DELL Technologies

Microsoft

ホワイト ペーパー

Windows Server 2022 と次世代 Dell EMC™ PowerEdge™ サーバーの機能を組み合わせることで、高度なセキュリティ保護を実現

より安全なハードウェア、ファームウェア、オペレーティング システム環境でビジネス クリティカルなワークロードを強化

Cybersecurity Ventures によると、世界規模のサイバー犯罪は、2021 年には合計 6 兆米ドルの損失をもたらし、2025 年には 10 兆 5,000 億米ドルに増加すると予想されています。[1] ランサムウェア攻撃だけでも 6 年間で 61 倍に増加し、2021 年には 200 億米ドルに達しており、現在 11 秒ごとに 1 回のペースで攻撃が発生しています。[1] 2021 年の IDC の調査によると、対象となった世界中の組織の 3 分の 1 以上が、過去 12 か月間にランサムウェア攻撃または侵害を受けていました（多くの場合、複数回）。[2] また、IBM は、1 件のデータ侵害のコストが 424 万米ドルに達すると推定していますが[3]、実際のセキュリティ侵害によるコストは大幅に上回る可能性があります。一部の事例では、米国の病院では、ランサムウェア攻撃によって、緊急患者を他の病院に移送し、救急車の受け入れを拒否した例もありました。[4]

ファームウェア攻撃は、組織にとって特に危険な脅威になる可能性があります。これは、ファームウェアを標的とした攻撃では、オペレーティング システム (OS) が起動してソフトウェアベースのセキュリティがその OS 上で実行される前に、マルウェアを埋め込まれる可能性があるためです。しかし、ファームウェア攻撃に対してシステムを強化するための対策を講じてきた組織は半数にも満たない一方、このような攻撃は過去 5 年間で 5 倍に増加しています。[5] 結局のところ、ワークロードは、それが実行されるスタック全体の安全性以上の安全を確保できません。

マルウェアの脅威の頻度、多様性、損失の急増に対応するには、最新のセキュリティをマルチレイヤーにする必要があります。これは、マルウェアがハードウェアやファームウェアのレベルで、あるいは起動中にシステムを侵害する可能性があり、ソフトウェア デファインド セキュリティだけでは無力な領域であるためです。この脆弱性に対抗するために、最新のサーバー セキュリティは単一の柱からなる戦略ではなくなっています。セキュリティはインフラストラクチャ スタック全体に組み込まれている必要があります。次世代 Dell EMC™ PowerEdge™ サーバーと Windows Server 2022 を組み合わせることで、管理者がハードウェア、ファームウェア、および OS を調整してビジネス クリティカルなワークロードを適切に保護する、重要なタスクがシンプル化されます。

Windows Server 2022 セキュアコア サーバーと次世代 PowerEdge サーバーのメリットの組み合わせ

セキュアコア サーバーは、ハードウェア、ファームウェア、および OS 機能を使用して現在および将来の脅威に対する保護を提供する Windows Server 2022 の新機能です。次世代の PowerEdge サーバー ハードウェアで実行される Windows Server 2022 セキュアコア サーバー ソフトウェアを組み合わせることで、皆さんのような組織に対して、次の 3 つの大きなメリットがもたらされます。

- 高度な保護
- 予防的防御
- シンプル化したセキュリティ

高度な保護

セキュアコア コンピューターは、Microsoft の脅威インテリジェンス データに基づいて、通常のコンピューターの 2 倍以上の感染保護能力を提供します。Microsoft は、Windows Server 2022 セキュアコア サーバーを使用して、これと同じテクノロジーをサーバー スペースに導入しています。[5] セキュアコア サーバーによって実現される保護は、そのサーバー上の重要なワークロードとデータのための安全なプラットフォームを構築することを目的としています。具体的には、セキュアコア サーバーは、Dynamic Root of Trust for Measurement (DRTM) テクノロジーのプロセッサー サポートを使用して、ファームウェアをハードウェア ベースのサンドボックスに配置します。この分離は、高度に特権を持つ数百万行のファームウェア コードに含まれる脆弱性の影響を制限するのに役立ちます。

