DELL Technologies

Sicherheitsvorteile von Dell ThinOS

Zuverlässiges, standortunabhängiges Arbeiten

mit Lösungen, die die Sicherheit Ihrer virtuellen Desktops und Desktop-as-a-Service-Umgebungen erhöhen

Mit der Cloud Client Workspace-Software und Dell Thin Client-Lösungen erfüllen Sie die sich stets ändernden Anforderungen der Arbeitswelt und steigern die Effizienz Ihrer Teams, ohne die Sicherheit zu beeinträchtigen.

Dell Thin-Client-Lösungen sind speziell entwickelte optimierte VDI-Endpunkte für den sicheren und nahtlosen Zugriff auf virtualisierte Desktops und Desktop-as-a-Service- (DaaS-)Umgebungen mit modernem IT-Management.

Minimieren Sie die Angriffsfläche und erleben Sie sorgenfreies Arbeiten mit dem exklusiven ThinOS von Dell, unserem sichersten Thin-Client-Betriebssystem[1], das speziell für virtuelle Arbeitsplätze entwickelt wurde.

Weitere Informationen zum Portfolio ->

Dell ThinOS: Zero-Trust-fähig

Zero-Trust-Strategien stärken mit Dell ThinOS und Wyse Management Suite

Angesichts der zunehmenden Cyberbedrohungen setzen Unternehmen Zero-Trust-Sicherheitsmodelle ein, um sich vor Datenschutzverletzungen zu schützen. Dell Technologies unterstützt IT- Führungskräfte dabei, die Endpoint Security in virtuellen Umgebungen mit Dell ThinOS und Wyse Management Suite (WMS) zu stärken, indem es eine sichere, einfach zu managende und Policy-gesteuerte Lösung bereitstellt.

Vertraue keinem Gerät

In einem Zero-Trust-Modell sollten selbst ThinOS-Geräte nicht standardmäßig als vertrauenswürdig eingestuft werden. Die Wyse Management Suite (WMS) ermöglicht ein sicheres Onboarding, indem neue Clients einer Standardrichtliniengruppe zugeordnet werden, die vor der Anwendung von Konfigurationen die Genehmigung durch einen Administrator erfordern. Sichere Verbindungen wie 802.1x oder EAP-TLS mit Zertifikaten, die über WMS oder einen SCEP-Server verwaltet werden, bieten einen verbesserten Schutz. Zusätzliche Maßnahmen, einschließlich der Einschränkung von Kontoberechtigungen, der Festlegung eindeutiger BIOS-Kennwörter und der Verwendung einer Gerätesicherheits-Sperrliste reduzieren Sicherheitsrisiken weiter.

Vertraue keiner Anwendung

Im Appliance-Modus gewährleistet Dell ThinOS per Design einen sicheren Anwendungssupport ohne Zugriff auf die Shell, AES-verschlüsselte Partitionen und Secure Boot, um Manipulationen zu verhindern. Nur von Dell genehmigte Anwendungspakete können über WMS über SSL mit Hash- und Signaturvalidierung bereitgestellt werden, um Beschädigungen oder unbefugte Änderungen zu erkennen. AdministratorInnen können Risiken verringern, indem sie nur die erforderlichen Softwarekomponenten bereitstellen und die Verwendung optionaler kommerzieller Browser auf wesentliche Workflows beschränken, wodurch eine Gefährdung minimiert und die Sicherheit auf Anwendungsebene erhöht wird.

Vertraue keinem Nutzer

Der Nutzerzugriff in ThinOS-Umgebungen wird streng im Einklang mit Zero-Trust-Prinzipien verwaltet. Die virtuelle Brokerauthentifizierung stellt sicher, dass NutzerInnen nur Zugriff auf die ihnen zugewiesenen Desktops oder Anwendungen haben. Die Multifaktor-Authentifizierung fügt eine wichtige Ebene des Identitätsschutzes hinzu, während die Integration mit Plattformen wie Imprivata OneSign oder Identity Automation die Sitzungskontrolle stärkt. Diese kombinierten Maßnahmen tragen dazu bei, jeglichen unbefugten Zugriff zu verhindern und die Compliance mit den Sicherheitsstandards des Unternehmens zu unterstützen.

Sicher per Design

Schutz des Nutzergeräts

Schutz lokaler Daten

Sicherer Zugriff auf die VDI-Sitzung

Sicheres Design

Das Dell ThinOS-Betriebssystem ist speziell mit Sicherheit als Kernkompetenz konzipiert. Es wurde als appliancebasierte Lösung mit einer geschlossenen Architektur entwickelt und trägt dazu bei, Sicherheitslücken zu minimieren. Nur Anwendungen und Treiber von Drittanbietern, die von Dell streng getestet, zusammengestellt und zertifiziert wurden, können installiert werden, um eine kontrollierte und sichere Umgebung für Ihre erfolgskritischen Vorgänge zu gewährleisten.

