DELL Technologies

Dell ThinOSのセキュリティ上のメリット

場所を問わず安全に作業

仮想デスクトップやデスクトップ アズ ア サービス環境のセキュリティを強化するように設計されたソリューションです。

Cloud Client Workspaceソフトウェアと Dellシン クライアント ソリューションで、セキュリティを損なうことなく、変化を続ける社員のニーズに対応し、効率を高めることができます。

Dellのシン クライアント ソリューションは、最新のIT管理機能によって、仮想デスクトップやデスクトップ アズ ア サービス環境への安全でシームレスなアクセスを提供することを目的に設計された、最適化されたVDIエンドポイントです。

仮想ワークスペース専用に設計された最も安全なシン クライアント オペレーティング システム[1]であるDell独自のThinOSにより、攻撃対象領域を最小限に抑え、安心感を得られます。

ポートフォリオについての詳細情報 ->

Dell ThinOS：ゼロトラスト対応

ゼロトラスト戦略の強化
Dell ThinOSとWyse Management Suiteを活用

サイバー脅威の進化に伴い、組織はデータ侵害からの保護のためにゼロトラスト セキュリティ モデルを採用しています。デル・テクノロジーズは、Dell ThinOSとWyse Management Suite (WMS)を使用して、ITリーダーが仮想環境でエンドポイント セキュリティを強化できるよう支援し、安全で管理しやすいポリシーベースのソリューションを提供します。

デバイスを信頼しない

ゼロトラスト モデルでは、ThinOSデバイスであっても自動的に信頼されるべきではありません。Wyse Management Suite (WMS)は、新しいクライアントをデフォルトのポリシー グループに配置し、構成を適用する前に管理者の承認を必要とすることで、安全なオンボーディングを可能にします。WMSまたはSCEPサーバーを介して管理される証明書を使用した、802.1xやEAP-TLSなどの安全な接続により、保護が強化されます。アカウント権限の制限、固有BIOSパスワードの設定、デバイス セキュリティ拒否リストの使用などの追加対策により、セキュリティ リスクをさらに軽減します。

アプリケーションを信頼しない

アプライアンス モードにおいて、Dell ThinOSは設計上、シェル アクセスなし、AES暗号化パーティション、改ざんを防ぐセキュア ブートなど、安全なアプリケーション サポートを保証します。WMS over SSLを介して導入できるのは、Dell承認のアプリケーション パッケージのみです。ハッシュと署名の検証により、破損や不正な変更を検出できます。管理者は、必要なソフトウェア コンポーネントのみを導入し、オプションのビジネス向けブラウザーの使用を重要なワークフローに限定することで、リスクを軽減し、露出を最小限に抑え、アプリケーションレベルのセキュリティを強化できます。

ユーザーを信頼しない

ThinOS環境でのユーザー アクセスは、ゼロトラストの原則に沿って厳密に管理されています。仮想ブローカー認証は、ユーザー アクセスを割り当て済みのデスクトップやアプリケーションのみに制限します。多要素認証は、ID保護の重要な層を追加すると同時に、Imprivata OneSignやIdentity Automationなどのプラットフォームとの統合によりセッション制御を強化します。これらを組み合わせた対策で、不正アクセスをブロックし、エンタープライズ セキュリティ標準へのコンプライアンスをサポートできます。

セキュア バイ デザイン

ユーザー デバイスの保護

ローカル データの保護

VDIセッションへの安全なアクセス

安全な設計

Dell ThinOSオペレーティング システムは、セキュリティを最優先に設計されています。クローズド アーキテクチャを採用したアプライアンスベースのソリューションとして設計されており、脆弱性を最小限に抑えるのに役立ちます。インストールできるのは、Dellが厳格にテストし、パッケージ化して認定したサードパーティー アプリケーションとドライバーのみであるため、制御された安全な環境をミッションクリティカルな業務向けに確保できます。

安全なストレージ

アプライアンス モードで動作している場合、コマンド シェルはなく、クライアントに保存されているオペレーティング システム、アプリケーション、設定ファイルをリモートで表示、変更、削除する機能もありません。セキュア ブートとAESデバイス固有のフラッシュ暗号化によってセキュリティがさらに強化され、重要なコンポーネントが強固に保護されます。

強化されたシステム

Dell ThinOSは、安全なイメージングとストレージを非公開APIと組み合わせることで、WindowsやLinuxデバイスを悩ませることの多いウイルスやマルウェアからの保護を構築しています。

一般的な脆弱性の防止

Dell ThinOSは安全性を念頭に置いて設計されています。一般的なセキュリティ上の脅威に対する堅牢な保護を実現するため、商用ブラウザーを介することなく仮想環境にシームレスに接続できます。高度なニーズを持つお客様には、インストール版も提供しています。