Windows Server 2022 のファームウェア分離を補完する仮想化ベースのセキュリティ (VBS) は、カーネルなどの OS の重要な部分をシステムの他の部分から分離します。これにより、サーバーが重要なワークロードの実行に専念させ続け、関連するアプリケーションとデータを攻撃や流出から保護することができます。

PowerEdge サーバーのファームウェアを攻撃に対してさらに強化するために、デル・テクノロジーズは PowerEdge サーバーのサプライ チェーンを保護し、工場からお客様のサイトに輸送中、サーバーの改ざんができないように支援します（以下の「デル・テクノロジーズのサプライ チェーンの整合性による追加セキュリティ」で詳しく説明します）。

予防的防御

セキュアコア機能は、攻撃者がシステムを悪用するために使用する可能性のある多くのパスをプロアクティブに防御し、切り離すのに役立ちます。VBS のハイパーバイザーで保護されたコードの整合性 (HVCI) は、コード整合性 (CI) 判定機能を Windows OS の残りの部分から分離します。これにより、カーネル メモリーを実行可能にする唯一の方法は CI 検証を通じて行われます。VBS では、Windows Defender Credential Guard を使用することもできます。この場合、ユーザー資格情報と機密情報は、OS が直接アクセスできない仮想コンテナに保存されます。

Trusted Platform Module 2.0 (TPM 2.0) は、セキュアコア サーバーに標準装備されており、起動中にロードされたコンポーネントの測定値など、機密キーとデータを格納する保護されたストアを提供します。起動中に実行されるファームウェアが、予想される作成者によって正しく署名されており、改ざんされていないことを確認できることは、セキュリティの向上に役立ちます。また、このハードウェアの信頼の基点 (Root of Trust) は、BitLocker ドライブ暗号化などの機能によって提供される保護を強化します。BitLocker ドライブ暗号化では、TPM 2.0 を使用し、ゼロトラスト セキュリティ戦略に組み込むことができる証明ベースのワークフローの作成を容易にします。これらの防御策を組み合わせることで、IT チームと SecOps チームは、注意が必要なセキュリティの多くの領域にわたって時間をより効果的に活用できるようになります。

次世代 PowerEdge サーバーは、業界標準の Unified Extensible Firmware Interface (UEFI) セキュア ブートをサポートします。UEFI セキュア ブートは、OS の実行前にロードされた UEFI ドライバーおよびその他のコードの暗号署名をチェックして、マルウェアがファームウェアを改ざんしていないか確認します。さらに、PowerEdge サーバーは、ファームウェアと OS のセキュリティを強化するために TPM 2.0 をサポートしています。

シンプル化したセキュリティ

セキュアコア PowerEdge サーバーを購入したユーザーは、デル・テクノロジーズが、セキュアコアの約束を満たす一連のハードウェア、ファームウェア、およびドライバーを提供しているという保証を得ることになります。Microsoft は、デル・テクノロジーズと緊密に連携して、PowerEdge サーバーでのセキュリティの有効化をシンプルにします。

Windows Admin Center の新機能により、管理者は Windows Server 2022 セキュアコア サーバーの OS セキュリティ機能を簡単に設定できます。新しい Windows Admin Center セキュリティ機能を使用すると、管理者はボタンをクリックするだけで高度なセキュリティを有効にすることができます。Windows Admin Center は、Windows Server 2022 セキュアコア サーバーに必要なすべてのセキュリティ機能のステータスを表示し、管理者は必要に応じて 1 つの場所から機能をオンにすることができます。

