信頼のパートナーシップ:
Dell サプライチェーン セキュリティ

© 2023 Dell Inc.

DELL Technologies

目次

サプライチェーンのセキュリティが重要な理由

情報技術は、よりつながりのある世界を創造しており、私たちの生活のあらゆる側面におけるテクノロジーへの依存度は増え続けています。しかし、このつながりを支える先進技術と高度な物流ネットワークは、前例のない攻撃に直面しており、成長、繁栄、国際関係の基盤である信頼を損なうリスクをはらんでいます。さらに事態を複雑にしているのは、攻撃の複雑さ、高度化、および潜在的な影響が、時代とともに大幅に増大している点です。

たった一度のランサムウェアインシデントが、業務の中断、収益の損失、データ漏洩、生産性の低下、ブランドや企業の評判を傷つける可能性があります。これらの理由でお客様は当然、購入するテクノロジー製品が改ざんや悪意ある変更を受けておらず、それらのデバイスで保存および処理するデータの保護能力が損なわれていないことの保証を求めています。

Dell は従業員、お客様、サプライヤー間の信頼のパートナーシップによるビジネスモデルを構築しています。

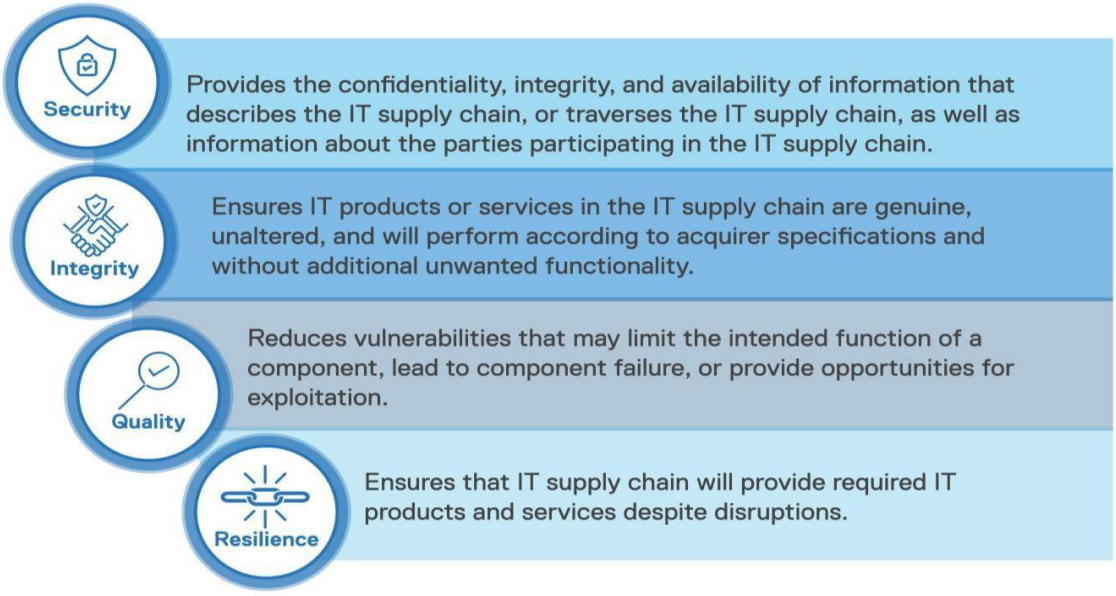
ITハードウェアのセキュリティとその生産と供給を担うサプライチェーンのセキュリティは、かつてないほどお客様の関心の中心にあります。Futurum社による「ハードウェアセキュリティの旅をナビゲートするための4つの鍵」では、44%の組織が過去12か月間に少なくとも1回、ハードウェアレベルまたは BIOS 攻撃を受けたと述べており、ITハードウェアのセキュリティ確保が優先事項となっています。

これらの理由により、デル・テクノロジーズは世界最高水準のサプライチェーンセキュリティ対策の構築と維持に注力しています。安全で信頼できる環境は、サプライチェーン エコシステムのセキュリティを高めながらシステミックリスクを軽減します。Dell は、この環境を念頭に置き、社員、お客様、サプライヤー間の信頼のパートナーシップを通じたビジネスモデルを構築しました。上流から下流まで、多様なサプライチェーンの基盤における主要な利害関係者との双方向の協力により、俊敏性、誠実さ、独創性を活かしながら、お客様に最高の価値とテクノロジーを提供することができます。

Dell のサプライチェーン

Dell は、サプライチェーンを保護しお客様が信頼できるソリューションを提供するための包括的なアプローチを採用しています。「多層防御」と「広域防御」という戦略には、サプライチェーンに持ち込まれる可能性のある脅威を軽減するために、何重もの制御層を設けています。これらの制御的措置と効果的なリスク管理を組み合わせることで、サプライチェーンのセキュリティを確立します。

サプライチェーンの各フェーズで実施すべき制御措置を決定する際に、Dell が重視するいくつかの能力があります。それは、セキュリティ、完全性、品質、および回復力です。



Dell のサプライチェーンにおけるセキュリティ

サプライチェーン セキュリティとは、物的資産、在庫、情報、知的財産、および人材を保護するための、予防的および検知的な管理措置の実践と適用です。情報、人的資源、物理的セキュリティに対処することで、マルウェアや偽造部品がサプライチェーンに悪意を持って持ち込まれる機会を減らし、サプライチェーン セキュリティを確保することができます。

Dell は、多面的なアプローチを採用してサプライチェーンを保護し、信頼できるソリューションを提供しています。デスクトップ、ノートパソコン、サーバー、データストレージアレイのいずれにおいても、製品の特徴はサプライチェーン セキュリティを最優先事項として、構想、設計、試作、実装、生産、導入、維持、および検証されています。

データの保護

サプライチェーン内のデータを保護することは、デジタルデータが不正アクセスや使用によって漏洩、悪用、削除または破損するのを防ぐために使用される実践、ポリシー、および原則を含みます。これには、情報セキュリティ、人的セキュリティ、および物理的セキュリティが含まれます。

Dell は、革新的な手法を取り入れてデジタルデータを保護し、強固な管理および物理的制御を確立し、多層的なアクセスプロトコルを維持することで機密性の高いお客様データを保護しています。当社のデータガバナンスの取り組みは、関係性とセキュリティの姿勢を最適化し、プロアクティブに脆弱性を特定し、リスクを軽減することに焦点を当てて構築されています。お客様データの機密性、完全性、可用性を保護するために、エンドツーエンドのバリューチェーン全体に信頼と保証を提供しています。当社は、デジタルデータや他のお客様に関する機密情報を保護するために、エンドユーザーの機能に対する影響を最小限に抑える方法で特別な措置を講じています。

情報セキュリティ

Dell は日常業務の過程で、サプライチェーンライフサイクル全体にわたって製品、ソリューション、サプライヤー、およびパートナーに関する情報を収集し利用しています。機密情報を漏洩や悪用から防ぐための様々な対策が講じられています。例えば、Dell とパートナー間のデータ転送には、暗号化方式とプライベート通信チャネルの組み合わせが使用されています。適切な場合には、業界のベストプラクティスに従って、安全なプロトコルとカプセル化技術も使用されます。また、生産ラインは情報の転送機能を管理できるよう設計および構築されています。