Gehärtete Oberflächen

Durch die Kombination von sicherem Imaging und Storage mit nicht öffentlich verfügbaren APIs schafft Dell ThinOS eine gehärtete Oberfläche, die vor Viren und Malware schützt, von denen Windows- und Linux-Geräte häufig bedroht sind.

Sicherer Storage

Beim Betrieb im Appliance-Modus gibt es keine Befehlsshell oder die Möglichkeit, Betriebssystem-, Anwendungs- oder Konfigurationsdateien, die auf dem Client gespeichert sind, remote anzuzeigen, zu ändern oder zu löschen. Die Sicherheit wird durch Secure Boot und die gerätespezifische AES-Flash-Verschlüsselung weiter untermauert, die einen robusten Schutz für kritische Komponenten bietet.

Gängige Sicherheitslücken verhindern

Dell ThinOS wurde mit Blick auf Sicherheit entwickelt. Für einen robusten Schutz vor gängigen Sicherheitsbedrohungen kann es sich nahtlos mit virtuellen Umgebungen verbinden, ohne dass ein kommerzieller Browser erforderlich ist. Für KundInnen mit erweiterten Anforderungen besteht die Möglichkeit, einen zu installieren.

Sicheres Management

Schutz des Nutzergeräts

Schutz lokaler Daten

Sicherer Zugriff auf die VDI-Sitzung

BIOS- und CMOS-Sicherheit

ThinOS erleichtert die Remotesicherung Ihres BIOS bei Verwendung eines Dell Client-Geräts. Mit nur wenigen Klicks können Sie BIOS-Upgrades und -Einstellungen wie BIOS-Kennwörter mit der Wyse Management Suite Pro Edition für mehrere Geräte bereitstellen.

Automatisiertes Zertifikatmanagement

Globale Zertifikate lassen sich mit der Wyse Management Suite einfach bereitstellen. Darüber hinaus unterstützt ThinOS Simple Certificate Enrollment Protocol (SCEP) und vereinfacht damit das Management eindeutiger Gerätezertifikate.

Sichere Verbindungen

Die Wyse Management Suite kann ThinOS-Geräte mithilfe sicherer, verschlüsselter HTTPS-Verbindungen in öffentlichen und privaten Netzwerken sicher managen und aktualisieren.

Sicheres Imaging

ThinOS-Images wurden speziell für die Installation auf bestimmten Dell Client-Geräten entwickelt, um optimale Kompatibilität und Performance zu gewährleisten. Zum Schutz vor Manipulationen enthalten diese Images erweiterte Sicherheitsmaßnahmen, wenn sie über die Wyse Management Suite oder das Dell OS Recovery Tool bereitgestellt werden.

Zu den wichtigsten Schutzmaßnahmen zählen:

- Prüfsummenvalidierung zur Überprüfung der Datenintegrität
- Validierung der digitalen Signatur zur Authentifizierung der Bildquelle
- Eindeutige Plattformschlüssel zur Gewährleistung der Kompatibilität mit der Client-Hardware und dem vorinstallierten Betriebssystem

Sichere Kommunikation

Schutz des Nutzergeräts

Schutz lokaler Daten

Sicherer Zugriff auf die VDI-Sitzung

SSL-Anschlüsse

Die gesamte Broker- und Protokollkommunikation kann über sichere Verbindungen abgewickelt werden. ThinOS-Kommunikations-Policies können auf globaler oder individueller Ebene definiert werden, um die gewünschte Sicherheitsstufe durchzusetzen. Die drei „unterstützten" Stufen sind wie folgt:

- Hoch – Zertifikatvalidierung erforderlich
- Warnung – Nutzerakzeptanz erforderlich, wenn die Zertifikatvalidierungsprüfung fehlschlägt
- Niedrig – keine Zertifikatvalidierung erforderlich

Kabelgebundene und drahtlose Sicherheit

Die gesamte kabelgebundene und drahtlose 802.1x- und Wireless-Enterprise-Kommunikation kann mit WPA/WPA2 PSK/Enterprise mit EAP-PEAP, EAP-LEAP, EAP-TLS oder EAP-FAST gesichert werden.

