DELL Technologies

Beveiligingsvoordelen van Dell ThinOS

Werk vol vertrouwen op elke locatie

met oplossingen die zijn ontworpen om de beveiliging van uw virtuele desktops en Desktop-as-a-Service-omgevingen te verbeteren.

Voldoe aan de veranderende behoeften van werknemers en verhoog de efficiëntie zonder in te leveren op beveiliging met Cloud Client Workspace-software en thin client oplossingen van Dell.

Dell thin client-oplossingen zijn geoptimaliseerde VDI-eindpunten die speciaal zijn ontworpen voor een beveiligde en naadloze toegang tot gevirtualiseerde desktops en Desktop-as-a-Service-omgevingen met modern IT-beheer.

Minimaliseer het aanvalsoppervlak en krijg gemoedsrust met de exclusieve ThinOS van Dell, ons veiligste thin client-besturingssysteem[1] dat speciaal is gebouwd voor virtuele werkruimten.

Meer informatie over de portfolio ->

Dell ThinOS: klaar voor Zero Trust

Versterk Zero Trust-strategieën met Dell ThinOS en Wyse Management Suite

In reactie op nieuwe cyberbedreigingen passen organisaties Zero Trust-beveiligingsmodellen toe om zich te beschermen tegen datalekken. Dell Technologies helpt IT-leiders de eindpuntbeveiliging in virtuele omgevingen te versterken met Dell ThinOS en Wyse Management Suite (WMS), die een veilige, beheerbare en beleidsgestuurde oplossing leveren.

Vertrouw geen enkel apparaat

In een Zero Trust-model mogen zelfs ThinOS-apparaten niet automatisch worden vertrouwd. Wyse Management Suite (WMS) maakt beveiligde onboarding mogelijk door nieuwe clients in een standaard beleidsgroep te plaatsen. Er is goedkeuring van de beheerder is voordat configuraties worden toegepast. Beveiligde verbindingen, zoals 802.1x of EAP-TLS met certificaten die worden beheerd via WMS of een SCEP-server, bieden verbeterde bescherming. Aanvullende maatregelen, waaronder het beperken van accountbevoegdheden, het instellen van unieke BIOS-wachtwoorden en een blokkeringslijst voor apparaatbeveiliging, verminderen de beveiligingsrisico's nog verder.

Vertrouw geen enkele applicatie

In de apparaatmodus zorgt Dell ThinOS standaard voor veilige applicatiesupport zonder shell-toegang, AES-versleutelde partities en veilig opstarten om manipulatie te voorkomen. Alleen door Dell goedgekeurde applicatiepakketten kunnen worden geïmplementeerd via WMS via SSL, met hash- en handtekeningvalidatie om beschadiging of ongeautoriseerde wijzigingen te detecteren. Beheerders kunnen risico's verminderen door alleen noodzakelijke softwarecomponenten te implementeren en het gebruik van optionele commerciële browsers te beperken tot essentiële workflows. Zo kunnen ze de blootstelling minimaliseren en de beveiliging op applicatieniveau versterken.

Vertrouw geen enkele gebruiker

Gebruikerstoegang in ThinOS-omgevingen wordt strikt beheerd volgens Zero Trust-principes. Virtuele broker-authenticatie zorgt ervoor dat gebruikers alleen toegang hebben tot de desktops of applicaties die aan hen zijn toegewezen. Meervoudige verificatie voegt een kritieke laag van identiteitsbescherming toe, terwijl integratie met platforms zoals Imprivata OneSign of Identity Automation de sessiecontrole versterkt. Deze gecombineerde maatregelen helpen ongeautoriseerde toegang te blokkeren en naleving van beveiligingsnormen voor ondernemingen te ondersteunen.

Ontworpen voor veiligheid

Bescherm het apparaat van de gebruiker

Bescherm de lokale data

Veilige toegang tot de VDI-sessie

Veilig ontwerp

Bij het bouwen van het Dell ThinOS besturingssysteem stond beveiliging centraal. Het is ontworpen als een apparaatgebaseerde oplossing met een gesloten architectuur en helpt kwetsbaarheden te minimaliseren. Alleen externe applicaties en drivers die grondig zijn getest, verpakt en gecertificeerd door Dell, kunnen worden geïnstalleerd. Dit zorgt voor een gecontroleerde en veilige omgeving voor uw bedrijfskritieke activiteiten.