Dell の社内ネットワーク環境と関連資産は、ウイルス検出、強力なパスワードの強制、E メール添付ファイルのスキャン、システムやアプリケーションのパッチ適用コンプライアンス、侵入防止およびファイアウォールなどの制御を通じて保護されています。また、マルウェアや資産の誤用に対する追加的な制御も実施されています。

また、当社はサプライチェーン全体にわたる主要な管理指針として、NIST (米国国立標準技術研究所) の「職務分離」と「最小権限」の原則を採用し、事業全体でのデータアクセスの誤用・悪用を防いでいます。これらの原則によって、機密情報へのアクセスは、特定の個人が職務を遂行するのに必要な範囲でのみ許可されることが保証されます。

人的セキュリティ

社内のセキュリティ対策が効果的であることを保証するために、従業員を対象にスクリーニングを行い、会社のデータ、資産、リソースへのアクセス、使用、操作を制限することが必要です。Dell の方針では、契約先のサプライヤーを含むサプライチェーン全体の従業員に、雇用前の適性スクリーニングプロセスが義務付けられています。これには、法律で許容される範囲のセキュリティ バックグラウンドチェック、薬物検査、身元確認、応募情報の確認が含まれます。

Dell の従業員にはセキュリティの文化があり、年次のセキュリティ意識とコンプライアンスのトレーニングを受ける必要もあります。このトレーニングは、サプライチェーン全体で製品を危険にさらす可能性のある行動のリスクを軽減することを目的としています。当社の従業員は、コーポレートニュースレター、社内外のセキュリティ Web サイトやホワイトペーパー、セミナーや企業のセキュリティ意識向上キャンペーンへの参加、さらに追加のビデオ講座の受講などにより、年間を通してセキュリティの最新動向を常に把握するよう奨励されています。また、社員も業務委託社員も、知的財産、お客様情報、その他の機密データの保護に同意する、在職中および退職後も含めた秘密保持規定への署名が必須とされます。

物理的セキュリティ

Dell 製品を設計、製造、カスタマイズ、または製造する施設は、輸送資産保護協会 (TAPA)、米国産業セキュリティ協会 (ASIS)、国際標準化機構 (ISO)、Business Alliance for Secure Commerce (BASC) など、国際的に認められた物理セキュリティ基準に準拠していることを証明する必要があります。

Dell は、デジタル閉回路TVカメラの使用、入退室管理システム、侵入検知、および警備サービスプロトコルなど、様々な面でサプライヤーと施設を監査しています。さらに、輸送・物流プロセス中の貨物を保護するため、改ざん防止パッケージ、貨物ロックとシール、主要な貨物ルートの脅威インテリジェンスの監視などの管理措置も適用しています。一部の貨物には IoT 追跡デバイスも導入されており、リアルタイムのテレメトリデータ監視を可能にし、輸送中に観察されるセキュリティ違反のエスカレーションを行います。

Dell は、米国 税関・国境警備局のC-TPAT (テロ防止のための税関産業界提携プログラム) の Tier 3 ステータス、カナダのPIP (Partners in Protection)、シンガポールの Secure Trade Partnership、複数国での Authorized Economic Operator (AEO) ステータスなど、安全な貿易および商取引プログラムにおける認証を維持しています。これらは、世界税関機構 (WTO) の加盟国により国際的に認識されており、民間企業での「最高水準」のサプライチェーン セキュリティを示しています。これらのプログラムは、サプライヤーの説明責任、セキュリティ管理ポリシー、密輸対策、取引管理および改ざん防止に重点を置いており、国際国境を越えた貿易の安全維持を目的とします。

Dell のサプライチェーンの健全性

サプライチェーンの完全性は、お客様の製品が安全に配送され、受け取った後に意図した通りに動作することを確保します。サプライチェーンの完全性の重要な特徴は、ハードウェアとソフトウェアの基本仕様を安全に保存し、後に不正な変更が行われていないことを検証するための参照先に使う点です。

ハードウェアの健全性

Dell はサプライチェーンに偽造パーツが侵入するリスクを最小限に抑えるための、様々な品質管理プロセスを活用しています。新製品の導入プロセスでは、部材が認定ベンダーのみから調達され、部品表と一致することが確認されます。各パーツは ODM (相手先ブランド製造業者) や OCM (相手先ブランド部品製造業者) から直接調達します。

Dell の品質管理システムは、認定ベンダーからの調達を含め、エンジニアリング仕様およびプロセスへの継続的な準拠を検証します。生産中の部材検査では、不当なマーキング、通常の性能パラメータから逸脱した部品、誤った電子識別子を含む部品の特定に役立ちます。

適切なトレーサビリティを実現するために、全ての主要部品は、製造プロセス中にキャプチャできるシリアル番号ラベルやマーキング、Dell が規定する PPID (Piece-Part Identification) ラベル、または電子識別子により固有に識別されます。PPIDは、SCV (Secured Component Verification) など、Dell が提供する下流のコンポーネント検証機能の基礎となります。さらに、Dell は世界中の全ての製造拠点での品質管理プラクティスに関する ISO 9001認証を維持しています。これらのプロセスの制御と遵守により、Dell 製品内に偽造部品が埋め込まれるリスクを最小限します。

ソフトウェアの健全性

ソフトウェア エンジニアリングのベストプラクティスは、OS、アプリケーション、ファームウェア、デバイス ドライバーなどのあらゆるコードの開発プロセス全体への、セキュリティの統合です。Dell が開発するソフトウェアに統合されるサード パーティ コンポーネントは、信頼できるサプライヤーから入手され、その健全性は統合前に検証されます。Dell は、セキュア開発ライフサイクル (SDL) を設計および開発プロセス全体に統合し、ソフトウェアのセキュリティ上の欠陥が悪用される機会を減らしています。これらの対策は、SAFECode ガイドライン[1] および ISO 27034[2]とも密接に連携しています。

ライフサイクル全体でのプロアクティブな検証、妥当性確認、およびセキュリティ テストの実践は、ソフトウェアの安全性を確保し、マルウェアやコーディングの脆弱性がソフトウェアに挿入される可能性を減らすのに役立ちます。堅牢なサイバーセキュリティ プログラムは、ソースコードへの不正アクセスを防止し、製品がお客様に出荷される前にマルウェアが導入される可能性を最小限に抑え、ソフトウェアの完全性を向上させます。

Dell は、ソフトウェア サプライチェーン セキュリティ管理の一環、および米国大統領令 14028号 と NIST 基準に準拠する形で、製品ポートフォリオ全体にわたって一部の製品の SBOM (ソフトウェア部品表) データを提供します。Dell の SBOM データは Software Package Data Exchange (SPDX) 標準に準拠しており、JSON形式で提供されます。SBOM データは、堅牢なソフトウェア サプライチェーンの透明性と迅速な脆弱性スキャンおよび対応が可能となり、ゼロトラスト アーキテクチャの重要な要素となっています。