Broker-Protokollsicherheit

Wie Windows- und Linux-Desktops bietet auch ThinOS Verschlüsselungs- und Komprimierungsfunktionen, wenn Sie sich über die Protokolle RDP, HDX, BLAST, DCV und PCoIP mit Brokern und Servern der virtuellen Umgebung verbinden. Darüber hinaus ist ThinOS FIPS 140-2-fähig, um eine sichere Kommunikation in sensiblen Umgebungen sicherzustellen.

Sicherheit lokaler NutzerInnen

Schutz der Endnutzerdaten und Kontrolle des lokalen Nutzerzugriffs

Schutz des Nutzergeräts

Schutz lokaler Daten

Sicherer Zugriff auf die VDI-Sitzung

Manipulationsschutz

Die ThinOS-Berechtigungseinstellungen sorgen für eine solide Desktop-Sicherheit, indem sie den Nutzerzugriff auf Desktopmenüs einschränken, um unbefugte Anzeigen oder Änderungen zu verhindern. IT-AdministratorInnen haben vollständigen Zugriff auf die Benutzeroberfläche, um eine vollständige Kontrolle und optimierte Betriebsabläufe zu gewährleisten. Darüber hinaus ist ThinOS für die Verbindung mit einer virtuellen Umgebung konzipiert, ohne dass ein lokaler Browser installiert werden muss.

Erweiterte Authentifizierung und Token

Unterstützung für tokenbasierte Authentifizierung mit CAC- und PIV-Smartcards mit 90Meter- und ActiveIdentity-Middleware sowie Yubikey-Geräte mit FIDO2.

Sichern der Endnutzerzugangsdaten

Standardmäßig speichern ThinOS-Geräte SignOn-Anmeldeinformationen und Anwendungscacheobjekte (z. B. Sitzungs-Bitmaps) ausschließlich im RAM, bis die Sitzung beendet wird. Es werden keine SignOn-Anmeldeinformationen oder Protokollobjekte in das Flash-Dateisystem des Geräts geschrieben. Im Gegensatz dazu verwenden Windows- und Linux-basierte Geräte häufig Festplattencache, um Anmeldeinformationen und Anwendungscache beizubehalten, was sie anfälliger für Datenschutzverletzungen oder Hacking macht.

Sicherheit von USB und lokaler Festplatte

Alle auf dem lokalen Flash-Dateisystem des Clients gespeicherten ThinOS-Image-Systemdateien, Paketdateien, zwischengespeicherten Konfigurationen und gespiegelten Repository-Objekte sind AES-verschlüsselt, um das Risiko einer Datenkompromittierung zu minimieren.

Bei Systemen, die mit einem Trusted Platform Module (TPM) ausgestattet sind, wird ein Teil der Hash-Schlüssel in dieser Komponente gespeichert. Folglich bleiben die Daten auf diesen Modulen selbst dann nicht zugänglich, wenn Flash-Module von den Geräten entfernt werden. Darüber hinaus können Zertifikate, die zum Herstellen sicherer SSL-Verbindungen verwendet werden, nach dem Laden und Speichern im Flash des Geräts nicht exportiert werden.

- **Die gesamte Zwischenspeicherung erfolgt im RAM und ist nicht persistent.**
- **Die AES-Verschlüsselung wird auf alle Partitionen/Dateien angewendet.**
- **Durch Zurücksetzen auf die Werkseinstellungen wird das Gerät auf den Konfigurationsstatus zurückgesetzt, in dem es vom Werk ausgeliefert wurde.**
- **Gerätespezifische Flash-Verschlüsselung und sicherer Start**

Dell ThinOS bietet Ihnen eine präzise Kontrolle über USB-Massenspeichergeräte. Sie können festlegen, welche NutzerInnen Zugriff haben und wie sie diese Geräte im Einzelnen verwenden können, um sowohl Sicherheit als auch Flexibilität zu gewährleisten.

1 Flexible controls for IT support

Mit Administratorrechten können Sie das Client-Troubleshooting steuern. Client-Protokolle können in WMS oder auf einen lokalen USB-Stick exportiert werden.

Client-Gerätekonfigurationen werden in einer sicheren Flash-Partition ohne Betriebssystem gespeichert. Diese Konfigurationen können durch Zurücksetzen auf die Werkseinstellungen gelöscht werden.

Client-Zertifikate und Image-Dateien werden in einer sicheren Storage-Partition ohne Betriebssystem gespeichert. Diese Zertifikate können durch Zurücksetzen auf die Werkseinstellungen gelöscht werden.

2 Flexible Steuerelemente für den Zugriff auf virtuelle USB-Massenspeicherumgebungen

ThinOS-BIOS

USB-Anschlüsse können über BIOS-Konfigurationen aktiviert/deaktiviert werden, entweder lokal auf dem Gerät oder über die Konsole der Wyse Management Suite. Die Deaktivierung von USB-Anschlüssen gilt für alle USB-Geräteklassen.