Veilige storage

De apparaatmodus heeft geen opdrachtshell of mogelijkheid om op afstand op de client opgeslagen besturingssysteem-, applicatie- of configuratiebestanden te bekijken, te wijzigen of te verwijderen. De beveiliging wordt verder afgedwongen via veilig opstarten en apparaatspecifieke AES-flash-versleuteling, die robuuste bescherming biedt voor kritieke componenten.

Verharde oppervlakken

Door beveiligde imaging en storage met niet-openbare API's te combineren creëert Dell ThinOS een verhard oppervlak dat bescherming biedt tegen virussen en malware die Windows- en Linux-apparaten vaak teisteren.

Voorkom veelvoorkomende beveiligingslekken

Dell ThinOS is ontworpen met het oog op veiligheid. Het systeem kan naadloos verbinding maken met virtuele omgevingen zonder dat u een commerciële browser nodig hebt, wat robuuste bescherming tegen veelvoorkomende beveiligingsbedreigingen biedt. Voor klanten met geavanceerde behoeften biedt het systeem de optie om er een te installeren.

Beveiligd beheer

Bescherm het apparaat van de gebruiker

Bescherm de lokale data

Veilige toegang tot de VDI-sessie

BIOS- en CMOS-beveiliging

Met ThinOS kunt u gemakkelijk op afstand uw BIOS beveiligen wanneer u een Dell clientapparaat gebruikt. Met Wyse Management Suite Pro Edition kunt u BIOS-upgrades en -instellingen, zoals BIOS-wachtwoorden, in een paar klikken op meerdere apparaten tegelijk implementeren.

Geautomatiseerd certificaatbeheer

U kunt algemene certificaten eenvoudig implementeren met behulp van de Wyse Management Suite. Bovendien ondersteunt ThinOS SCEP (Simple Certificate Enrollment Protocol), wat het beheer van unieke apparaatcertificaten vereenvoudigt.

Beveiligde verbindingen

Wyse Management Suite kan ThinOS apparaten veilig beheren en upgraden met behulp van beveiligde, versleutelde HTTPS-verbindingen op zowel openbare als privénetwerken.

Veilige imaging

ThinOS images zijn speciaal ontworpen voor exclusieve installatie op gespecificeerde Dell clientapparaten, zodat optimale compatibiliteit en prestaties gegarandeerd zijn. Om manipulatie te voorkomen, bevatten deze images geavanceerde beveiligingsmaatregelen wanneer ze worden geïmplementeerd via de Wyse Management Suite of de Dell OS Recovery Tool.

Belangrijke beveiligingen zijn onder andere:

- Checksum-validatie om data-integriteit te verifiëren
- Validatie van digitale handtekening om de imagebron te verifiëren
- Unieke platformsleutels om compatibiliteit met de clienthardware en het vooraf geïnstalleerde besturingssysteem te garanderen

Beveiligde communicatie

Bescherm het apparaat van de gebruiker

Bescherm de lokale data

Veilige toegang tot de VDI-sessie

SSL-verbindingen

Alle leverancier- en protocolcommunicatie kan via beveiligde verbindingen verlopen. ThinOS communicatiebeleid kan op algemeen of individueel niveau worden gedefinieerd om het gewenste beveiligingsniveau af te dwingen. De drie 'ondersteunde' niveaus zijn:

- Hoog – certificaatvalidatie vereist
- Waarschuwing – acceptatie door de gebruiker vereist als de validatiecontrole van het certificaat mislukt
- Laag – geen certificaatvalidatie vereist

Bekabelde en draadloze beveiliging

Alle bekabelde en draadloze 802.1x-bedrijfscommunicatie kan worden beveiligd met WPA/WPA2 PSK/Enterprise met EAP-PEAP, EAP-LEAP, EAP-TLS of EAP-FAST.

Beveiliging van leveranciersprotocol

Net als Windows- en Linux-desktops schakelt ThinOS versleutelings- en compressiefuncties in bij de koppeling met makelaars van virtuele omgevingen en met servers, met behulp van RDP-, HDX-, BLAST-, DCV- en PCoIP-protocollen. Bovendien is ThinOS geschikt voor FIPS 140-2 om veilige communicatie in gevoelige omgevingen te garanderen.

