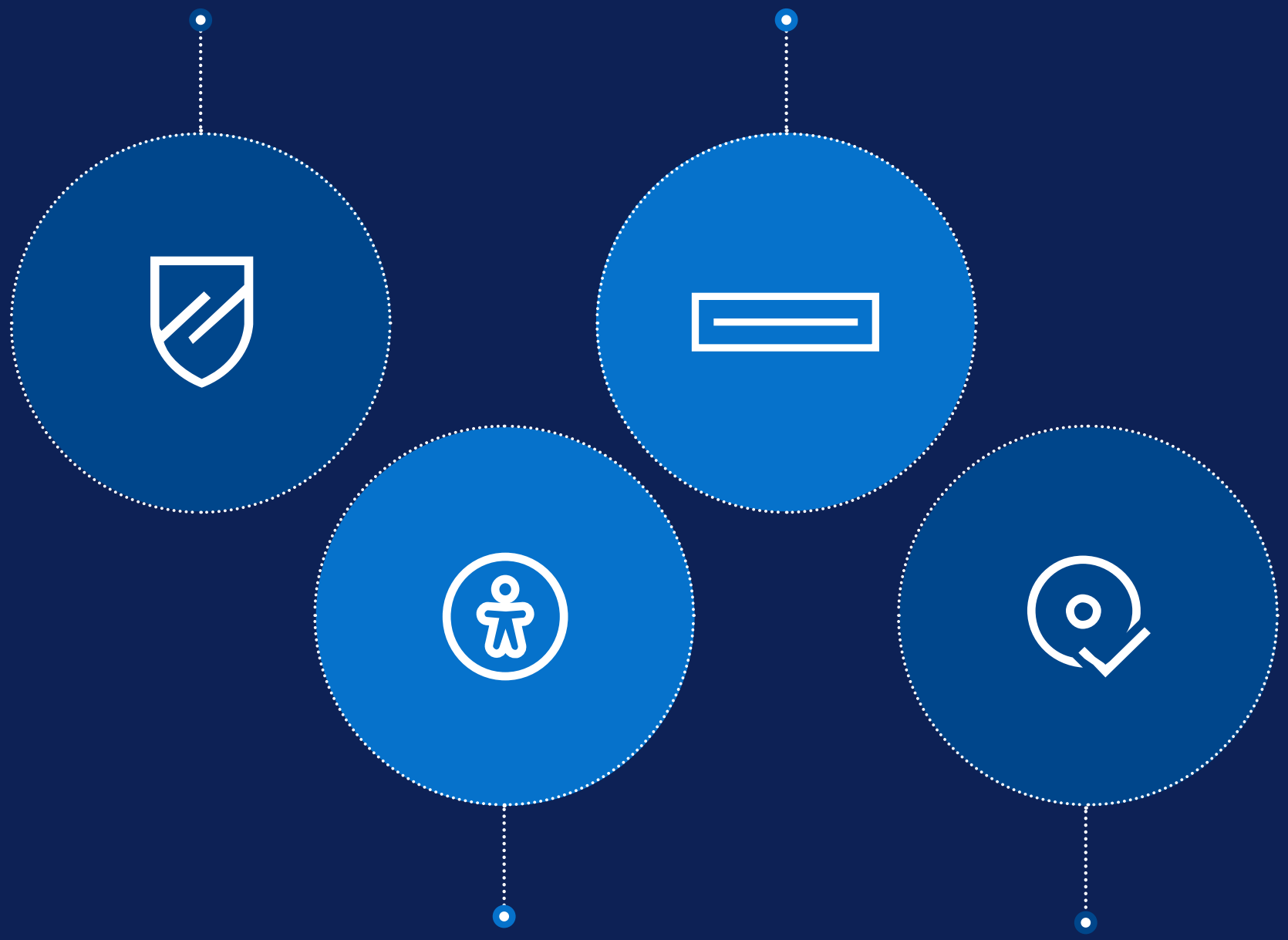
分散環境全体のセキュリティ

急速に変化する顧客の好みや市場のダイナミクスに対応するために、組織は新しいアプリケーション、アップデート、コンピューティング インフラストラクチャを比類のない量と速度で導入しています。データ、インフラストラクチャ、アプリケーションの急増により、これらの新しいテクノロジーが存在する分散環境を保護することがますます重要になっています。企業が運用を拡大するにつれ、物理デバイスの改ざんやデータのハッキングなどセキュリティ リスクに対する脆弱性が高まります。さらに、これらのシステムでは機密性の高い個人データを処理することが多く、企業が顧客を保護する責任も増すことになります。