Datenschutz & Sicherheit

Die Gerätesicherheit erlaubt oder verweigert den Zugriff auf USB-Geräte basierend auf VID/PID oder USB-Klasse. Sie ermöglicht die selektive Einschränkung des Zugriffs auf jedes Gerät, das mit dem ThinOS-Client-Gerät verbunden ist.

Peripheriegeräte

Mit USB-Umleitungseinstellungen können Sie erzwingen, dass die Unterstützung für USB-Gerätetreiber von einem virtuellen Host und nicht vom ThinOS-Client-Gerät kommt.

Sitzungseinstellungen

Globale und anbieterspezifische Partner-Policies können verwendet werden, um die Zuordnung und Umleitung von USB-Geräten zu steuern.

Die sichersten Thin Clients mit Dell ThinOS[1]

Sicherheit ab dem ersten Start

Das exklusive Thin-Client-Betriebssystem von Dell ist sicher konzipiert, um Risiken zu minimieren und virtuelle Desktops und Desktop-as-a-Service-Sitzungen zu schützen.

Sicheres Management

Die granulare, zentrale Steuerung durch die Wyse Management Suite hilft bei der Durchsetzung von Sicherheitsrichtlinien, der Konfiguration von Geräte-Compliance-Einstellungen und dem Management des BIOS.

Sichere ENDNUTZER-ANMELDEINFORMATIONEN

Das Speichern von Nutzerzugangsdaten im RAM trägt dazu bei, sie vor Malware zu schützen. Sie werden beim Neustart gelöscht, wodurch das Risiko eines unbefugten Zugriffs reduziert wird.

Vertrauenswürdiger Endpunkt

Unterstützung gängiger Authentifizierungsmethoden, Compliance-Standards und nicht persistente Informationen helfen beim Schutz von Sitzungsdaten und für eine sichere Verbindung an jedem Ort.

Geschlossene Architektur

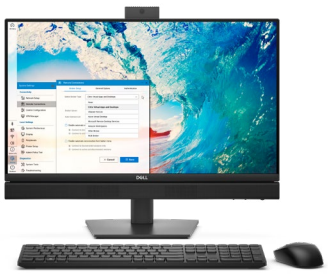
Keine sensiblen oder personenbezogenen Daten sind auf dem lokalen Gerät verfügbar. Härten des Systems zur Begrenzung von Angriffsflächen, unveröffentlichte APIs, verschlüsselte Daten sowie exklusiv von Dell zusammengestellte Dateien helfen bei der Abwehr von Viren und Malware.

Sichere Kommunikation

ThinOS sorgt für eine sichere Kommunikation, indem es SSL-Verbindungen für alle Broker-Protokolle und erweiterten Verschlüsselungsmethoden für den sicheren Zugriff auf kabelgebundene und drahtlose Unternehmensnetzwerke unterstützt.