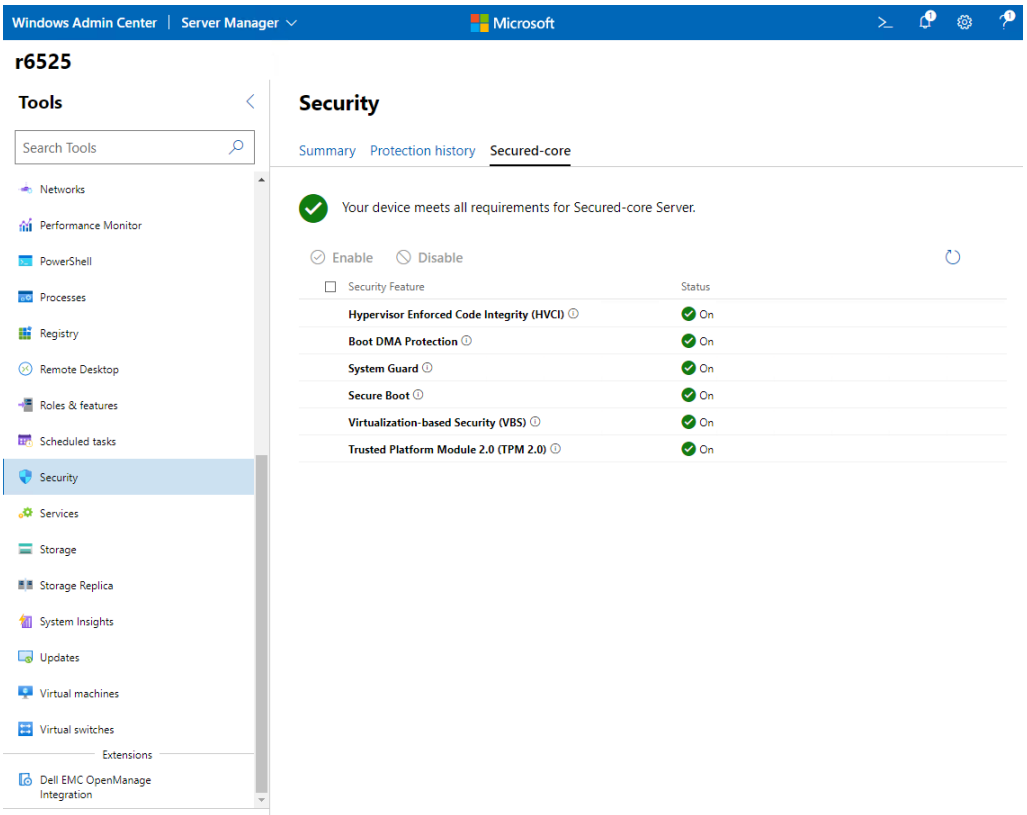


図 1. Windows Admin Center のセキュアコア確認画面

Dell EMC™ OpenManage™ Integration with Windows Admin Center は、セキュアコア サーバーの管理をさらにシンプルにする Windows Admin Center の拡張機能です。この Windows Admin Center 拡張機能は、PowerEdge サーバーをリモートで管理することで、IT 管理者のセキュリティ タスクなどをシンプルにします。Windows Server 2022 セキュアコア サーバーのコンテキストでは、OpenManage Integration with Windows Admin Center 拡張機能を使用すると、Windows Admin Center 内から PowerEdge サーバーのインベントリーを表示でき、PowerEdge サーバー コンポーネントの健全性、ハードウェアおよびファームウェアのインベントリー情報を統合表示できます。

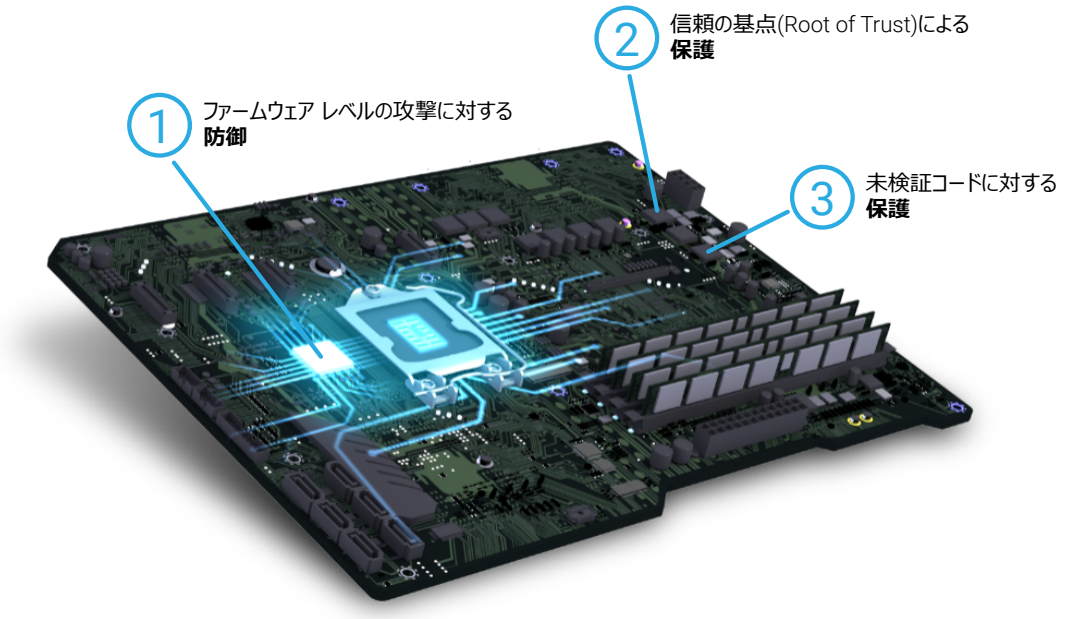
Windows Server 2022 セキュアコア サーバーに対する PowerEdge サーバーのサポート