運用を保護するために、企業が実施すべき事項

分散した場所に導入されたインフラストラクチャの物理的な安全性の確保

デバイスの改ざんを検出し、脅威を修復



あらゆるレベルでのユーザー アクセス制御

数千台のデバイスへの、プロビジョニングとソフトウェア アップデートの拡張

Dell NativeEdge

あらゆる場所でイノベーションを実現

エッジと分散型データセンター全体における多様なインフラストラクチャとアプリケーションの導入、オーケストレーション、ライフサイクル管理を、セキュリティを維持しながら一元化する、エンドツーエンドのフルスタック ソリューションです。

ゼロタッチ オンボーディング、ゼロトラスト セキュリティ、高度なワークロード オーケストレーションなどの機能により、エッジおよび分散型データセンター環境をシンプル化、最適化し、保護します。NativeEdgeは、KVMハイパーバイザーとコンテナのランタイムを活用して、組織が仮想マシン(VM)とコンテナの両方を導入および管理できるようにします。AIワークロードとフレームワークのオーケストレーションを行うよう最適化されており、AI主導型アプリケーションの導入と管理が、エッジおよび分散型データセンター全体でシームレスに行えるようになります。また、NativeEdgeはどのようなハードウェア環境にも適応でき、Dell PowerEdgeサーバーからデスクトップやサードパーティー インフラストラクチャまで、さまざまなフォーム ファクターで幅広いオプションをサポートします。

Dell NativeEdgeは、運用の複雑さ、拡張性、セキュリティなど、分散環境固有の課題に対処するように設計されています。エッジ コンピューティングのパワーを活用しながらコストを削減し、効率性を向上させることに重点を置いた、現代の組織向けにカスタマイズされたソリューションです。

シンプル化
成果を加速し、
運用を一元化

1分
未満でインフラストラクチャと
アプリケーションを導入可能[1]

最適化
シームレスな仮想化と
拡張性のあるAIを構築

エッジアプリケーションオーケストレーションの自動化で時間を最大
68%
短縮[1]

保護
ゼロトラスト セキュリティで
安心の運用

世界で
最も安全な
エッジ運用[2]

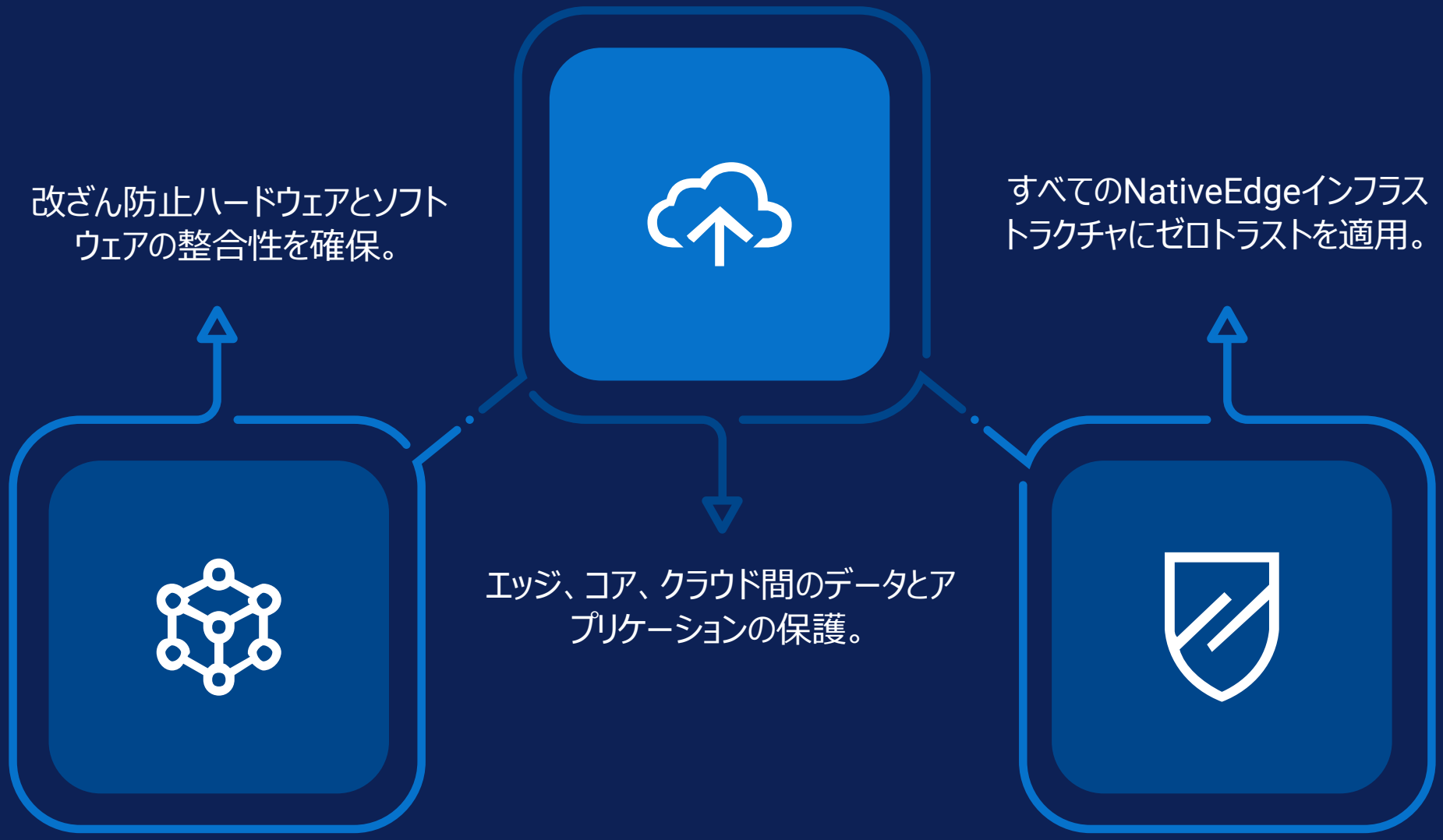
[1] Enterprise Strategy Group by TechTarget Technical Validation（デル・テクノロジーズより委託）『Dell NativeEdge - Edge Operations Software Platform』（2025年2月）。