セキュアな管理

ユーザー デバイスの保護

ローカル データの保護

VDIセッションへの安全なアクセス

BIOSおよびCMOSのセキュリティ

ThinOSでは、Dellクライアント デバイスを使用する際に、BIOSをリモートで簡単に保護できます。Wyse Management Suite Pro Editionを使用すると、数回クリックするだけで、BIOSのアップグレードと設定（BIOSパスワードなど）を複数のデバイスに一括導入できます。

証明書の自動管理

グローバル証明書は、Wyse Management Suiteを使用して簡単に導入できます。さらに、ThinOSはSimple Certificate Enrollment Protocol (SCEP)をサポートしているため、一意のデバイス証明書の管理が簡素化されています。

セキュアな接続

Wyse Management Suiteは、パブリック ネットワークとプライベート ネットワークの両方で、暗号化された安全なHTTPS接続を使用して、ThinOSデバイスを安全に管理およびアップグレードできます。

ThinOSイメージは、特定のDellクライアント デバイスへのインストール専用に設計されており、互換性とパフォーマンスを最適に保ちます。改ざんを防ぐため、これらのイメージには、Wyse Management SuiteまたはDell OS Recovery Toolを使用して導入される場合、高度なセキュリティ対策が施されています。

主な保護：

- データの整合性を検証するためのチェックサム検証
- 画像ソースを認証するためのデジタル署名検証
- クライアント ハードウェアおよびプリインストールされたオペレーティング システムとの互換性を確保するための独自のプラットフォーム キー

セキュアな通信

ユーザー デバイスの保護

ローカル データの保護

VDIセッションへの安全なアクセス

SSL接続

ブローカーとプロトコルの通信は、すべてセキュアな接続を介して完了できます。ThinOSの通信ポリシーは、必要なセキュリティレベルを適用するためにグローバル レベルまたは個別レベルで定義できます。3つの「サポートされる」レベルは次のとおりです。

- 高 - 証明書の検証が必要
- 警告 – 証明書の検証が失敗した場合はユーザーによる承認が必要
- 低 - 証明書の検証不要

有線およびワイヤレスのセキュリティ

すべての有線および無線802.1xエンタープライズ通信は、EAP-PEAP、EAP-LEAP、EAP-TLS、またはEAP-FASTでWPA/WPA2 PSK/Enterpriseを使用して保護できます。

ブローカー プロトコル セキュリティ

WindowsやLinuxデスクトップと同様に、ThinOSはRDP、HDX、BLAST、DCV、PCoIPプロトコルを使用して仮想環境ブローカーやサーバーに接続する際に、暗号化と圧縮機能を使用できます。さらに、ThinOSはFIPS 140-2に対応しているため、機密性の高い環境でも安全な通信を確保できます。

ローカル ユーザーのセキュリティ

エンド ユーザー データを保護し、ローカル ユーザー アクセスを制御

ユーザー デバイスの保護

ローカル データの保護

VDIセッションへの安全なアクセス

改ざん防止

ThinOSの権限設定は、デスクトップ メニューへのユーザー アクセスを制限し、不正な表示や変更を防止することで、堅牢なデスクトップ セキュリティを提供します。IT管理者にはユーザー インターフェイスへのフルアクセス権限が付与されているため、完全な制御と効率的な運用が可能です。さらに、ThinOSは、ローカル ブラウザーをインストールすることなく仮想環境に接続できるように設計されています。

エンド ユーザー資格情報の保護

デフォルトで、ThinOSデバイスは、サインオン認証情報とアプリケーション キャッシュ オブジェクト（セッション ビットマップなど）を、セッションが終了するまでRAMに排他的に格納します。デバイスのフラッシュ ファイル システムには、サインオン認証情報やプロトコル オブジェクトが書き込まれません。対照的に、WindowsやLinuxベースのデバイスは、認証情報とアプリケーション キャッシュを保持するためにディスク キャッシュを使用することが多く、データ侵害やハッキングに対して脆弱になりがちです。

高度な認証とトークン

90MeterおよびActiveIdentityミドルウェアを備えたCACおよびPIVスマートカード、およびFIDO2を備えたYubiKeyデバイスを使用したトークンベースの認証がサポートされます。

USBおよびローカル ディスクのセキュリティ

クライアントのローカル フラッシュ ファイル システムに保存されるすべてのThinOSイメージ システム ファイル、パッケージ ファイル、キャッシュされた構成、ミラーリングされたリポジトリ オブジェクトは、データ侵害のリスクを最小限に抑えるためにAES暗号化されます。

Trusted Platform Module (TPM)を搭載したユニットの場合、ハッシュ キーの一部がこのコンポーネント内に格納されます。これにより、フラッシュ モジュールをデバイスから取り外しても、これらのモジュール上のデータにはアクセスできません。さらに、セキュアSSL接続を確立するために使用される証明書は、デバイスのフラッシュにロードされて保存されるとエクスポートできなくなります。