セキュアコア サーバーの防御はマルチレイヤーであるため、ハードウェア OEM からのサポートが非常に重要です。PowerEdge サーバーは、ハードウェアとファームウェアが Windows Server 2022 セキュリティ機能の要件を満たしていることを確認するために、デル・テクノロジーズによってテストおよび認定されています。さらに、PowerEdge サーバーのハードウェアとファームウェアは、Windows Server 2022 セキュアコア サーバーを有効にするように構成されています。表 1 は、PowerEdge サーバーのハードウェアが Windows Server 2022 の機能をサポートする仕組みの詳細を示しています。

表 1. 次世代 Dell EMC™ PowerEdge™ サーバーでの Windows Server 2022 セキュリティ機能と主要なサポート機能のマッピング

	Windows Server 2022	次世代 Dell EMC™ PowerEdge™ サーバー
高度な保護	セキュアコア システムは、ファームウェアをハードウェアベースのサンドボックスに配置し、ファームウェアベースの脆弱性の影響を制限するのに役立ちます。 VBS は、OS の重要な部分を高度なマルウェアから分離します。	デル・テクノロジーズは、PowerEdge サーバーのサプライ チェーンを保護し、工場からお客様のサイトへの輸送中に、サーバーの改ざんやファームウェアの侵害が起こらないように支援します。
予防的防御	HVCI や Windows Defender Credential Guard などの VBS 機能は、あらゆる種類の脆弱性を防止し、認証情報などの機密性の高い資産をより適切に保護します。 TPM 2.0 は、安全な基盤として使用されるハードウェアの信頼の基点 (Root of Trust) を提供します。	PowerEdge サーバーは、業界標準の UEFI セキュア ブートをサポートしており、OS の実行前にロードされた UEFI ドライバーやその他のコードの暗号署名を確認します。 PowerEdge サーバーは TPM 2.0 をサポートしています。
シンプル化したセキュリティ	Windows Admin Center を使用すると、セキュアコア サーバーを簡単に設定できます。	Microsoft は、デル・テクノロジーズと連携して、PowerEdge サーバーでのセキュリティの有効化をシンプルにします。Windows Admin Center integration with Dell EMC™ OpenManage™ により、セキュアコア サーバーの管理がさらにシンプルになります。

高度なマルチレイヤー セキュリティの詳細



1 信頼の基点 (Root of Trust) による保護

セキュアコア サーバーは、デル・テクノロジーズなどの主要 OEM や、インテル、AMD などのシリコン ベンダーと提携し、業界標準のハードウェアの信頼の基点 (Root of Trust) と、最新の CPU に組み込まれているセキュリティ機能を組み合わせて使用します。

セキュアコア サーバーは、TPM 2.0 と DRTM を備えた最新の CPU を使用してサーバーをより安全に起動し、ファームウェアの脆弱性を最小限に抑えます。

2 ファームウェア レベルの攻撃に対する防御

セキュアコア サーバーは、最新の CPU でハードウェアルートのセキュリティを使用してシステムを信頼できる状態に起動し、高度なマルウェアによるシステムの改ざんやファームウェア レベルでの攻撃を防止します。