[2] デル・テクノロジーズの社内分析（2025年5月）に基づきます。

Dell.com/NativeEdge

IT部門の介入なしに、インフラストラクチャ、アプリケーション、データ、ネットワーク、ユーザーのセキュリティを永続的かつ自動的に強化することで、分散した運用の拡大を保護します。

Dell NativeEdgeは、次の手法で分散した運用を保護します。



ゼロトラスト セキュリティを強化

現代の企業は、地理的に分散したすべてのサイトで数千のアプリケーションを管理する責任を負っており、多くの場合、異機種混在のインフラストラクチャに依存しています。これにより、管理が非効率的で、セキュリティ保護が困難な、アップデートに時間がかかる複雑に交錯したテクノロジー サイロが発生します。組織が分散した場所に新しいアプリケーション、新しいセンサー、新しいデバイスを導入し続けるにつれて、潜在的なサイバー脅威の攻撃対象領域が拡大します。

企業は、分散データ運用の継続的なセキュリティをどのように確保できますか？

Dell NativeEdgeは、ゼロトラスト セキュリティの基盤で、自信を持った運用を後押しします。デバイスの電源がオンになった瞬間から、UEFIセキュア ブートや仮想Trusted Platform Module (vTPM)などの機能を使用して、デバイスの整合性を確保し、ハードウェアに根ざした信頼のチェーンが確立されます。NativeEdgeは、GDPRやその他のグローバルなデータ主権の要件をサポートしており、分散環境に安心感をもたらします。このアプローチとゼロトラスト マイクロセグメンテーションなどの機能の組み合わせにより、アプリケーションとデータが保護されるため、作業の場所を問わず安全にイノベーションを起こすことができます。

ゼロトラストのセキュリティ

デバイスの信頼性

ユーザーの信頼性

転送とセッションの信頼性

データの信頼性

ソフトウェアの信頼性

可視性と分析

自動化とオーケストレーション

セキュリティ体制は、リソースのすべてのアクションを監視して理解することで、さらに強化されます。これを可能にするのは、関連するビジネス管理、一元化されたコントロール プレーン、およびセキュリティ体制のために明確に機能するインフラストラクチャです。NativeEdgeのゼロトラスト設計原則を利用すれば、企業は分散型の運用を拡大するにあたり、接続されているあらゆるリソースの整合性の証明と検証を継続的に得られるため、安心できます。

サプライチェーンとそのライフサイクルを通じてハードウェアの整合性を確保

グローバルな店舗や工場の拠点を持つ小売業者やメーカーの例を見ると、場所に応じて仕様やプロファイルが異なる多様なハードウェアの管理と保護は、ますます困難になっています。時間の経過とともに、これらのデバイスは継続的に検証されなくなり、長期的なコンプライアンスは実証できなくなります。これらのデバイスの分割払いに複数の関係者が関与すると、リスクは急激に増大します。