設計と開発

ハードウェア、およびハードウェアが設計されたとおりの機能を果たすためのソフトウェア コードの設計・開発において、Dell は「Intrinsic Security (イントリンシック セキュリティ) 」を実践しています。この実践は、セキュリティ機能をハードウェア製品とソフトウェア製品の開発時点で実装し、それが開発サイクル全体で継続されるためのプロセスとポリシーを含みます。要するに、「組み込まれた」セキュリティです。この実践を効果的に実行するために、当社の開発エンジニアは、コードを取り扱う前に必ずセキュリティ トレーニングを受けることが義務付けられています。また、各開発チームにセキュリティ チャンピオンが任命され、組織内でセキュリティ文化が推進しています。

Secure Development Lifecycle

Dell のセキュア開発ライフサイクル (SDL) は、業界標準とベストプラクティスに基づいています。このプログラムには、当社の製品チームが製品開発ライフサイクル全体を通じて安全なコードを生成するために実施する、セキュリティ管理の包括的な項目も含まれます。アプリケーション セキュリティの ISO 27034に準拠した SDL プログラムに加え、当社は、SAFECode[3]、BSIMM (Building Security in Maturity Model) 、および IEEE の Center for Secure Design など多くの業界標準団体と協力して、自社の SDL 制御が業界のベストプラクティスと密に連携するようにしています。

Dell の SDL は、特定の主要なリスク領域に対する分析活動と、規範的な予防策の両方を含みます。脅威モデリング、静的コード分析、脆弱性スキャン、セキュリティテストなどの分析活動が統合され、開発ライフサイクル全体で数千の潜在的なセキュリティリスクや脆弱性を、より効果的に特定して修正します。SDLは、ソフトウェアや Web アプリケーションにおける多くの一般的な設計上の弱点を緩和します。例えば、認証されていないコードの更新、公開または有効化されたデバッグインターフェース、安全でないデフォルト設定、およびハードコードされたパスワードなどです。Dell の SDLは、業界や官民のパートナーシップによって開発されたツールを活用しています。これらのツールは、コード内で時間の経過とともに発見される、新規や既知の弱点や脆弱性を特定して対処します。これには、MITRE が公開している CVE (Common Vulnerabilities and Exposures)[4] 、CWE (Common Weaknesses Enumeration)[5] 、OWASP (Open Web Application Security Project) の Top 10[6] 、SANS のTop 25 Most Dangerous Software Errors[7] などが該当します。

Dell の SDL プログラムは、全てのソフトウェアとファームウェアの設計とテストを管理します。エンジニアが新しい機能を設計し始めるとき、彼らは SDL によって定義された厳格な手順に従うことが求められます。これにより、プロプライタリのコードとサードパーティのコンポーネントの両方で脆弱性が防止されます。製品設計時、エンジニアリングチームは脅威評価とモデルを作成し、脅威対象領域の特定と、コード開発後のテストをどこに集中させるべきかを決定します。コードを作成し改良した後は、3段階の厳格なテストプロセスに従わなければなりません。通常、ソフトウェアやファームウェアを開発するエンジニアにとって、これは静的コード分析から始まります。この分析は、特別なツールを活用して脆弱性や弱点を見つけて修正する、自動化されたプロセスです。第2段階では、エンジニアチームがソースコードを一行ごとに詳細に読みこむという包括的アプローチをとります。これは通常、悪意ある行為よりも、コード内の未知の誤りを指摘する厳格な作業です。これにより、ソースコードが安全な方法で設計されていることが、さらに保証されます。

[1] https://safecode.org/ Last reviewed January 9, 2023.
[2] https://www.iso.org/standard/44378.html Last reviewed January 9, 2023.
[3] https://safecode.org/ Last reviewed January 9, 2023.
[4] https://cve.mitre.org/ Last reviewed January 9, 2023.
[5] https://cwe.mitre.org/ Last reviewed January 9, 2023.
[6] https://owasp.org/www-project-top-ten/ Last reviewed January 9, 2023.
[7] https://www.sans.org/top25-software-errors Last reviewed January 9, 2023.

設計段階の終盤では、特別なツールを使用して既知のセキュリティの脆弱性をスキャンし、最終的に脅威モデルが正確であることを確認するためのリスク評価が実施されます。コードの統合とデリバリーパイプラインでのソフトウェアは、アプリケーションのビルド、テスト、および展開時に SDL の自動化を活用し、ライフサイクルの各段階でセキュリティが統合されていることを確認します。最後に、脅威評価とモデルの結果に応じ、専門のハッカーチームによる侵入テストが指示されることもあります。このレッドチームは、それ以前の段階で見落とされた潜在的な脆弱性を発見する場合があります。こうした発見もそのリスクに応じて最小化され、追加で露呈するあらゆる発見は、文書化され修正されていきます。

Dell のセキュア開発ライフサイクルに関するさらなる詳細は Dell Security and Trust Center をご覧ください。

ファームウェアのデジタル署名

サプライチェーンに対する潜在的な脅威の1つは、不正なコードやデータ改さんのリスクです。Dell のエンジニアは、ソフトウェア、アプリケーション、ファームウェアに暗号化デジタル署名を追加し、コード署名と呼ばれるプロセスで、その信頼性と完全性を確認できるようにします。

このプロセスは、次の手順に従います:

- Dell のコア BIOS は主に米国で設計・開発されており、商用クライアント製品 (OptiPlex、 Latitude、 Precision、XPS Notebooks) 、Dell サーバー、Dell ストレージに使用されています。
- Dell を含む PCメーカーやデータセンターインフラ ベンダーの OEM (相手先ブランド製品製造業者) は、テクノロジー パート ナーが提供するチップセットおよび BIOS ファームウェア コンポーネントを組み込みます。
- 特定のプラットフォーム固有の機能は、台湾の Dell ファームウェア開発が開発し、Dell のコア BIOS にテクノロジー パートナーのファームウェアを統合します。
- 最終的なBIOS ビルドとデジタル署名は全て、米国の Dell 施設内に物理的に設置された商用システムで実行されます。

侵入テスト

ペネトレーション (侵入) テストは業界全体で成熟したセキュリティ プラクティスの代名詞となっています。Dell は社内のチームと外部ベンダーを活用して、PC、サーバー、ストレージのペンテストを、製品がまだ開発のエンジニアリング段階にある間に実施しています。これらのテストは物理的アクセスに焦点を当てており、デバイスに組み込まれている個々のコンポーネントのリスク評価に基づいて優先順位が付けられます。

BIOS保護

BIOSはハードウェアの初期化プロセスと OS への制御の移行を容易にするファームウェアです。BIOS は事実上、デバイスを制御しており、もし攻撃者が BIOS を破損させることに成功した場合、デバイスを制御できます。BIOS が

デバイス アーキテクチャの中で、一意かつ特権的な位置にあるためです。

Dell は、NIST SP 800-147「BIOS 保護に関するガイドライン」に準拠した手順を、商用サーバーと PC で全面的に導入しています。このガイドラインは、署名され認証された BIOS のみがシステム上で実行されることを指定し、BIOS を攻撃から守るためのセキュリティガイドラインと管理のベストプラクティスを含んでいます。

また、当社はサーバーとストレージの起動およびファームウェアの更新を認証するために、シリコンベースのセキュリティと暗号化ハードウェアのルート オブ トラスト (HwROT) を導入しています。読み取り専用の暗号化キーは、Dell 自社設計製品で使われるプロセッサーのシリコンマイクロチップに焼き付けられているため、改ざんや消去はできません。電源を入れると、チップは BIOSコードが正当であることを検証します。この技術は、検出されない BIOS の改ざんのリスクを著しく低減し、起動前のマルウェアや望ましくない機能の追加リスクを軽減します。