System Guard Secure Launch は、CPU を使用してデバイスをより安全に起動することを検証し、高度なファームウェア攻撃を防ぎます。

3 未検証コードに対する保護

信頼できるコンピューティング ベース内で実行されるコードは整合性を持って実行され、悪用や攻撃の対象になりません。

HVCI を有効にすると、セキュアコア サーバーは、既知の承認された機関によって署名された実行可能ファイルのみを起動します。 ハイパーバイザーは、権限を設定および適用することにより、マルウェアがメモリーを変更して実行可能にしようとすることを防ぎます。

Windows Server 2022 でのセキュアな接続のための次世代 PowerEdge サーバーのサポート

次世代 PowerEdge サーバーは、セキュリティを重視するワークロード向けに SMB (Server Message Block) AES-256 暗号化をサポートします。このサポートは、Windows Server 2022 を実行している PowerEdge サーバーが、ワークロード データのエンドツーエンドの暗号化を提供し、セキュリティを強化できることを意味します。また、Windows Server 2022 の SMB に使用される 256 ビット AES 暗号化は、十分なパスワードが使用されている限り、量子コンピューターによるブルートフォース攻撃にも耐えられるほど堅牢です。

PowerEdge サーバーと Windows Server 2022 では、East-West SMB データ トラフィックに AES-256 暗号化を使用して、個々のサーバーからクラスターの内部通信まで、エンドツーエンドの SMB 暗号化をさらに拡張します。これらの追加の SMB 暗号化制御は、ワークロードをさらに強化し、攻撃の手段を封じます。

最後に、Windows Server 2022 では、第 3 世代インテル® Xeon® スケーラブル・プロセッサーに含まれるインテル® Advanced Encryption Standard New Instructions（インテル® AES-NI）と、AMD EPYC™ Zen 3 プロセッサーに含まれる 256 ビットのベクトル化された AES 暗号化 (vAES256) を使用しています。これらの高度なプロセッサー命令セットは、PowerEdge サーバーでの AES-256 暗号化のパフォーマンスを向上させます。これらの高度なセキュリティ テクノロジーを活用することで、デル・テクノロジーズと Microsoft は、ビジネスクリティカルなワークロードに対して堅牢なセキュリティと応答性のどちらかを選択する必要がないように支援します。

デル・テクノロジーズのサプライ チェーンの整合性によるセキュリティの強化

デル・テクノロジーズのサプライ チェーンの整合性により、ハードウェアとファームウェアのコンポーネントが製造時および出荷時のセキュリティ侵害から保護されます。ハードウェアの整合性の分野において、デル・テクノロジーズは、製品をお客様に出荷する前に、製品の改ざんや偽造コンポーネントの挿入がないことを確認するための取り組みを推進しています。デル・テクノロジーズは、監査とテストによって、サプライヤーの選定、調達、生産プロセス、およびガバナンスに対応する管理策を講じています。生産中に材料の検査を行うことによって、マーキング ミスがあったり、正常な性能パラメーターから逸脱していたり、または正しくない電子 ID が含まれていたりするコンポーネントを特定できます。

ソフトウェアの整合性を確保するために、デル・テクノロジーズは、コーディングの脆弱性を防ぐだけでなく、製品をお客様に出荷する前に、ファームウェアまたはデバイス ドライバーにマルウェアが挿入されないようにすることを目指しています。さらに、デル・テクノロジーズはすべてのグローバル製造拠点で ISO 9001 認定を取得しています。これらのプロセスと管理策を厳格に遵守することで、Dell Technologies™ 製品の中に偽造コンポーネントが組み込まれるリスク、またファームウェアまたはデバイス ドライバーにマルウェアが挿入されるリスクを最小限に抑えることができます。さらに、デル・テクノロジーズは、ソフトウェア開発ライフサイクル (SDLC) プロセスの一環としてこれらの対策を実装しています。

