DELL Technologies

Dell ThinOS-säkerhetsfördelar

Arbeta tryggt var som helst

med lösningar som är konstruerade för att öka säkerheten i dina virtuella skrivbordsmiljöer och Desktop-as-a-Service-miljöer.

Uppfyll de föränderliga behoven för arbetsstyrkan och öka effektiviteten utan att kompromissa på säkerheten med Cloud Client Workspace-mjukvara och Dells lösningar med tunna klienter.

Dells lösningar för tunna klienter är optimerade för VDI-slutpunkter som har utformats särskilt för att ge säker och smidig åtkomst till virtualiserade stationära datorer och Desktop-as-a-Service-miljöer med modern IT-hantering.

Minimera angreppsytan och känn dig trygg med Dells exklusiva ThinOS, vårt säkraste operativsystem för tunna klienter[1] som har utformats särskilt för virtuella arbetsytor.

Mer information om portföljen ->

Dell ThinOS: Klar för nollförtroende

Stärk nollförtroendestrategier med Dell ThinOS och Wyse Management Suite

I takt med att cyberhoten utvecklas använder organisationer säkerhetsmodeller med nollförtroende för att skydda sig mot dataläckor. Dell Technologies hjälper IT-ledare att stärka slutpunktssäkerheten i virtuella miljöer med Dell ThinOS och Wyse Management Suite (WMS) som tillhandahåller en säker, hanterbar och policydriven lösning.

Lita inte på några enheter

I en nollförtroendemodell ska inte ens ThinOS-enheter automatiskt bli betrodda. Wyse Management Suite (WMS) möjliggör säker introduktion genom att placera nya klienter i en standardpolicygrupp, vilket kräver administratörsgodkännande innan konfigurationer tillämpas. Säkra anslutningar, till exempel 802.1x eller EAP-TLS med certifikat som hanteras via WMS eller en SCEP-server, ger förstärkt skydd. Ytterligare åtgärder, inklusive begränsning av kontobehörigheter, inställning av unika BIOS-lösenord och användning av en lista över nekade enheter, minskar säkerhetsriskerna ytterligare.

Lita inte på några program

I enhetsläge säkerställer Dell ThinOS säkert applikationsstöd genom sin utformning utan shell-åtkomst, AES-krypterade partitioner och säker start för att förhindra manipulering. Endast Dell-godkända programpaket kan distribueras via WMS via SSL, med hash- och signaturvalidering för att upptäcka skador eller obehöriga ändringar. Administratörer kan minska riskerna genom att endast distribuera nödvändiga mjukvarukomponenter och begränsa den kommersiella webbläsaranvändningen som tillval till viktiga arbetsflöden, minimera exponeringen och stärka säkerheten på programnivå.

Lita inte på några användare

Användaråtkomst i ThinOS-miljöer hanteras strikt i enlighet med nollförtroendeprinciper. Virtuell broker-autentisering säkerställer att användare endast kan komma åt de skrivbord eller program som tilldelats till dem. Multifaktorautentisering lägger till ett viktigt lager med identitetsskydd, samtidigt som integrering med plattformar som Imprivata OneSign eller Identity Automation stärker sessionskontrollen. Tillsammans hjälper dessa åtgärder till att blockera obehörig åtkomst och stödja efterlevnad av företagets säkerhetsstandarder.

Säker genom design

Skydda användarenheten

Skydda lokala data

Säker åtkomst till VDI-sessionen

Säker utformning

Dell ThinOS-operativsystemet är specialbyggt med säkerhet i centrum. Den är utformad som en enhetsbaserad lösning med en sluten arkitektur och hjälper till att minimera sårbarheter. Endast program och drivrutiner från tredje part som har testats noggrant, förpackats och certifierats av Dell får installeras, vilket säkerställer en kontrollerad och säker miljö för ditt verksamhetskritiska arbete.

Härdade ytor

Genom att kombinera säker avbildning och lagring med API:er som inte är offentligt tillgängliga bildar Dell ThinOS en härdad yta som skyddar mot virus och skadliga program som ofta utgör problem för Windows- och Linux-enheter.

Säker lagring

När du arbetar i enhetsläge finns det inget kommandogränssnitt eller möjlighet att fjärrvisa, ändra eller ta bort operativsystems-, program- eller konfigurationsfiler som lagras på klienten. Säkerheten upprätthålls ytterligare genom säker start och AES-enhetsspecifik flashkryptering, vilket ger ett robust skydd för kritiska komponenter.

Förhindra vanliga sårbarheter

Dell ThinOS är utformat med säkerhet i åtanke. Det kan ge ett robust skydd mot vanliga säkerhetshot genom att smidigt ansluta till virtuella miljöer utan att behöva en kommersiell webbläsare. Kunder som har avancerade behov kan välja att installera en.