- **キャッシュはすべてRAMに保存されるため非永続的**
- **AES暗号化はすべてのパーティション/ファイルに適用されます**
- **工場出荷時のデフォルトにリセットすると、デバイスは工場出荷時の設定状態に復元されます**
- **デバイス固有のフラッシュ暗号化とセキュア ブート**

Dell ThinOSでは、USB大容量ストレージ デバイスを正確に制御できます。アクセス権を持つユーザー、およびユーザーがデバイスをどのように使用できるかを定義し、セキュリティと柔軟性の両方を確保することができます。

1 Flexible controls for IT support

管理者権限を使用して、クライアントのトラブルシューティングを制御できます。クライアント ログは、WMSまたはローカルUSBキーにエクスポートできます。

クライアント デバイスの設定は、非OSのセキュアなフラッシュ パーティションに保存されます。これらの設定は、工場出荷時のデフォルト設定にリセットすることでクリアできます。

クライアント証明書とイメージ ファイルは、非OSの安全なストレージ パーティションに格納されます。これらの証明書は、工場出荷時のデフォルトにリセットすることでクリアできます。

2 USB大容量ストレージの仮想環境へのアクセスを柔軟に制御

ThinOS BIOS

USBポートは、デバイス上でローカルに、またはWyse Management Suiteコンソールを使用して、BIOS設定を介して有効/無効にすることができます。USBポートの無効化は、すべてのUSBデバイス クラスに適用されます。

プライバシーとセキュリティ

デバイス セキュリティは、VID/PIDまたはUSBクラスに基づいてUSBデバイスへのアクセスを許可または拒否します。ThinOSクライアント デバイスに接続されているすべてのデバイスへのアクセスを選択的に制限できます。

周辺機器

USBリダイレクト設定を使用して、ThinOSクライアント デバイスではなく仮想ホストからUSBデバイス ドライバーを強制的にサポートすることができます。

セッションの設定

グローバルおよびベンダー固有のパートナー ポリシーを使用して、USBデバイスのマッピングとリダイレクトを制御できます。

Dell ThinOSで優れた安全性を備えたシンクライアントに[1]

最初の起動時から安全性を確保

Dell独自のシン クライアント オペレーティング システムはセキュア バイ デザインで、リスクを最小限に抑え、仮想デスクトップとデスクトップ アズ ア サービス セッションを保護するように設計されています。

セキュアな管理

Wyse Management Suiteのきめ細かな一元管理により、セキュリティ ポリシーの適用、デバイス コンプライアンス設定の構成、BIOSの管理が可能です。

エンド ユーザー資格情報の保護

RAMにユーザー資格情報を保存することで、マルウェアの攻撃から保護され、再起動時には自動的に削除されるため、不正アクセスのリスクが低減されます。

信頼できるエンドポイント

セッション データを保護し、どこからでも安心して接続できるように、一般的な認証方法、コンプライアンス標準、非永続的な情報をサポートしています。

クローズド アーキテクチャ

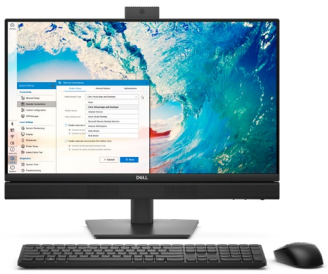
ローカル デバイスでの機密データや個人情報の漏洩を防止します。攻撃対象領域を制限するシステム ハードニング、非公開API、Dellが独自にパッケージ化した暗号化データおよびファイルにより、ウイルスとマルウェアに対する優れた耐性があります。

セキュアな通信

ThinOSは、すべてのブローカー プロトコルでSSL接続に対応し、有線およびワイヤレスエンタープライズネットワークへの安全なアクセスを実現する高度な暗号化方式をサポートすることで、安全な通信を確保します。