分散インフラストラクチャを一貫して保護するにはどうすればよいでしょうか？

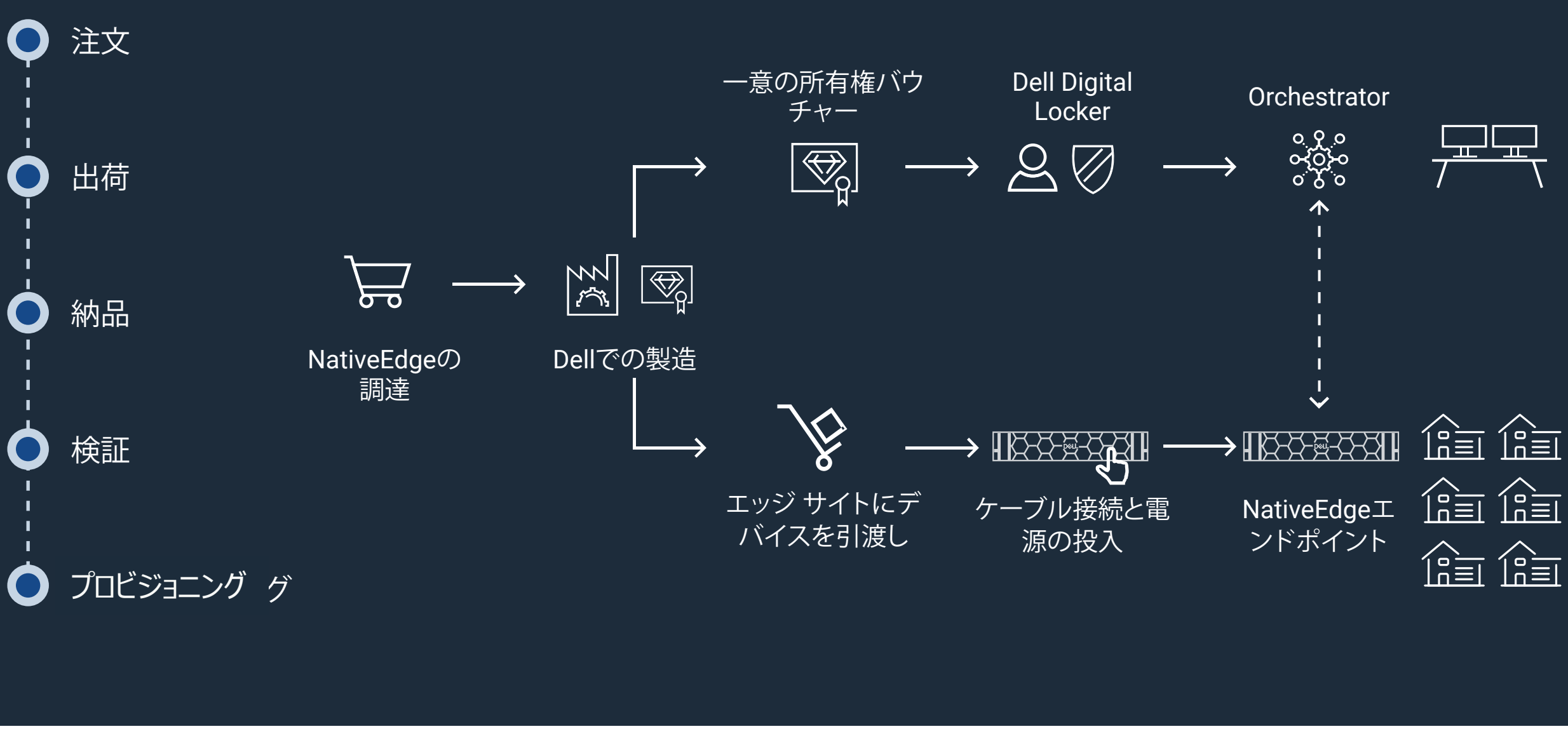
インフラストラクチャの保護は当社の工場から始まります。NativeEdgeエンドポイントは、暗号化セキュリティとSecured Component Verification (SCV)によって保護され、信憑性を保証します。これにより、FIDOデバイス オンボーディング(FDO)を使用した安全なゼロタッチ導入プロセスが可能になります。任意の場所でデバイスの電源がオンになると、その整合性が自動的に検証され、手動による介入なしで安全な管理チェーンが確立されます。これにより、インフラストラクチャが初日から安全であることを保証しながら、運用を拡張できます。

NativeEdgeエンドポイントは、NativeEdgeとの互換性を持つよう最適化されており、Dellの工場出荷時には暗号形式のセキュリティで保護されています。

NativeEdgeは、Secured Component Verification (SCV)プロセスを活用して、ハードウェア コンポーネントの信頼性と整合性を確保します。NativeEdgeはSCVを通じて、サプライチェーンの整合性、コンポーネント検証、ファームウェア検証、セキュア ブート プロセス、暗号署名を適用し、不正アクセスや改ざんから保護します。