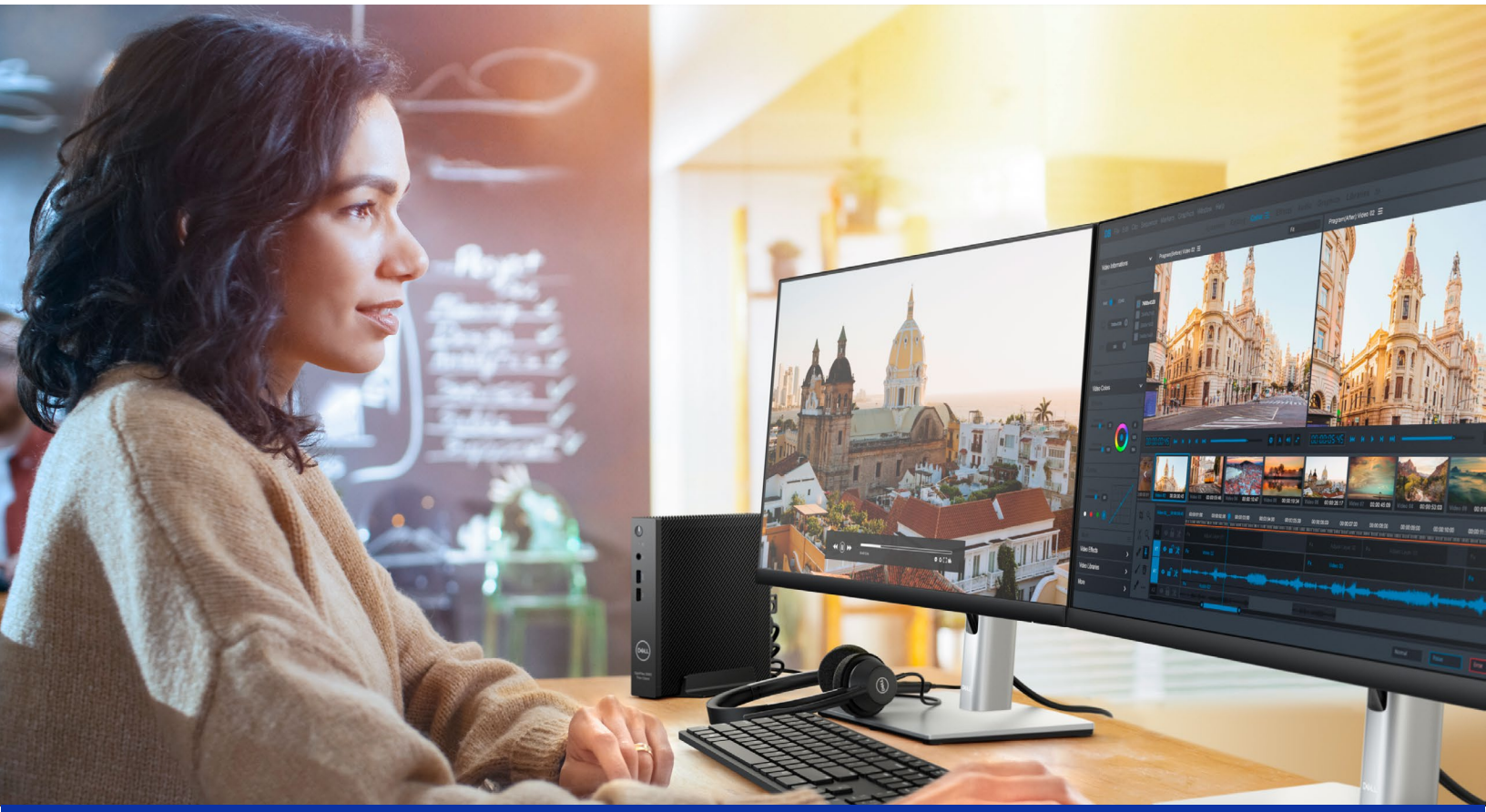
Dell Thin-Client-Lösungen erkunden

OptiPlex 3000 Thin Client ->



Dell Pro All-in-One 35 W - >

Dell Pro 14 Laptop - >



Sicheres Arbeiten von überall aus mit **Dell ThinOS- und Dell Thin Client-Lösungen**

Ein optimierter und sicherer VDI-Endpunkt für Ihre Virtual Desktop Infrastructure- und Desktop-as-a-Service-Lösungen.

Besuchen Sie uns
dell.com/CloudClientWorkspace

Weitere Informationen
Blog zum Vereinfachen der IT – >

An Unterhaltung teilnehmen
LinkedIn / X

Quellen und rechtliche Hinweise

[1] Basierend auf einer Analyse von Dell, bei der Dell ThinOS im Appliance-Modus mit Produkten von Mitbewerbern verglichen wurde, Januar 2025

[2]Der Dell ThinOS Appliance-Modus ist der Standardbetriebszustand von Dell ThinOS, der entwickelt wurde, um von Anfang an einen stabilen Sicherheitsstatus zu gewährleisten. Mit Version 2508 und höher bietet ThinOS IT-Administratoren mehr Flexibilität, indem es die Installation kommerzieller Browseroptionen und die Bereitstellung von Softwarekomponenten von Drittanbietern ermöglicht. Um die Kompatibilität mit ThinOS 10 sicherzustellen, müssen Drittanbieteranwendungen mit Ubuntu 24.04 x86_64 kompatibel sein, ein Debian-Installationspaket enthalten und alle BS-Abhängigkeitsprüfungen im App Builder-Tool erfolgreich bestehen (abhängig von der Funktion des Client-Geräts). Die Bereitstellung erfordert das Auswählen zwischen dem isolierten oder dem nativen Modus. Anwendungen, die im nativen Modus ausgeführt werden, können aufgrund ihres Betriebsverhaltens Einschränkungen unterliegen. Es wird dringend empfohlen, vor der Bereitstellung gründliche Tests durchzuführen, um eine erfolgreiche Installation und die ordnungsgemäße Funktionalität sicherzustellen. Weitere Informationen zu unterstützten Anwendungen und Bereitstellungsrichtlinien finden Sie im Kundeninstallations-handbuch unter Dell.com/support.