Beveiliging lokale gebruikers

Bescherm eindgebruikersdata en beheer toegang van lokale gebruikers

Bescherm het apparaat van de gebruiker

Bescherm de lokale data

Veilige toegang tot de VDI-sessie

Beveiliging tegen manipulatie

Privilege-instellingen van ThinOS bieden robuuste desktopbeveiliging door de gebruikerstoegang tot desktopmenu's te beperken, waardoor ongeautoriseerde weergave of wijzigingen worden voorkomen. IT-beheerders hebben volledige toegang tot de gebruikersinterface om volledige controle en gestroomlijnde activiteiten te garanderen. Bovendien is ThinOS ontworpen om verbinding te maken met een virtuele omgeving zonder dat u een lokale browser hoeft te installeren.

Geavanceerde verificatie en tokens

Ondersteuning voor op tokens gebaseerde verificatie met CAC- en PIV-smartcards met 90Meter en ActiveIdentity middleware, en Yubikey-apparaten met FIDO2.

Beveiligde eindgebruikersreferenties

ThinOS apparaten slaan standaard aanmeldgegevens en applicatiecacheobjecten (zoals sessiebitmaps) uitsluitend op in RAM totdat de sessie wordt beëindigd. Er worden geen aanmeldgegevens of protocolobjecten naar het flash-bestandssysteem van het apparaat geschreven. Windows- en Linux-apparaten gebruiken daarentegen vaak een schijfcache om referenties en applicatiecache te bewaren, waardoor ze kwetsbaarder zijn voor datalekken of hacking.

Beveiliging van USB en lokale schijf

Alle ThinOS imagesysteembestanden, pakketbestanden, in de cache opgeslagen configuraties en gespiegelde repository-objecten die zijn opgeslagen op het lokale flash-bestandssysteem van de client zijn AES-versleuteld om het risico op data-inbreuk te minimaliseren.

Bij eenheden die zijn uitgerust met een Trusted Platform Module (TPM), wordt een deel van de hashsleutels in dit onderdeel opgeslagen. Hierdoor blijven de data op deze modules ontoegankelijk, zelfs als flash-modules van de apparaten worden verwijderd. Bovendien kunnen certificaten die zijn gebruikt om beveiligde SSL-verbindingen tot stand te brengen, niet worden geëxporteerd nadat ze zijn geladen en opgeslagen in de flash van het apparaat.

- **Alle caching is naar RAM en is niet-permanent**
- **AES-versleuteling wordt toegepast op alle partities/bestanden**
- **Terugzetten naar fabrieksinstellingen herstelt het apparaat naar de configuratie waarmee hij vanuit de fabriek is verzonden**
- **Apparaatspecifieke flash-versleuteling en veilig opstarten**

Met Dell ThinOS hebt u nauwkeurige controle over USB-storageapparaten. U kunt bepalen welke gebruikers toegang hebben en hoe ze deze apparaten precies kunnen gebruiken, zodat zowel beveiliging als flexibiliteit gegarandeerd zijn.

1 Flexible controls for IT support

Met beheerdersbevoegdheden kunt u probleemoplossing voor clients beheren. U kunt clientlogboeken exporteren naar WMS of een lokale USB-stick.

Configuraties van clientapparaten worden opgeslagen op een veilige flash-partitie zonder besturingssysteem. U kunt deze configuraties wissen door de fabrieksinstellingen te herstellen.

Clientcertificaten en imagebestanden worden opgeslagen op een veilige storagepartitie zonder besturingssysteem. U kunt deze certificaten wissen door de fabrieksinstellingen te herstellen.

2 Flexibele bedieningselementen voor toegang tot virtuele omgevingen voor USB-massastorage

ThinOS BIOS

U kunt USB-poorten in- en uitschakelen via BIOS-configuraties,ofwel lokaal op het apparaat ofwel via de console van de Wyse Management Suite. Het uitschakelen van USB-poorten is van toepassing op alle USB-apparaatklassen.