これらのデバイスがFIDOベースのデバイス オンボーディング プロセスを経ると、整合性が自動的に認証され、Dellの工場での製造から導入サイトでの受領と設置までのセキュリティが確保されます。ハードウェアが何らかの方法で改ざんされた場合、プラットフォームは自動的にハードウェアを隔離し、不正な要素から操作を保護します。

セキュアなデバイス オンボーディング とゼロトラスト フレームワーク

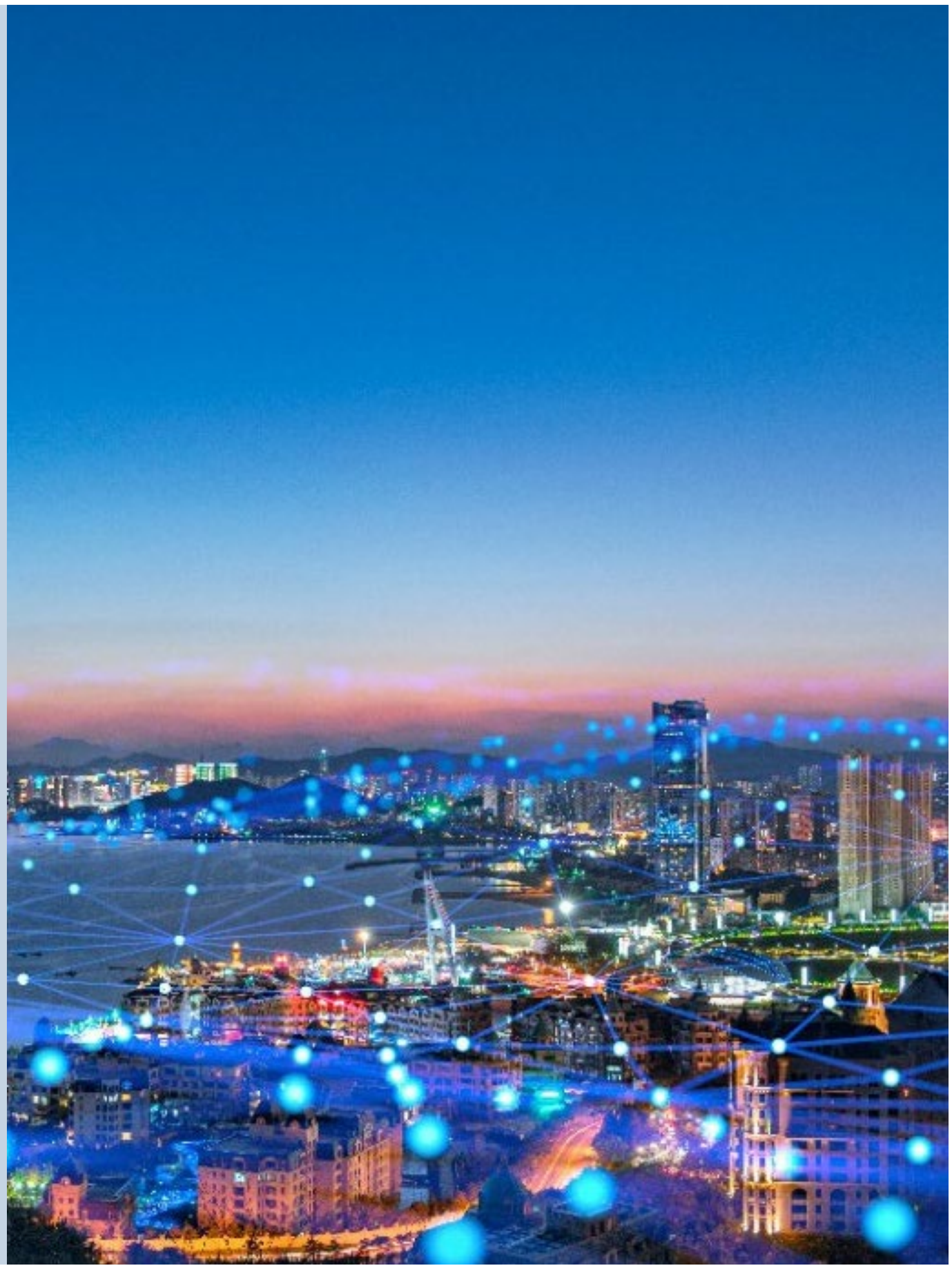


エッジからクラウドまで、データやアプリケーションを保護

グローバルな小売業者の例を考えてみましょう。小売環境の多様性と分散性により、アプリケーションやワークロードにアクセスするユーザーのIDが常に検証されるとは限らない状況が生じます。その場合、状況はその環境に対してローカルなものであり、一元的に表示して監査することはできません。