Säker hantering

Skydda användarenheten

Skydda lokala data

Säker åtkomst till VDI-sessionen

BIOS- och CMOS-säkerhet

ThinOS gör det enkelt att fjärrskydda BIOS när du använder en Dell-klientenhet. Med bara några få klick kan du massdistribuera BIOS-uppgraderingar och -inställningar, till exempel BIOS-lösenord, på flera enheter med Wyse Management Suite Pro Edition.

Automatiserad certifikathantering

Globala certifikat kan enkelt distribueras med Wyse Management Suite. Dessutom har ThinOS stöd för SCEP (Simple Certificate Enrollment Protocol), som förenklar hanteringen av unika enhetscertifikat.

Säkra anslutningar

Wyse Management Suite kan hantera och uppgradera ThinOS-enheter på ett säkert sätt med hjälp av säkra, krypterade HTTPS-anslutningar i både offentliga och privata nätverk.

Säker avbildning

ThinOS-avbildningar är specialbyggda för att endast installeras på angivna Dell-klientenheter, vilket säkerställer optimal kompatibilitet och prestanda. Som ett skydd mot manipulering omfattar dessa avbildningar avancerade säkerhetsåtgärder när de distribueras via Wyse Management Suite eller Dell OS Recovery Tool.

Exempel på viktiga skydd:

- Validering av kontrollsumma för att verifiera dataintegritet
- Validering av digital signatur för att autentisera bildkällan
- Unika plattformstangenter för att säkerställa kompatibilitet med klienthårdvaran och det förinstallerade operativsystemet.

Säker kommunikation

Skydda användarenheten

Skydda lokala data

Säker åtkomst till VDI-sessionen

SSL-anslutningar

All kommunikation mellan utjämnare och protokoll kan utföras via säkra anslutningar. ThinOS-kommunikationspolicyer kan definieras på global eller individuell nivå för att upprätthålla önskad säkerhetsnivå. De tre nivåerna som stöds är:

- Hög – certifikatvalidering krävs
- Varning – användargodkännande krävs om kontrollen för certifikatvalidering misslyckas
- Låg – ingen certifikatvalidering krävs

Säkerhet för trådbunden och trådlös anslutning

All trådbunden och trådlös 802.1x företagskommunikation kan säkras med WPA/WPA2 PSK/Enterprise med EAP-PEAP, EAP-LEAP, EAP-TLS eller EAP-FAST.

Säkerhet för utjämnarprotokoll

Precis som stationära Windows- och Linux-datorer möjliggör ThinOS krypterings- och komprimeringsfunktioner vid anslutning till virtuella miljöutjämnare och servrar med hjälp av RDP-, HDX-, BLAST-, DCV- och PCoIP-protokoll. ThinOS är dessutom FIPS 140-2-kompatibelt för att upprätta säker kommunikation i känsliga miljöer.

Lokal användarsäkerhet

Skydda slutanvändardata och kontrollera lokal användaråtkomst

Skydda användarenheten

Skydda lokala data

Säker åtkomst till VDI-sessionen

Manipuleringsskydd

Behörighetsinställningarna för ThinOS ger robust säkerhet för stationära datorer genom att begränsa användaråtkomst till skrivbordsmenyer, vilket förhindrar obehörig visning eller ändringar. IT-administratörer har fullständig åtkomst till användargränssnittet för att säkerställa fullständig kontroll och effektiv drift. ThinOS är dessutom utformat för att ansluta till en virtuell miljö utan att du behöver installera en lokal webbläsare.

Avancerad autentisering och tokens

Stöd för tokenbaserad autentisering med CAC- och PIV-smartkort med mellanprogrammen 90Meter och ActiveIdentity och Yubikey-enheter med FIDO2.

Skydda slutanvändaruppgifter

Som standard lagrar ThinOS-enheter inloggningsuppgifter och cacheobjekt för program (t.ex. sessionsbitmaps) enbart i RAM-minnet tills sessionen avslutas. Inga inloggningsuppgifter eller protokollobjekt skrivs till enhetens flashfilsystem. Däremot använder Windows- och Linux-baserade enheter ofta diskcacheminne för att bevara inloggningsuppgifter och programmens cacheminne, vilket gör dem mer sårbara för dataintrång eller hackning.

USB- och lokal disksäkerhet

Alla ThinOS-avbildningssystemfiler, paketfiler, cachelagrade konfigurationer och speglade datalagerobjekt som lagras på klientens lokala flashfilsystem är AES-krypterade för att minimera risken för att data utsätts för risk.

På enheter utrustade med TPM (Trusted Platform Module) lagras en del av hashnycklarna i den här komponenten. Även om flashmoduler tas bort från enheterna förblir data på dessa moduler oåtkomliga. Dessutom kan certifikat som används för att upprätta säkra SSL-anslutningar, när de har lästs in och lagrats på enhetens flash, inte exporteras.