Privacy en veiligheid

Apparaatbeveiliging staat toegang tot USB-apparaten toe of weigert deze op basis van VID/PID of USB-klasse. Hiermee kunt u de toegang tot elk apparaat dat is aangesloten op het ThinOS clientapparaat selectief beperken.

Randapparaten

U kunt de instellingen voor USB-omleiding gebruiken om te forceren dat ondersteuning voor USB-apparaatdrivers van een virtuele host komt in plaats van het ThinOS clientapparaat.

Sessie-instellingen

Met algemeen en leveranciersspecifiek partnerbeleid kunt u de toewijzing en omleiding van USB-apparaten beheren.

De veiligste thin clients met Dell ThinOS[1]

Wees veilig vanaf de eerste keer opstarten

Het exclusieve thin client-besturingssysteem van Dell is ontworpen voor veiligheid, zodat risico's worden geminimaliseerd en virtuele desktops en Desktop-as-a-Service-sessies worden beschermd.

Veilig BEHEER

Door gedetailleerd gecentraliseerd beheer van Wyse Management Suite kunt u het beveiligingsbeleid afdwingen, nalevingsinstellingen voor apparaten configureren en het BIOS beheren.

Veilige EINDGEBRUIKERSREFERENTIES

Door gebruikersreferenties in RAM op te slaan blijven ze veilig voor malware en worden ze verwijderd bij opnieuw opstarten, wat het risico op onbevoegde toegang vermindert.

Vertrouwd eindpunt

Ondersteuning voor populaire verificatiemethoden, nalevingsstandaarden en niet-aanhoudende informatie helpt om sessiedata te beschermen en overal met vertrouwen verbinding te maken.

Gesloten architectuur

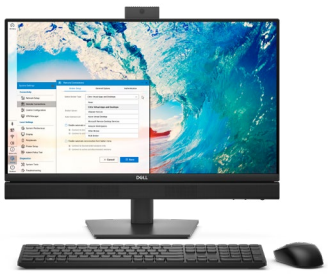
Er worden geen gevoelige data of persoonlijke informatie op het lokale apparaat blootgesteld. Systeemverharding om kwetsbaarheid voor aanvallen te beperken, niet-gepubliceerde API's, en versleutelde data en bestanden die exclusief door Dell zijn verpakt, helpen om virus- en malware te voorkomen.

Veilige COMMUNICATIE

ThinOS garandeert veilige communicatie door SSL-verbindingen te ondersteunen voor alle leveranciersprotocollen en geavanceerde versleutelingsmethoden voor veilige toegang tot bekabelde en draadloze bedrijfsnetwerken.