さらに、BIOS の保護策は、NIST SP 800-193「プラットフォーム ファームウェア回復性基準」に準拠して作成されています。これにより、不正な BIOS およびファームウェアコードは、単純に、実行されないようになります。もしコードが何らかの方法でマルウェアに置き換えられても、デバイスは機能しません。この耐性は、サーバーの導入から廃棄までの寿命を通じて、維持されるよう設計されています。

シャーシ侵入

Dell PowerEdge サーバーのシャーシが開けられた場合、iDRAC (Integrated Dell Remote Access Controller) にエントリーが登録されます。iDRAC は、マザーボードに搭載された専用のマイクロコントローラーであり、サーバーがオフの状態でも管理者はシステムを更新および管理できます。この機能により、侵入源を追跡することが可能になります。

同様に \ Dell の商用クライアント デバイスの多くには、Microsoft Configuration Endpoint Manager や Dell Command Suite などの管理ツールを介して監視することができる、シャーシ侵入機能が搭載されています。

組み込まれたその他のセキュリティ対策：*Dell* サーバーと *Dell* ストレージ

長年、Dell PowerEdge サーバーは堅牢なセキュリティを提供してきました。第14世代以降の PowerEdge はサイバーレジリエント、つまりサイバー攻撃への保護・検出・回復を担う堅牢な設計を備えています。最新のサーバーには信頼性の高い復旧機能も備えており、ファームウェアベースのサイバー攻撃であれば、ビジネスに殆どまたは全くの支障を与えずに克服できます。たとえば、もしマザーボードが故障か破損して交換が必要になった場合も、iDRAC によって PowerEdge サーバーの設定とファームウェアを最小限の手間でバックアップおよび復元することができます。

サーバーと同様、Dell ストレージもお客様のデータを保護するために必要な堅牢なセキュリティ対策を採用しています。

- Dell PowerStore および PowerScaleは、NIST SP800-193 ファームウェア耐障害性ガイドラインや、NIST 800-147 BIOS保護ガイドラインなどのセキュリティ基準に準拠しています。これらの仕様は、トラステッド

プラットフォーム モジュール (TPM) 、デジタル署名付きファームウェア更新、Unified Extensible Firmware Interface (UEFI) セキュア ブート、インテル ブートガード、HwROT 機能に統合されています。

- PowerScale と PowerProtect は、ハードウェアに PowerEdge を採用しているため、そのセキュリティ回復機能の恩恵を直接受けます。
- 次世代の PowerStore、PowerScale、PowerMax は、現在の機能に加え、ディスクアレイとファブリックレベルの HwROT を搭載し、競合他社と差別化を図ります。さらに、BMC HwROT は、より長い製品耐用年数をサポートするために、国家安全保障局 (NSA) の最高機密レベルのアルゴリズムをサポートするようアップグレードされました。同様に、セキュアな UEFI ブート機能と暗号化署名を有効により、HwROTは、悪意ある、または未認証の BIOS、ファームウェア、ドライバー、アプリケーションコードがストレージ プラットフォーム内にインストールや実行されないようにします。
- さらに、新世代の Dell データ ストレージ デバイスである PowerMax と PowerStore には、TPMによるデフォルトの暗号化、保存データと転送中のデータの暗号化、構成ロックなどの追加の防衛手段が備わっています。通常、格納されたデータはパスワード、ファイアウォール、基本的な暗号化、およびウイルス対策ソフトにより保護されますが、PowerMax および PowerStore には、連邦情報処理標準 (FIPS) 140-2 に準拠したデータ静止時の暗号化も備わっています。これにより、データは暗号化され、外部キーマネージャーとの統合が実現し、一元化された鍵管理プラットフォームを通じたセキュリティの簡素化が可能になります。

組み込まれたその他のセキュリティ対策：*Dell PC*

Dellは、商用PC向けに革新的で世界トップクラスの技術の開発に投資し、業界最高水準のセキュアな商用PCを提供しています。これらの機能の一部は、生産時よりも使用中の PC でより高い適用性がありますが、一部の機能は生産プロセスで使用して、より高いレベルの保証を提供し、潜在的なマルウェアの侵入を防ぐことができます。

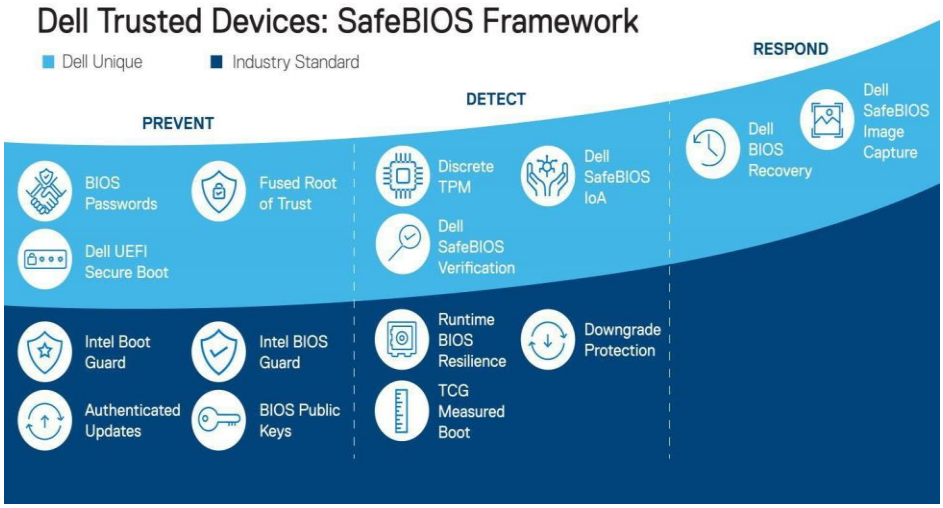
これらの内蔵セキュリティ機能には以下が含まれます。

- セキュアなオフ ホスト SafeBIOS検証：Dell がホストするオフホスト ソースに対しBIOSイメージを安全に検証
- セキュアなオフ ホスト ファームウェア検証：Intel vProに関連するインテル・マネージャビリティー・エンジンを活用、重要なファームウェアを安全に検証
- Dell SafeID with ControlVault：攻撃者にとって最も価値の高い標的であるエンドユーザーの認証情報用に、強化されたストレージを単一のチップで提供
- SafeBIOS Indicators of Attack：BIOS レベルで、振る舞いベースの脅威検出を活用し、高度なエンドポイント脅威検出を提供
- SafeBIOS Image Capture：侵害されたBIOSイメージを検出した場合、そのイメージをキャプチャしてPC に安全に保存し、攻撃の性質を特定するための分析を実現

- Dell Secured Component Verification (SCV) : インストールされたコンポーネントのマニフェストをキャプチャして生成し、Dell 認証局が暗号的に署名したうえで、将来の検証のためにシステム内に安全に保存

Dell の商用 PC は TPM (Trusted Platform Module) を搭載しており、UEFI ブートプロセス中に BIOS と協調して BIOS 測定の信頼性を維持します。最も重要なのは Root of Trust for Measurement (RTM) と Root of Trust for Reporting (RTR) です。