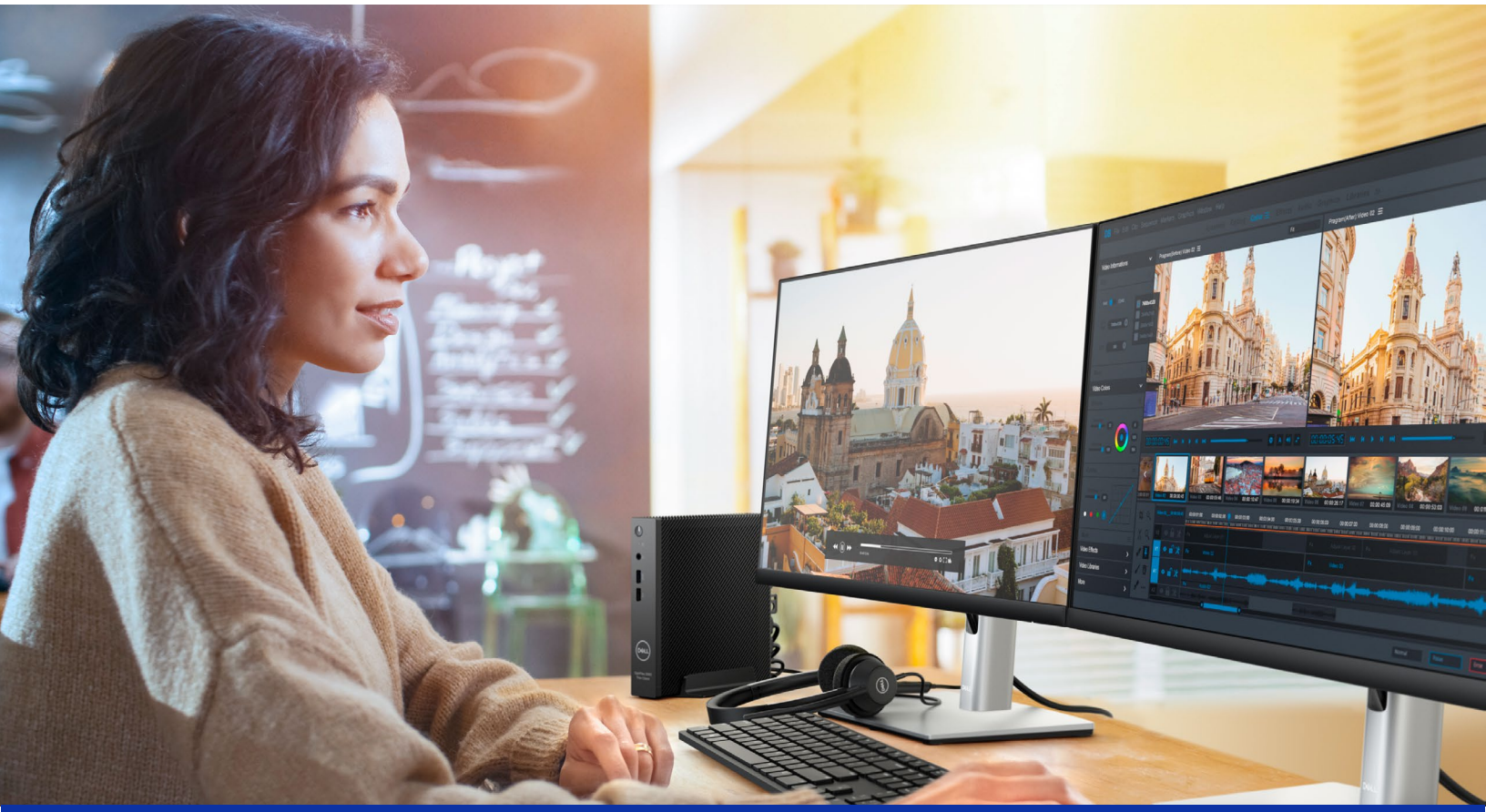
Dellシン クライアント ソリューションの詳細を見る

OptiPlex 3000シン クライアント - >



Dell Proオールインワン35 W - >

Dell Pro 14ノートパソコン - >



Dell ThinOSとDellシン クライアント ソリューションで、どこでも安心して仕事に取り組める環境を確保

仮想デスクトップ インフラストラクチャおよびデスクトップ アズ ア サービス ソリューション向けに最適化された安全なVDIエンドポイント。

ぜひご参加ください
dell.com/CloudClientWorkspace

詳細を表示
ITのシンプル化に関するブログ-->

ぜひご参加ください
LinkedIn / X

出典と免責事項

[1]Dell ThinOSと競合製品を比較したDellの分析（2025年1月）に基づきます。

[2]Dell ThinOSアプライアンス モードは、Dell ThinOSのデフォルトの動作状態であり、最初から堅牢なセキュリティ体制を適用するように設計されています。バージョン2508以降では、ThinOSでIT管理者の柔軟性が向上し、ビジネス向けブラウザー オプションのインストールとサードパーティー製ソフトウェア コンポーネントの導入が可能になります。ThinOS 10との互換性を確保するには、サードパーティー製アプリケーションにUbuntu 24.04 x86_64との互換性があること、Debianインストール パッケージが含まれていること、App Builderツールを使用したすべてのOS依存関係チェックに合格していることが必須条件です。ただし、クライアント デバイスの機能によって異なる場合があります。導入では、分離モードまたはネイティブ モードのいずれかを選択する必要があります。ネイティブ モードで実行しているアプリケーションは、その動作に基づいて制限される場合があります。導入前に、インストールと機能が正常に動作することを確認するために、徹底的なテストを実施することを強くお勧めします。サポートされているアプリケーションと導入ガイドラインの詳細については、Dell.com/supportにあるカスタマー インストール ガイドを参照してください。