- **All cachelagring sker till RAM-minne och är icke-beständig**
- **AES-kryptering tillämpas på alla partitioner/filer**
- **Återställning av fabriksinställningarna återställer enheten till det konfigurationstillstånd som levererades från fabriken**
- **Enhetsspecifik flashkryptering och säker start**

Dell ThinOS ger dig exakt kontroll över USB-masslagringsenheter. Du kan definiera vilka användare som har åtkomst och exakt hur de kan använda dessa enheter, vilket säkerställer både säkerhet och flexibilitet.

1 Flexible controls for IT support

Administratörsbehörighet kan användas för att styra felsökning av klienter. Kundloggar kan exporteras till WMS eller ett lokalt USB-minne.

Konfigurationer av klientenheter lagras på en säker flashpartition utan OS. Dessa konfigurationer kan rensas genom att återställa till fabriksinställningarna.

Klientcertifikat och avbildningsfiler lagras på en säker lagringspartition utan OS. Dessa certifikat kan rensas genom att återställa till fabriksinställningarna.

2 Flexibla kontroller för åtkomst till virtuella miljöer med USB-masslagring

ThinOS-BIOS

USB-portar kan aktiveras/inaktiveras via BIOS-konfigurationer, antingen lokalt på enheten eller via Wyse Management Suite-konsolen. Inaktivering av USB-portar gäller för alla USB-enhetsklasser.

Sekretess och säkerhet

Enhetssäkerhet tillåter eller nekar åtkomst till USB-enheter baserat på VID/PID eller USB-klass. Det gör det möjligt att selektivt begränsa åtkomsten till alla enheter som är anslutna till ThinOS-klientenheten.

Kringutrustning

USB-omdirigeringsinställningar kan användas för att tvinga stöd för USB-enhetsdrivrutiner att komma från en virtuell värd i stället för från ThinOS-klientenheten.

Sessionsinställningar

Globala och leverantörsspecifika partnerpolicyer kan användas för att styra mappning och omdirigering av USB-enheter.

De säkraste tunna klienterna med Dell ThinOS[1]

Säkerhet direkt från uppstart

Dells exklusiva operativsystem för tunna klienter har en säker utformning för att minimera risker och skydda virtuella skrivbord och Desktop-as-a-Service-sessioner.

Säker Hantering

Detaljerad centraliserad kontroll med Wyse Management Suite hjälper till att upprätthålla säkerhetspolicyer, konfigurera inställningar för enhetsöverensstämmelse och hantera BIOS.

Säkra SlutAnvändarUppgifter

Lagring av användaruppgifter i RAM-minnet hjälper till att skydda dem från skadliga program och rensar dem vid omstart, vilket minskar risken för obehörig åtkomst.

Betrodd slutpunkt

Stöd för populära autentiseringsmetoder, överensstämmelsestandarder och icke-beständig information hjälper till att skydda sessionsdata och tryggt ansluta var som helst.

Sluten arkitektur

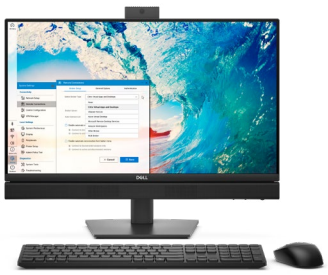
Inga känsliga data eller personliga uppgifter exponeras på den lokala enheten. Systemhärdning för att begränsa angreppsytor, opublicerade API:er samt krypterade data och filer som exklusivt förpackats av Dell för att förhindra virus och skadliga program.

Säkra Kommunikationer

ThinOS ger säker kommunikation genom att stödja SSL-anslutningar för alla utjämnarprotokoll och avancerade krypteringsmetoder för säker åtkomst till trådbundna och trådlösa företagsnätverk.