デル・テクノロジーズは、製造施設と輸送チェーンの物理的なセキュリティの確保にも取り組んでいます。デル・テクノロジーズでは、デル・テクノロジーズ製品を製造する特定の工場に、Transported Asset Protection Association (TAPA) 施設の特定のセキュリティ要件を満たすことを求めています。重要エリアでの監視閉回路カメラの使用、入出管理、入退の継続的な警備などです。また、デル・テクノロジーズは、業界をリードする物流プログラムの一環として、輸送中の盗難や改ざんから製品を保護するための対策を講じています。最後に、PowerEdge サーバー向け Dell Technologies Secured Component Verification (SCV) により、デル・テクノロジーズのお客様は、手元に届いた PowerEdge サーバーが工場で製造されたものと一致することを確認できます。

Windows Server 2022 および次世代 Dell EMC PowerEdge サーバーによる強化されたセキュリティ基盤で、重要なワークロードを保護

ワークロードの安全性は、それが実行される基盤の安全性以上には確保できません。マルウェアやデータ侵害による脅威は、今後も増加し続けます。なにより、悪意のある攻撃者は、従来のソフトウェアベースのセキュリティに対する攻撃の影響を受けない手段を探り続けています。ファームウェア攻撃は、ソフトウェアベースのセキュリティがシステムの保護を開始する前の、起動プロセス中のサーバーを特にターゲットとします。最新のサーバー保護には、ハードウェア、ファームウェア、および OS にまたがる複数のセキュリティが必要です。

Windows Server 2022 へのアップグレードは、これまで以上に理にかなっていると言えます。Windows Server 2022 のセキュアコア サーバー機能は、組織がファームウェアと OS の両方に対する脅威に対抗するうえで威力を発揮します。デル・テクノロジーズのハードウェアおよびソフトウェアの整合性保護と組み合わせることで、Windows Server 2022 を実行する次世代の Dell EMC PowerEdge サーバーは、ハードウェア、ファームウェア、OS のスタック全体に最新のセキュリティを提供できます。また、Windows Server 2022 のセキュアな接続機能と次世代 PowerEdge サーバーでサポートされる機能により、個々のサーバーだけでなく、データ センター内のクラスター全体にこのセキュリティが拡張されます。さらに、Windows Server 2012 のサポートは 2023 年 10 月に終了します。これは、アップグレード計画を開始する時期が来ていることを意味します。[6]

Windows Server 2022 および次世代の Dell EMC PowerEdge サーバーが重要なワークロードとデータの保護にどのように役立つかについては、www.delltechnologies.com/en-us/solutions/microsoft-oem/を参照してください。

[1] Cybersecurity Ventures。「2025 年までに世界中で年間 10.5 兆ドルの損失をもたらすサイバー犯罪」、2020 年 11 月。
https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/
[2] IDC。「IDC の調査によると、世界中の組織の 3 分の 1 以上がランサムウェア攻撃または侵害を経験しています」、2021 年 8 月。
www.idc.com/getdoc.jsp?containerId=prUS48159121
[3] IBM。「How much does a data breach cost?」、2021 年。www.ibm.com/security/data-breach
[4] Dan Goodin 氏。「ランサムウェアによる病院の機能停止は患者の受け入れ拒否を引き起こしています」、*Ars Technica*、2021 年 8 月。
https://arstechnica.com/gadgets/2021/08/hospitals-hamstrung-by-ransomware-are-turning-away-patients/
[5] Microsoft。「Security Signals による新しい調査では、ファームウェア攻撃の増加が示されています。Microsoft が、このクラス全体の脅威を排除するためにどのように取り組んでいるかをご紹介します」、2021 年 3 月。
www.microsoft.com/security/blog/2021/03/30/new-security-signals-study-shows-firmware-attacks-on-the-rise-heres-how-microsoft-is-working-to-help-eliminate-this-entire-class-of-threats/
[6] このホワイト ペーパーの執筆時点。Windows Server 2012 のサポート終了に関する最新情報については、次の Windows Server 2012 ライフサイクル ページを参照してください。
https://docs.microsoft.com/en-us/lifecycle/products/windows-server-2012

DELL Technologies

Microsoft

Modernize with Windows Server 2022.
The cloud-ready operating system that boosts on-premises investments with hybrid capabilities.