さらに、小売業者で、導入されたアプリケーションのソフトウェア サプライチェーンを可視化できることはほとんどありません。これらは多くの場合、マネージド サービス プロバイダー(MSP)によって処理され、これらのアプリケーションの忠実度の自動チェックが表示されない場合があります。これらのアプリケーションは、多くの場合、同じMSPによって最初に構成されますが、時間の経過とともに構成が変化する可能性があります。そのため、ステークホルダーはセキュリティ ポリシーに対するアプリケーションのコンプライアンスを判断できません。

メーカーの場合、運用テクノロジー(OT)チームは通常、さまざまなアプリケーション ワークロードを実行します。これらのアプリケーションの一部は、PLCなどの機器とインターフェイスし、内部の可視性を持たない独自のアプリケーションです。



ITネットワークの機能は、論理的に分離されているOTネットワークには引き継がれません。その結果、製造元のOTネットワーク内のインフラストラクチャとアプリケーション ワークロードは、安全なOT環境を実現するために必要なレベルのネットワーク セキュリティ制御にアクセスできません。アプリケーションとデータ セキュリティに関連する同様の課題は、すべての業界で共通しています。

Dell NativeEdgeは、組織がデータ ソースからローカルまたはクラウドで実行されているアプリケーションまでのデータパイプラインを保護できるよう支援します。暗号化、ユーザー アクセス制御、アプリケーション ブループリントカタログ、ネットワーク セグメンテーション、セキュリティ オーケストレーションなどの高度なセキュリティ対策を組み合わせています。NativeEdgeはまた、テレメトリーと分析を使用して、分散した場所のセキュリティ体制をプロアクティブに評価します。これにより、監査能力を備えたエキスパートが各サイトを訪問する必要がなくなります。

高度なセキュリティ対策

高度なセキュリティ対策で耐障害性の高い運用を確保

ユーザー アクセス制御

NativeEdgeは、ロールベースのアクセス制御(RBAC)を提供し、ユーザーの役割と責任に基づいてアクセスレベルを解析します。デバイスと導入されたアプリケーション ワークロードのユーザーは、アクセス セッションごとに検証され、IDとアクセス管理を通じて一元的かつ可視的な方法で証明されます。

ネットワーク区分化

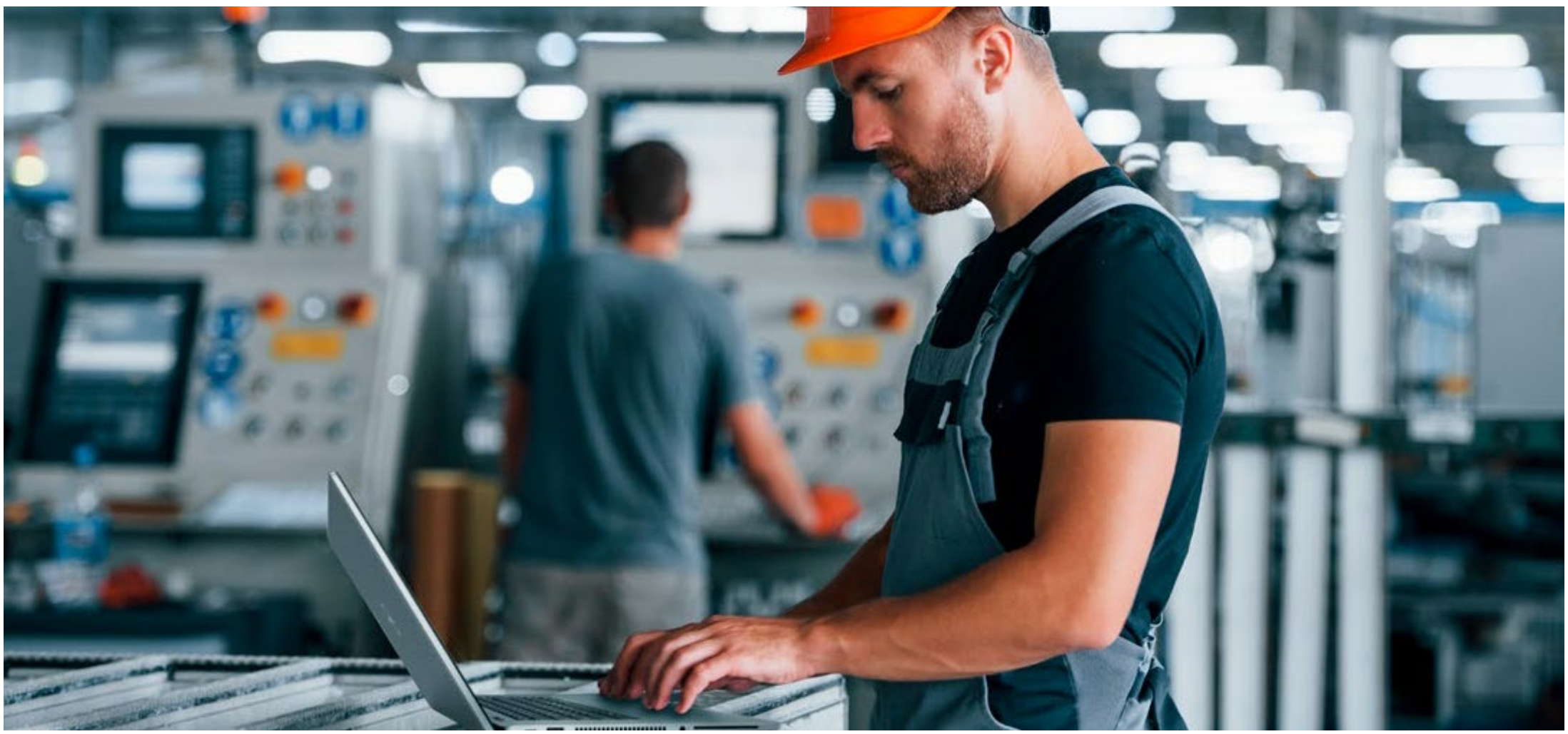
アプリケーションのネットワークをマイクロセグメント化することで、これらのアプリケーションをターゲットとするポリシーを簡単に開発および管理して、セキュリティを強化できます。このアプローチにより、仮想化環境内での潜在的な侵害のリスクと脅威の横方向の移動が軽減されます。