Trusted Computing Group (TCG) の Measured Boot は、PC の TPM を保護されたストレージ領域として使い、ブートプロセス中にロードおよび実行される BIOS やファームウェア コードのハッシュを保存します。TPM はこれらイベントを安全に保存するよう設計されており、起動後に「証明 (attestation)」と呼ばれるプロセスで検証できます。



Dell の BIOSは、お客様が自社のインフラストラクチャ内のデバイスを検知および検証できるよう、2つの独立した永続的「タグ」をサポートしています。サービスタグは、製造プロセス中に BIOS の不揮発性RAMにプログラムされ、システムの寿命が尽きるまで所定の位置に固定されます。これにより、デバイスを一般的な資産管理やサービス、保証サポートのために識別することができます。アセットタグも BIOS の不揮発性RAM に保存されており、お客様による設定、変更、クリアが可能です。BIOS 管理者パスワードを使用すると、アセットタグを変更する権限を制御することができます。

調達する

製品設計が完了すると、それを完成品に変える準備が整います。Dell は、グローバルな製造拠点の約半数を直接管理しており、同時に、追加の製造施設や原材料、個々の部品を供給するパートナー企業とも連携しています。Dell のサプライヤー選定プロセスには、各サプライヤーが誠実さ、セキュリティ、品質、信頼性の面でDell の高い基準を満たすことを確認するための厳格なオンボーディングプロセスが含まれます。高品質の製品を成功裏に提供し、増加するセキュリティ脅威を緩和する上で、これらのサプライヤーは極めて重要です。
Dell は、単なるサプライヤーを選ぶのではなく「パートナー」を選ぶことを目標に、徹底した選定プロセスを続けています。

サプライヤー リレーションシップ管理

Dell のサプライチェーンにおける品質管理は、安全なサプライチェーンにおけるセキュリティと完全性と同じくらい重要です。

この能力は、調達段階と製造段階で極めて重要です。プロセスと管理体制を整えることで、潜在的な脆弱性や悪用の機会を減らすことができます。

Dell のサプライヤー選定プロセスは、コモディティマネージャーが国、地域、コスト、財務の健全性、および品質ニーズなどの広範な戦略的カテゴリーに適合するサプライヤーのターゲットリストを作成することから始まります。次に、各サプライヤーに非常に詳細な製品仕様書が送られ、サプライヤーはどのようにその仕様に適合するかを条項ごとに回答しなければなりません。これらのサプライヤーはその後、厳格なセキュリティ評価を含む詳細な品質プロセス監査 (QPA) を受けます。QPA は現地で実施され、その場所でのエンドツーエンドの活動が評価されます。Dell の基準を満たすためのセキュリティ要件は、多くの場合、業界標準を超えます。次に、提供されるデバイスの「ベンチマーク」レベルのテストが実施され、例えばマザーボードやハードドライブなどが評価されます。通常、これには信頼性実証テストと包括的な破壊的物理解析が行われ、各デバイスは構成部品に分解されます。サプライヤーのコンポーネントやデバイスは、完成したデスクトップ、サーバー、または他の製品に組み込まれ、その性能を確認します。

当社のサプライヤー リレーションシップ マネジメント (SRM) 戦略とアプローチの日常的な一環として、ストラテジックサプライヤーは定期的なパフォーマンスレビューを受ける必要があります。サプライヤーはコスト、納期、革新性、セキュリティ、および Dell のサプライヤー原則への遵守など、予め定められた基準リストを使用して包括的にレビューされます。これらはすべて、Dell と取引を行う条件です。施設のセキュリティ要件 (FSR) は、調達契約に組み込まれています。通常、サプライヤーの工場は、Dell の期待に照らして評価され、監査されます。是正措置が必要な場合、Dell はサプライヤーの努力を積極的にサポートし、サプライヤーが新たな能力を構築できるよう支援します。

サプライチェーンのパートナーとの協力的なアプローチは、多くの直接およびサブティアのサプライヤー施設が対象です。2021年には、Dell は16か国にわたる317の工場を評価し、社会的、環境的、倫理的な業界基準である RBA (Responsible Business Alliance) の行動規範を遵守しているかどうかを監査しました。当社はさらに、物流サービスプロバイダー (LSP) および ODM パートナーに、Dell サプライチェーンセキュリティ基準の遵守を義務付けています。

多岐にわたるサプライチェーンの重点領域にわたるDell の継続的改善モデルを通じて、当社はサプライヤーと連携し、サプライヤーが自社内で能力を構築できるよう、強固な能力構築プログラムを提供しています。

Dell は、最も厳しいお客様こそが当社の最良の教師であると考え、サプライヤーには常に、セキュリティ、品質、効率、物流、卓越性におけるベストプラクティスに磨きをかけるよう求めています。持続可能性、責任、誠実さ、品質、回復力

に重点を置いたこれらの取り組みにより、当社はサプライヤーとのより強固な関係を築き、お客様により高いレベルの保証を提供しています。

製造する

現在、世界180カ国で数千万人のお客様向けに年間約5,300万台の Dell PC を生産するグローバル拠点が数多くあります。これらの工場の約半分は、Dell が直接管理しています。当社が管理する工場であれ、ODM や契約製造業者が管理する工場であれ、全ての施設は TAPA 施設のセキュリティ要件を満たし、Dell のサプライヤーセキュリティ基準に準拠する必要があります。

これらの基準には以下が含まれます。

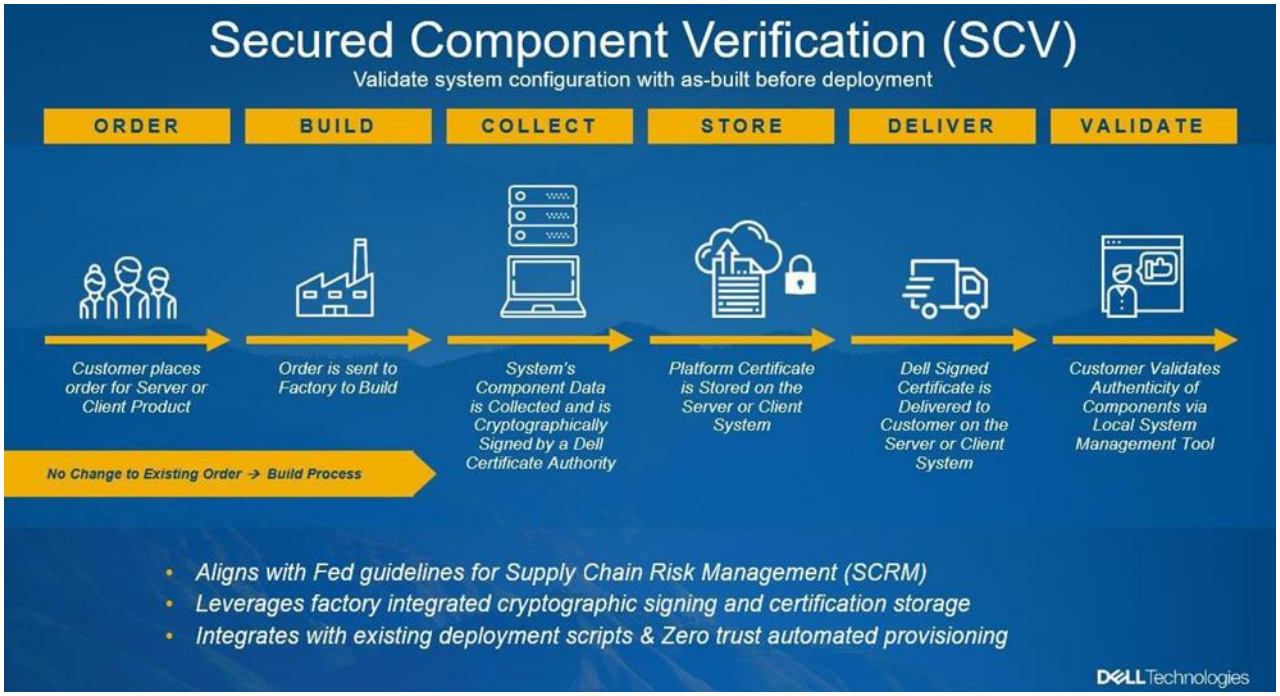
1. 調達セキュリティ：コンポーネントの調達管理、在庫管理、ソフトウェアとファームウェアのセキュリティ、および偽造品の防止に関する要件。
2. サイバーセキュリティ：サプライヤーが自社のデジタルインフラストラクチャを管理するための要件。ネットワークセキュリティ、暗号化、パッチ、脆弱性からインシデント管理とレポート作成まで。
3. 物理的セキュリティ：輸送中および製造施設における物理的資産の保護に関する要件。アクセス制御、文書化、その他の関連手順を含む。
4. セキュリティ管理システム：サプライヤーが業務全体にセキュリティを組み込む方法に関する要件 (適切な認証の維持、雇用慣行、セキュリティトレーニングなど。)

