DELL Technologies

ソリューション概要

Dell Technologies Secured Component Verification for PowerEdge

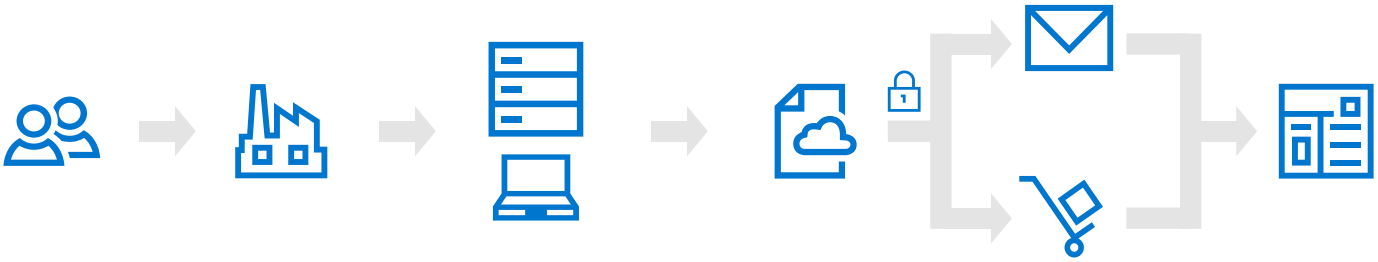
サイバーセキュリティ攻撃に対する防御は、インフラストラクチャのあらゆるレベルで IT 運用部門とセキュリティ チームの課題であり続けています。アプリケーションとオペレーティング システムの侵害は、より一般的な攻撃ベクトルです。一方で、マルウェアやランサムウェアを利用したハードウェア攻撃も増えつつあります。このような脅威の増加により、サーバーに対してより一層の注意が払われており、システムが構築されてから導入されるまでの間に、そのサーバー ハードウェアの構成が何の変更も行われていないことの保証に注目が集まっています。Forrester Research のアンケート[1] への回答者の 84% が、ハードウェア / サプライ チェーンのセキュリティがビジネスにとって不可欠であるか、または非常に重要であると回答していることもうなずけます。

Dell Technologies Secured Component Verification は、PowerEdge サーバー用に現状で構築されているハードウェア構成の検証を行います。検証により、そのハードウェア構成がミッション クリティカルなアプリケーションの強固な基盤になるという確信を持って、データセンターに新しいサーバーを導入することができます。Secured Component Verification は、テクノロジー サプライ チェーンのセキュリティに関する米国政府の新たなガイドラインに沿っています。

確信を持ってサーバーを導入

Dell Technologies Secured Component Verification は現在、Dell EMC PowerEdge サーバー ラインの不可欠な要素になっています。これにより、IT 管理者は導入前に引き渡されたシステムを安全に検証することができます。組織は、デル・テクノロジーズの製造施設でインストールされたものと同じコンポーネントとともに、新しいサーバーが引き渡されていることを保証できます。

システムの出荷準備が整ったら、サーバー コンポーネントとそのユニーク ID が評価され、結果として得られたデータは、署名された証明書を使用して暗号化でセキュリティが確保されます。暗号化されたインベントリーはサーバーに埋め込まれ、システムとともにデータセンターに出荷されます。システムを受け取った後、IT 管理者は、提供された SCV ツールを使用して、引き渡されたシステムのインベントリーを実行し、システムに格納されている証明書を使用してインベントリーを認証します。認証が完了し、コンポーネントが適合することが確認されると、システムのプロビジョニングと導入の準備が整います。



注文

お客様がサーバー製品を注文する

構築

注文が工場に送信され、ビルドされる

収集

システムのコンポーネント データが収集され、暗号化される。そして、プラットフォーム証明書が HSM（高セキュリティ モジュール）によって作成され、署名される

保存

プラットフォーム証明書は、中央の場所（サービス用 DL）とサーバー（iDRAC）に保存される

デリバリー

デルが署名した証明書は、サーバー（iDRAC）上でお客様に引き渡される

検証

お客様はローカル システム管理ツールを使用してコンポーネントの信頼性を検証する

現在の注文に変更がない
→
ビルド プロセス

[1] 出典：Forrester Research, Inc.『The Next Frontier for Endpoint Protection』

安全なテクノロジー サプライ チェーンの必要性に注目が集まる

米国政府は、国際貿易相手国と協力して、サイバーセキュリティに関するガイダンスの改善を続けています。サーバー インフラストラクチャに関しては最近、サーバー コンポーネントの検証、およびそれらのサーバーのファームウェアの信頼性について注目が集まっています。最新の草案で、国立標準技術研究所の一部である National Cybersecurity Center of Excellence（NCCOE）は、その課題を明確に示しています。すべてのサーバー OEM は、多数のコンポーネント ベンダーとサブシステム ベンダーと連携しています。サプライヤーのコンポーネントの品質とセキュリティを保証するために、すべてにサプライ チェーンの保証プログラムが導入されています。しかし、エンドユーザーにとっては、工場でインストールされたものがまさに受け取ったものであることを確認する簡単な方法はありませんでした。デル・テクノロジーズは、サプライ チェーンの保証に関するビルディング ブロック コンソーシアムである NCCoE と協力して、複雑な情報技術（IT）システムの実際のニーズに取り組む、実用的で相互運用性のあるサイバーセキュリティ アプローチを開発しています。[2]

Dell Technologies Secured Component Verification：信頼できるアプリケーションのための安全な基盤

現在の進化するサイバーセキュリティ環境では、ソフトウェアとハードウェアが侵入の標的となる可能性があるため、サーバー インフラストラクチャの保証と信頼性を高める必要があるのは明白です。アプリケーションの開発、テスト、および導入を高速化するための需要の増加に対応するために、Secure Component Validation などの新しい機能をインフラストラクチャのライフサイクルに組み込む必要があります。SCV によって、IT 運用部門とセキュリティチームに対しては、現状で提供するシステムがサーバーの仕様とセキュリティ フレームワークに適合していることが保証されます。このようにして、潜在的な攻撃ベクトルを排除して、ビジネス上の成果に力を注ぐことができます。

Secured Component Verification の機能とメリット：

- 暗号形式で署名されたインベントリー証明書を PowerEdge サーバー ポートフォリオ全体で利用可能
- 工場からラックまでの保証。安全な自己検証により、データセンターへの輸送中に十分なハードウェアの完全性を保証
- 既存のスクリプトとの統合により、検証プロセスを容易にし、信頼できる導入および自動化プロセスにすることが可能
- サイバーセキュリティが最優先事項である業界において重要なサプライ チェーン セキュリティの新たな基準に適合

[2] NIST は、本コンソーシアムに基づくビジネス向け製品を評価せず、使用されている製品またはサービスについては一切保証しません。このコンソーシアムの関連情報については、以下を参照してください。https://www.nccoe.nist.gov/projects/building-blocks/supply-chain-assurance

PowerEdge サーバーをもっと詳しく知る

Dell Technologies Secured Component Verification の詳細はこちら

Dell Technologies のシステム管理ソリューションの詳細はこちら

リソース ライブラリーを検索する

Twitter で PowerEdge Servers をフォローする

セールスまたはサポートについて Dell Technologies のエキスパートに問い合わせる