アプリケーション ブループリントのカタログ

NativeEdgeは、アプリケーションの安全性を高めるように設計されています。その基盤となるのは、ブループリントを使用してアプリケーションを導入するためにカタログに依存する、安全なソフトウェア サプライチェーンです。カタログは、独立系ソフトウェア ベンダー(ISV)のアプリケーションを導入するためのブループリントや、企業が開発したDellの事前検証済みブループリントがまとめられたもので、すべてが安全なソフトウェア サプライチェーンの維持を目的としています。これらのブループリントは、TOSCA標準とYAML形式に基づいており、多くのエッジ デバイスで同時に実行されるアプリケーションとAIフレームワークの導入を自動化します。NativeEdgeを使用すると、導入されたアプリケーションのプロアクティブなセキュリティ制御をきめ細かく設定し、アプリケーションを一貫して導入し、セキュリティ ポリシーに沿って調整することができます。最後に、アプリケーションワークロードは、NativeEdgeエンドポイントまたはマルチクラウド環境でVMおよびコンテナとして実行でき、NativeEdgeによって一元的に管理されます。

データの暗号化と保護

NativeEdgeは、データの状態（静止中、転送中、使用中）を問わず、侵害や不正アクセスからデータを保護します。NativeEdgeは、連邦政府のコンプライアンス基準を満たす堅牢な静止データ暗号化(DARE)を提供し、保存されたデータを暗号化し、物理的な盗難や改ざんから保護します。NativeEdgeは、ゼロトラスト セキュリティ原則ですべてのデータリソースを管理し、厳格なアクセス制御を実施して、アクセス制御を継続的に証明および検証します。これにより、エンタープライズ アプリケーションのデータの整合性が保護されるだけでなく、すべてのビジネス ステークホルダーの信頼も高まります。



セキュリティ オーケストレーション

不正なアクション/イベントは、多くの場合、気付かれずに発生し、多くの場合、修復されません。このため、手動プロセスによるリスクが発生し、優先度の高いビジネス タスクが後回しにされがちです。さらに、IDアクセス管理(IAM)/ロールベースのアクセス制御(RBAC)、コントロール プレーンに関するIT統合にもさまざまなバリエーションがあります。

これにより、セキュリティ オーケストレーションが途切れ、しばしば各サイトで個別の管理が行われます。OTの多くの事例では、これらのデバイスはマシンツーマシン(M2M)環境にあり、ユーザーは認識していません。これらの環境では、一元的なオーケストレーションが不可欠です。