製造施設でのセキュリティ対策に加え、到着する全ての部品、コンポーネント、原材料が本物、正規品、新品であることを保証します。Dell 製品の部品は、OCM または認定ベンダーリストに掲載されている OCM の認定代理店から直接調達されます。必要なコンポーネントの入手後は、ハードウェア製品に偽造部品が組み込まれたり、ソフトウェアやファームウェアにマルウェアが挿入されたりするリスクを最小限に抑えるように設計された、堅牢なプロセスを通じて取り扱われます。たとえば Dell の各拠点では、特定のマザーボードと表面実装技術 (SMT) のアセンブリ管理が実施されます。品質エンジニアは、マザーボードの部品を検査および検証し、信頼できる担当者が SMT ラインを操作することを保証するプロセスを継続的に強化および改善しています。マザーボードが組み立て後も、マザーボードが設計通りに製造されていることを確認するための堅牢なプロセスが存在します。

検証とトラッキング

サーバーとクライアント製品に対し実施されている管理の1つは、特定の高リスク コンポーネントに固有の PPID ラベルを貼付することです。これにより Dell は、これらのコンポーネントを識別、認証、追跡できます。PPIDには、サプライヤー、部品番号、原産国、製造日に関する情報が含まれています。最終製品に組み立てられた後、対象コンポーネントの PPID は記録され、固有のシステム追跡識別番号に関連付けられて、製造時の構成履歴が提供されます。

また、Secured Component Verification (SCV) は、Dell の工場で注文が履行されてからエンドユーザーに納品されるまで、製品の完全性を最終段階で保証することを目的とした機能です。クライアントまたはサーバー製品が構築されると、インストールされたコンポーネントのマニフェストが生成され、Dellの認証局によって暗号的に署名され、システム内に安全に保存されます。製品を受け取ると、お客様は指定されたSCV検証アプリケーションを使用して、コンポーネントに不正なシステム変更が加えられていないことを確認および検証することができます。



プロセッサーやメモリのような特定の小型コンポーネントや、PPID ラベリング要件や SCV 機能を活用しないストレージやネットワーク製品に使用されるコンポーネントについては、OCM によってシリアル番号または電子識別子を通じて固有のラベル付けおよび識別され、その情報はそれらの各製品の一意のシステム識別子にも関連付けられます。品質の観点からは、これらの管理によってDell は、特定のサプライヤーやロットコードの性能の傾向を監視できます。完全性とセキュリティの観点からは、最終組立前にコンポーネントを認証することができます。

このプロセスの中核となるのは、製造中の一連の検査であり、マークが間違っているコンポーネント、通常の性能パラメーターからの逸脱、または誤った電子識別子を含むコンポーネントの特定に役立ちます。全てのシステムは、Dell 製品がお客様の期待に応え、またはそれを上回る動作をすることを確実にするため、防御策のあらゆるギャップを埋めることを目的として、製造プロセス中に機能的にテストされます。

配送する

製品がお客様に届けられる最終段階は、我々のサプライチェーンプロセスの最終ステージです。製品が完成すると、工場からお客様へ直接出荷されるか、または世界各地で稼働している数多くのフルフィルメントハブの一つに送られます。製品をお客様にお届けするために、Dellは空路、陸路、鉄道、海路で信頼できる多数のロジスティクスプロバイダーと協力して、年間34,000個の海上コンテナを満タンにするのに十分な数百万個の製品を輸送することで、毎日179,000件以上の注文に対応しています。当社の全ての物流サービスプロバイダーは、TAPA貨物セキュリティ要件または同様の地域ガイドラインに準拠する必要があります。また、サイバーセキュリティフレームワークを含む、Dell が特別に開発した貨物セキュリティ要件への準拠も必要です。

お客様の期待を超えて：Dell は配送中の製品をどう保護しているか

Dell の物流セキュリティプログラムの特徴の一つは、世界中に配置されたリスク管理コマンド＆コントロールセンターです。これらのセンターは24時間365日体制で専門家が常駐し、輸送のホットスポットに関する最新情報を利用しながら、複数の監視技術を用いて出荷を追跡し、製品が中断なく目的地に到達することを確実にます。コマンドセンターは、道路車両が取る予定のルートに関するリアルタイムデータやその他の情報を集約します。専門家は、異なる地域の脅威レベルの変化に注視しながら、トラックや貨物資産の様々なセンサーを監視して、その情報を基に必要なセキュリティレベルについて意思決定を行います。このインテリジェンスを活用して、コマンドセンターの専門家は Dell 製品を移動させる責任を持つサプライヤーに対し、輸送中のセキュリティリスクに関して助言することができます。

Dell の貨物を運ぶ専用貨物の場合、物流サービスプロバイダーには改ざん防止シールとドアロック機構の使用が義務付けられます。また、テレマティクスデータや内蔵 GPS、Bluetooth タグ、さらに盗まれた資産を回復する為の無線周波数技術を備えた秘密のトラッカーなど、多様な追跡デバイスが提供されています。これらのデバイスは、不正な停車やルートの逸脱があった場合にコントロールセンターに警告を発します。要請があり承認されれば、このセンターの専門家は、装甲車や警備員の同行を命じたり、緊急時には専用の緊急対応チーム (ERT) の派遣も可能です。サイバーセキュリティ防御がプロのハッカーによる侵入テストで試されるのと同じく、Dell は出荷シミュレーションを行い、このセンターの対応と反応プロトコルをテストします。お客様のニーズに応じたセキュリティ ソリューションのカスタマイズ能力も持ちます。セキュリティ提供に加えて、Dellは製品が目的地に到達するまでの間、完全性と管理制御をさらに確保するための追加サービスも提供できます。これらのサービスは、特定のサプライチェーンプログラムのために最初に開発されましたが、現在では他のお客様にも利用可能です。例えば、トラックに積まれた製品は、防犯テープで密封された箱に入れることができ、切断されたり取り外されたりした場合に明らかな兆候を残すことができます。