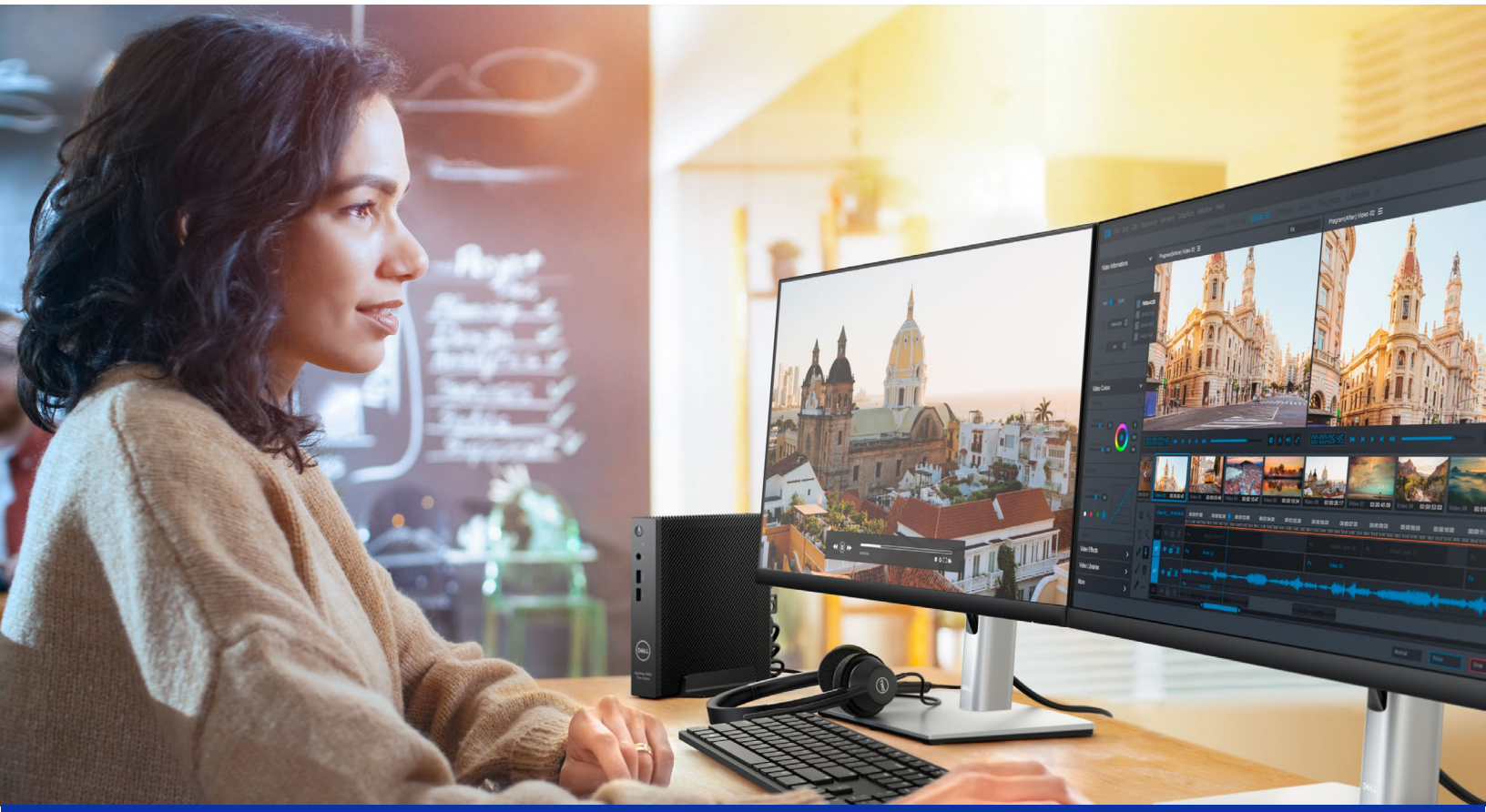
Utforska Dells lösningar för tunna klienter

OptiPlex 3000 tunn klient - >



Dell Pro allt-i-ett 35W - >

Dell Pro 14 bärbar dator - >



Arbeta tryggt var som helst med **Dell ThinOS och Dells lösningar för tunna klienter**

En optimerad och säker VDI-slutpunkt för den virtuella stationära datorinfrastrukturen och Desktop-as-a-Service-lösningar.

Besök oss
dell.com/CloudClientWorkspace

Läs mer
Bloggen Förenkla IT-hanteringen -->

Delta i konversationen
LinkedIn/X

Källor och ansvarsfriskrivningar

[1]Enligt Dells analys av Dell ThinOS i enhetsläge jämfört med konkurrerande produkter i januari 2025.

[2]Dell ThinOS Appliance Mode är standarddriftläget för Dell ThinOS, och det har utformats för att upprätthålla en robust säkerhetsställning från början. Med version 2508 och senare inför ThinOS större flexibilitet för IT-administratörer, vilket möjliggör installation av kommersiella webbläsaralternativ och distribution av mjukvarukomponenter från tredje part. För att säkerställa kompatibilitet med ThinOS 10 måste tredjepartsprogram vara kompatibla med Ubuntu 24.04 x86_64, inkludera ett Debian-installationspaket och klara alla OS-beroende kontroller i App Builder-verktyget, beroende på klientenhetens kapacitet. Distribution kräver att du väljer mellan isolerat eller inbyggt läge. Program som körs i inbyggt läge kan vara föremål för begränsningar baserat på deras driftsbeteende. Noggranna tester rekommenderas starkt för att bekräfta lyckad installation och funktion före driftsättning. Fullständig information om program som stöds och riktlinjer för distribution finns i Kundinstallationsguiden på Dell.com/support.