NativeEdgeは、エッジ環境全体で一貫したセキュリティ オーケストレーションを実現します。エッジ環境で発生するアクションとイベントの集計に基づいて、セキュリティ体制の統合ビューを提供し、すべてのサイトで一元的な認証と一貫性のあるポリシー適用を可能にします。IAMおよびRBAC機能の使用により、最小権限の原則に基づくプラットフォームの安全な管理が可能になるため、企業が求める高粒度がもたらされます。また、ログと構成管理を自動化することで、GDPR、PCI、HIPAAなどの規制へのコンプライアンスをシンプルにします。これにより、ガバナンス、リスク、コンプライアンス(GRC)やセキュリティ運用(SecOps)のルールを組み込むことが可能になるため、あらゆる環境で自信を持って運用できます。

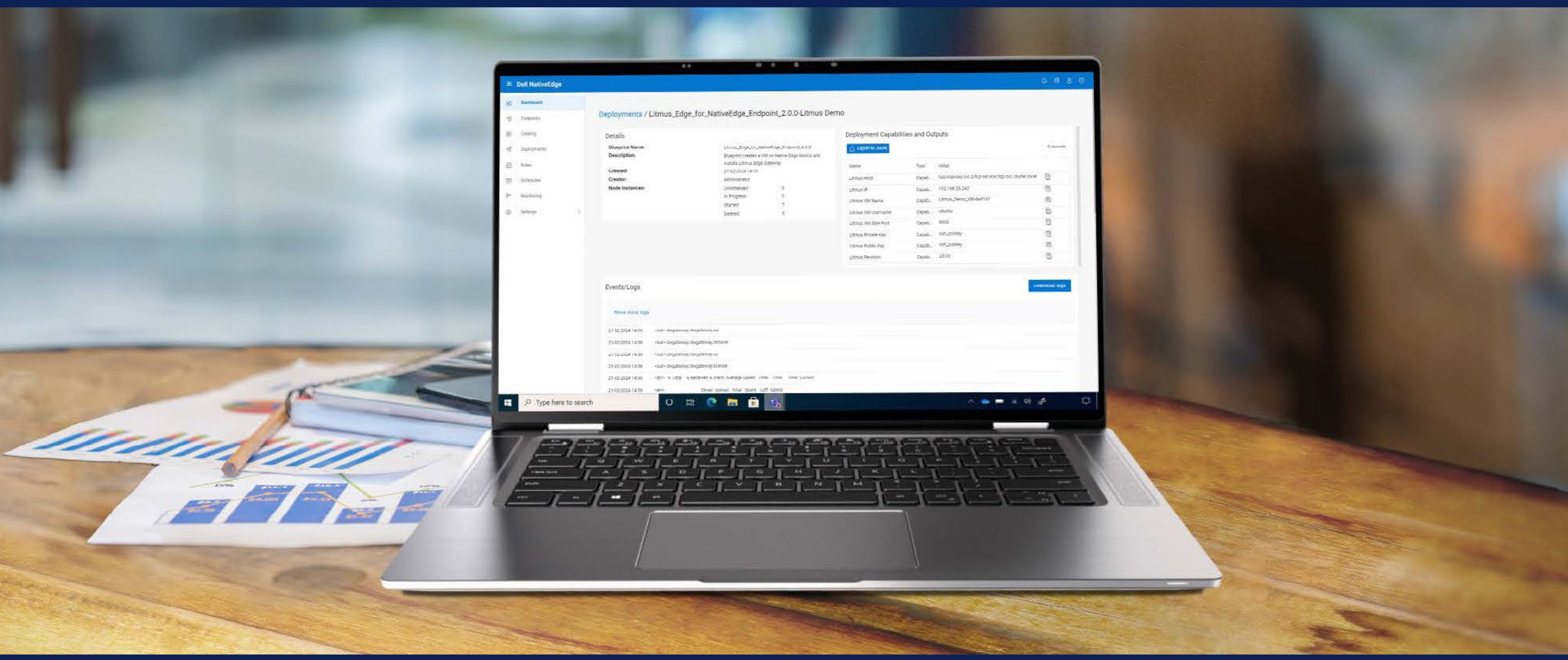
テレメトリーと分析

NativeEdgeは、ハードウェアと運用環境からのテレメトリーに依存して、定義されたコンプライアンス基準に沿ってセキュリティ評価を継続的に実施します。これらは、構成のドリフト検出、構成ミス、セキュリティ アップデートの必要性を判断するために使用されます。

エッジ資産を保護

Dell NativeEdgeは、FIDOベースのセキュアなデバイス オンボーディングと強化された安全なNativeEdge OSを組み合わせるなどのゼロトラスト セキュリティ原則でエッジ資産を保護します。Dell NativeEdgeの使用により、インフラストラクチャ、ユーザー、ネットワーク、アプリケーション、データが分散した場所全体で継続的に検証され確認されていることを保証できます。

あらゆる場所でイノベーションを実現



DELL Technologies

詳細はこちら：**Dell.com/NativeEdge**