さらに、箱そのものをパレットに載せて標準的な金属製の締め具を取り外し、かわりに、特別に強化された特別な強化ストラップに置き換えることができます。パレットがトラックに積み込まれると、ドアはシリアル番号付きのボルトシールで安全に施錠され、到着時にお客様によって確認されます。

納品後

Dell 製品がお客様の手元に届いた後も、セキュリティプログラムは終わりません。特にソフトウェアやファームウェアに関連する新たな脆弱性が業界全体で定期的に発見されるためです。このため、Dell は製品セキュリティ インシデント レスポンスチーム (PSIRT) を設立しました。PSIRTは、Dell の脆弱性対応ポリシーに基づいて、すべての確認された製品の脆弱性に対する対応と開示の調整を担当しています。Dell は、セキュリティ脆弱性に関連するリスクを最小限に抑えるために、お客様にタイムリーな情報、ガイダンス、および緩和策を提供することに努めています。

通常、セキュリティ更新プログラムは、新たな脅威が発生した場合にリリースされます。Dell のセキュリティ勧告と通知は、セキュリティ アドバイザリーおよび通知サイトに掲載されます。これらアップデートは、Dell 製品と、お客様が Dell システム内で使用する Dell 以外の製品に関連する場合があります。当社はBIOS、iDRAC、ネットワークアダプタ、電源装置を含む主要コンポーネントに対する全てのアップデートが、Dell の暗号署名付きであることを保証します。ハードウェア ルート オブ トラストと、ソフトウェアやファームウェアの各コンポーネントを検証するチェーン オブ トラストを組み合わせ、最新のセキュリティアップデートを実行するで、強力なサイバーレジリエンスのある防御境界が Dell 製品に提供されます。

Dell のサプライチェーンが持つレジリエンス

Dell のグローバルな事業展開、サプライヤーとの関係、そして機動力は、サプライチェーンの強靭性の鍵となっています。セキュリティの継続的な改善に重点を置くことに加えて、当社は事業全体にわたり事業継続、危機管理、災害復旧プログラムも確立しています。この戦略的プログラムを通じて、ビジネスインパクト分析やテストの実施など、リスクを特定し軽減するための積極的な対策を講じています。こうしたレジリエンス戦略により、Dellは複雑なサプライチェーンの脅威に対してリスクを評価し、重要な意思決定を行うための統合的アプローチを開発することができました。また、Dell は重要なオペレーションとサプライヤーの拠点に対して強靭性と供給の継続性を維持する計画を策定し、調達戦略の一環として代替拠点を積極的に検討しています。

サプライチェーン デジタルトランスフォーメーション

Dell のグローバル サプライチェーンは、規模が大きく複雑ですが、お客様とそのビジネスにより良いサービスを提供べく、進化を続けています。2018年には、カスタマーエクスペリエンスの向上、運用の機動性向上、および効率の最適化を目指してデジタル トランスフォーメーションの旅を始めました。これらのエクスペリエンスにおける主要な能力を提供するためのアプローチは、以下の3つの基本原則に基づいています。

- 現代的で中央集権化されたスケーラブルなデータ インフラストラクチャを構築し、一元的な真実の情報源を確保する厳格な品質とガバナンスプロセスを実装

- アジャイルな開発プロセスを使用してスケーラブルなカスタムソリューションを構築します。迅速に開始し、開発中に目標を調整し、もしソリューションや技術が提供できない場合には、迅速に失敗することができます。
- プロセス、データ、関係、およびシステムのサプライチェーンデジタルツインを作成し、ほぼリアルタイムの可視性とシナリオプランニングを、単一のツールセットとオーケストレーションレイヤーに統合することで、ツインとエンタープライズシステム間のシームレスな相互作用を実現します。

当社のデータ構造は、社内システム、お客様、サプライヤーからの正確でタイムリーなデータへのアクセスを可能にすると同時に、データ主導型のソリューション導入を促進します。

- データガバナンス: 今後作成されるデータの一貫性を確保するための監視体制を確立します。これには、フレームワークとガバナンスプロセスの確立、業務データの所有者と管理者の任命、データガバナンスの品質監視および管理などの活動が含まれます。
- 適切なマスターデータとトランザクションデータの定義: マスターデータには、サプライヤー、拠点、品目、製品、その他の参照データに関連するデータが含まれる。トランザクションデータは、データモデルを使用して格納されます。これらの論理データモデルは、フィールドとテーブル間の最適な関係を構築し、データの流れをプロセスやシステムにマッピングするのに役立ちます。
- 適切なツールとインフラストラクチャの構築: マスター/トランザクションデータをITがサポートする最適なインフラストラクチャに展開し、信頼性を確保します。
- コンテンツ管理システム: 単一の管理ポータルを作成して、グローバルオペレーション全体で複数のツールの出力にアクセスします。

未来志向： 機械学習と人工知能 *(AI/ML)* の活用

当社のスケーラブルなアプリケーションについて詳しく掘り下げると、これらの AI/ML ツールは、需要生成、供給マッチング、混乱管理、在庫レベル目標の設定など、サプライチェーンチームがエンドツーエンドのコントロールを得るのに役立ちます。以下に、私たちが構築したいくつかのソリューションを紹介します。

Dell は、回復力と堅牢性の向上のため、エンド ツー エンドのプランニング プロセスを通じて様々なデータサイエンスモデルと効率的なワークフローを採用した、インテリジェント プランニングと予測モジュールのスイートを構築しました。これは、破壊的な需要を特定して管理する一連の異常検出ツールを使用して、自動化された統計ベースライン予測を提供します。その結果得られた予測を組み合わせることで、在庫最適化エンジンが駆動し、可能な限り高いお客様サービスレベルと、必要な運転資本を最低限に抑える構造のバランスをとることができます。これらのアプローチを組み合わせることで、予測精度、運転資本効率、リードタイム、充足率、納期遵守率が大幅に向上します。

当社はこのデジタルツイン機能を、Build-to-Stock サプライチェーンでの適用に向けて拡張しており、新しい戦略を展開する際のビジネス結果とリスクを評価するための「What-if」シナリオ分析を実行するのに役立てようとしています。

これに続いて、プライチェーンのさまざまな側面や、供給の制約、自然災害、事業拡大、地政学的緊張、サイバー攻撃などの課題を組み込むためにもデジタルツインを拡張する予定です。これにより、経営幹部は戦略やフットプリント投資を評価し、期待される結果を比較し、ビジネスおよび財務リスクを評価し、さまざまな市場および経済条件下での潜在的な欠点を理解することができます。

Dell は、在庫を最適化して不足を最小限に抑え、過剰在庫を減らすことができる機械学習モデルを開発しています。その延長として、世界中の何百もの拠点における部材のリバランス戦略を加速するために、リバランスの意思決定を促進および最適化する動的な在庫バランシングアプリケーションも構築しています。