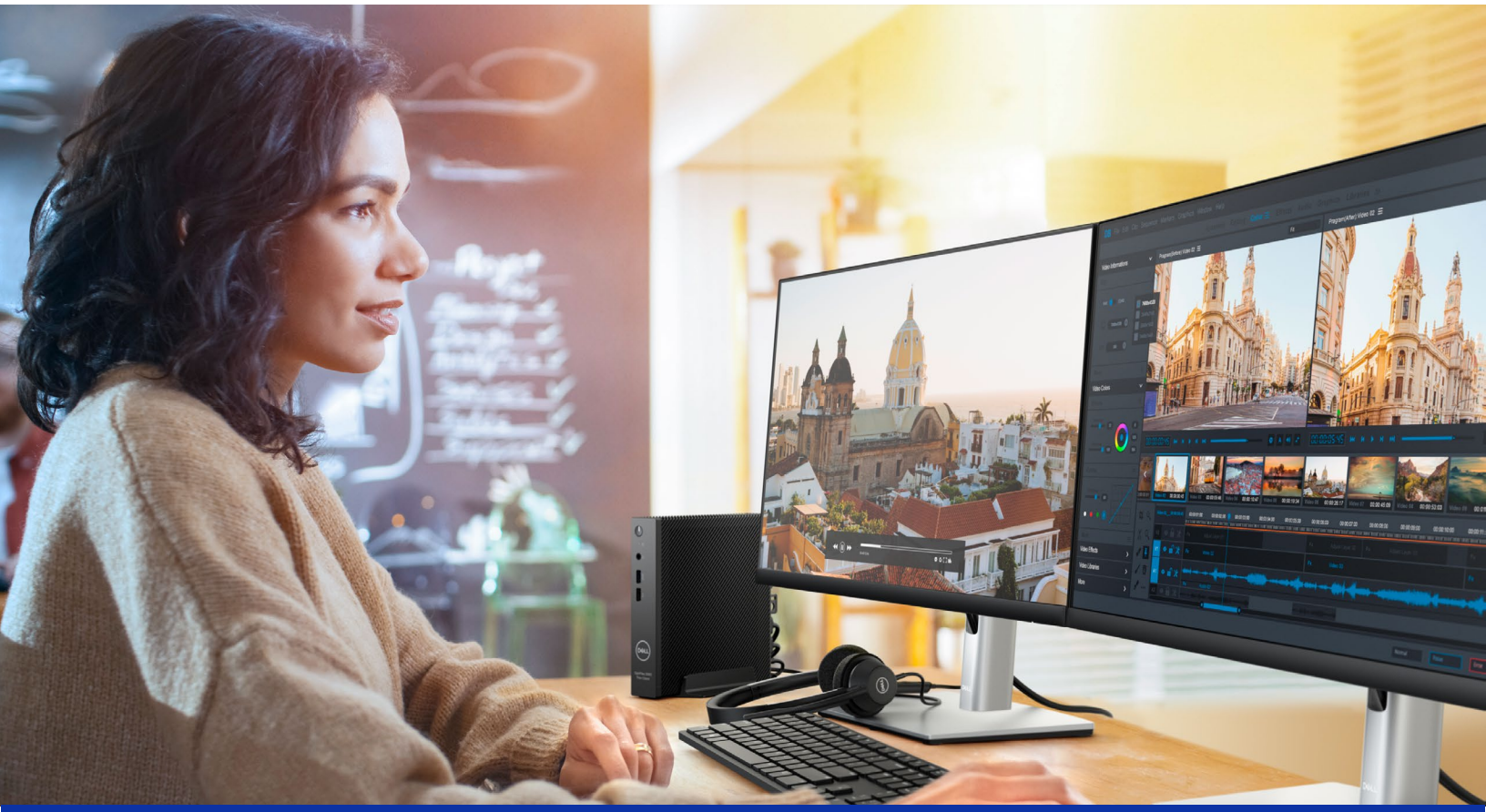
Ontdek Dell Thin Client-oplossingen

OptiPlex 3000 thin client - >



Dell Pro alles-in-één 35 W - >

Dell Pro 14 laptop - >



Werk vol vertrouwen op elke locatie met **Dell ThinOS en Dell thin client-oplossingen**

Een geoptimaliseerd en veilig VDI-eindpunt voor uw Virtual Desktop Infrastructure en Desktop-as-a-Service-oplossingen.

Ga naar:
dell.com/CloudClientWorkspace

Meer informatie
Blog IT vereenvoudigen -->

Deelnemen aan het gesprek
LinkedIn / X

Bronnen en disclaimers

[1]Gebaseerd op een analyse van Dell van ThinOS in apparaatmodus versus concurrerende producten, januari 2025.

[2] De Dell ThinOS apparaatmodus is de standaard werkingsstatus van Dell ThinOS. Deze is ontworpen om vanaf het begin een robuuste beveiligingsmentaliteit af te dwingen. Vanaf versie 2508 biedt ThinOS IT-beheerders meer flexibiliteit, waardoor de installatie van commerciële browsers en de implementatie van softwarecomponenten van derden mogelijk is. Om compatibiliteit met ThinOS 10 te garanderen, moeten applicaties van derden compatibel zijn met Ubuntu 24.04 x86_64, een Debian-installatiepakket bevatten en met succes alle OS-afhankelijkheidscontroles in de App Builder-tool doorstaan, afhankelijk van de mogelijkheden van het clientapparaat. Voor de implementatie moet u kiezen tussen de geïsoleerde of systeemeigen modus. Op applicaties die in de systeemeigen modus worden uitgevoerd, worden mogelijk beperkingen toegepast afhankelijk van hun werkingsgedrag. Dell raadt sterk om voorafgaand aan de implementatie grondig te testen op een succesvolle installatie en functionaliteit. Voor volledige informatie over ondersteunde applicaties en implementatierichtlijnen raadpleegt u de installatiehandleiding voor klanten die beschikbaar is op dell.com/support.