費用対効果の高いサプライヤーの選択と事業配分は、マルチソースのコモディティーの調達計画ではよく知られた、また、きわめて重要な側面です。購入者の意思決定に影響を与える要因が多数存在する中、各部材の調達量を各サプライヤーから最適に調整することは、非常に難しい課題です。このような課題に対処するため、当社は TAM (Total Addressable Market) オプティマイザー エンジンを構築してサプライヤーへの最適な取り分を決定しています。このエンジンの目的は、コスト競争力を達成し、供給の継続性に対するリスクを軽減することです。

当社はさらに、物流および貿易業務のパフォーマンス管理とインサイトのためのワンストップ セルフサービスポータルを構築し、納期遵守率、二酸化炭素排出量、サイクルタイム、直送と混載の機会、遅延注文の原因分析などを追跡しています。このプラットフォームは、制限された第三者スクリーニング、製品分類、ライセンス管理など、貿易コンプライアンスのユースケース全体でさまざまな主要業績評価指標(KPI)を追跡するのにも役立ちます。
将来のサプライチェーンの自律的な状態への移行を見据え、私たちは「摩擦のない」サプライチェーンの構築に投資しています。このサプライチェーンは、既存のデジタル体験のレイヤーを活用し、人間と機械がそれぞれの強みを最大限に発揮できるシームレスな連携を実現する最終形態を目指します。「摩擦のない」サプライチェーンは、既存のツールやプロセスの単なる漸進的な進化ではなく、役割と責任および運用モデルの根本的な変革に焦点を当てます。
これにより、次のことが可能になります:

- エコシステムの接続: サプライチェーン全体を接続するプラットフォームを用いて、新旧のソリューション全体でデータからより多くの価値を得ます。
- 破壊的事象へのより適切な対応: サプライチェーンの中断を事前に予測し、インテリジェントなオーケストレーションを通じてリスクにプロアクティブに対処します。
- 俊敏性: 変化する市場に迅速に適応し、進化するお客様の要求に応える俊敏性を備えたシームレスなサプライチェーンフローを構築します。

Dellは、プロセスのデジタルトランスフォーメーションとを活用した意思決定のオーケストレーションにより、将来の「摩擦のない」サプライチェーンでのサプライチェーンセキュリティの進化に取り組んでいます。サイバーセキュリティ、物理的管理、エンドポイントセキュリティの複数のレベルを備えたセキュアなサプライチェーンを構築し、高い信頼性とインテリジェンスを備えた応答性の高いサプライチェーンエコシステムであり続けたいと考えています。

週7日24時間体制のアプローチ：継続的な改善活動

Dell のサプライチェーンセキュリティプロセスは、脅威の状況とともに継続的に進化しています。Dellは、いかにリスクを軽減し、いかにセキュリティ目標を達成するかの方法を明確にしたサプライチェーンリスク管理フレームワークに基づいて行動しています。このフレームワークは、変化する脅威、新たな法的要件、お客様の新たな要求や懸念など、様々な要因に対応することで当社が持続的に改善する方法を定めています。

業界とのコラボレーション

Dell内部では、数多くの部門横断的なセキュリティガバナンスフォーラムを多数開催し、既存の脅威を常に見直し、潜在的な脅威を探ることを行っています。社外的には、「共に強くなる」という信念のもと、Dell のサプライチェーン保証の専門家を信頼できる業界団体や官民パートナーシップに派遣し、業界標準や規制要件の策定において主導的な役割を果たすこともあります。セキュリティはさまざまなベンダーに影響を与えるため、Dell は業界全体のグループに参加し、他の主要ベンダーと協力して、IT製品のセキュリティに関する最良の実践を定義し、進化させ、共有することで、すべてのIT製品の安全な開発をさらに促進しています。

Dellの業界との協力の例は以下の通りです。

- Dell は、ソフトウェアの品質向上を目指す The Software Assurance Forum for Excellence in Code (SAFECode: https://www.safecode.org) の設立メンバーで、現在はその理事会の議長を務めています。その他の理事会メンバーにはMicrosoft、Adobe、SAP、Intel、Siemens、および Symantec が含まれています。SAFECode のメンバーは、ソフトウェア保証の実践とトレーニングを共有し、公開しています。
- Dell は、インシデント対応および脆弱性対応における国際的なリーダーであるフォーラム オブ インシデント レスポンス アンド セキュリティ チーム (FIRST: https://www.first.org) の、正会員です。
- Dell は、2008年に Building Security In Maturity Model (BSIMM: https://www.bsimm.com/) プロジェクトにより最初に評価された9社のうちの1社であり、現在もこのプロジェクトに参加しています。Dell の代表者は BSIMM のアドバイザリーボードのメンバーの一員です。
- 複数の Dell 社員が、IEEE Center for Secure Design の創設メンバーでした。これは、ソフトウェアアーキテクトが一般的なセキュリティ設計上の欠陥を理解し、対処できるよう支援する目的で、IEEE サイバーセキュリティイニシアチブの下で設立されました。

Dell は、世界中の政府機関との業界全体での取り組みに参加しています。ICT（情報通信技術）セクター全体でこれらの脅威に対処するのに役立つ可能性のある最近の取り組みの1つに、米国国土安全保障省の ICT サプライチェーンリスク管理 (SCRM) タスクフォースがあります。このタスクフォースは、連邦政府パートナー20団体とIT および通信セクターの企業20社で構成されています。さらに Dell は、NIST の国立サイバーセキュリティセンター

(NCCoE) に貢献し、の「*Validating the Integrity of Computing Devices* (コンピューティングデバイスの完全性を検証する)」プロジェクトを通じて、ガイドの作成にも貢献しました。

業界団体や官民パートナーシップは、業界の水準を上げるのに大いに役立ちますが、Dell の最も重要な取り組みは通常、お客様との直接的なコラボレーションを通じて特定されます。創業当初から、お客様の声に耳を傾け、お客様から学び、お客様のために提供することがDellの特長でした。当社は、世界中のお客様と積極的に関わり、対話する膨大な営業体制を敷いています。Dellは、エグゼクティブブリーフィングプログラムを開催しており、お客様に、Dellのトップリーダーやデザイナー、技術者、エンジニアと直接対話し、アイデアを探求し、戦略を練り、洞察を共有する機会をお客様に提供しています。

セキュリティは我々の DNA に深く刻まれています。当社は、製品の設計から、部品の調達、製品の製造、お客様への納品まで、サプライチェーンのあらゆる段階でセキュリティを提供します。1984年にマイケル・デルが会社を設立して以来変わらぬ私たちの目標は、信頼できる製品を、箱から出してすぐに大切なお客様のお手元に届けることです。

参考資料

1. Dell PowerEdge サーバーのサイバーレジリエントセキュリティ
2. Dell Security and Trust Center
3. Dell ISO Certifications
4. Dell Trusted Device
5. Dell Technologies Trusted Device Whitepaper, 2020
6. Dell SafeID
7. Dell Technologies: Secured Component Verification
8. Dell Signed Firmware Update (NIST SP800-147)
9. NIST Platform Firmware Resiliency SP800-193
10. Environmental, Social and Governance Report 2022