DELL Technologies

Beneficios para la seguridad de Dell ThinOS

Trabaje con confianza desde cualquier lugar

con soluciones diseñadas para aumentar la seguridad de sus escritorios virtuales y entornos de escritorio como servicio.

Satisfaga las necesidades cambiantes de los empleados y aumente la eficiencia sin arriesgar la seguridad con el software Cloud Client Workspace y las soluciones de cliente ligero de Dell.

Las soluciones de cliente ligero Dell son puntos finales de VDI optimizados y diseñados específicamente para ofrecer un acceso seguro y sin complicaciones a escritorios virtualizados y entornos de escritorio como servicio con una administración de TI moderna.

Minimice la superficie de ataque y disfrute de tranquilidad con el exclusivo ThinOS de Dell, nuestro sistema operativo de cliente ligero más seguro[1], diseñado a medida para espacios de trabajo virtuales.

Obtenga más información sobre el catálogo ->

Dell ThinOS: preparado para la confianza cero

Refuerce las estrategias de confianza cero con Dell ThinOS y Wyse Management Suite

Con la evolución de las ciberamenazas, las organizaciones están adoptando modelos de seguridad de confianza cero para protegerse contra las vulneraciones de datos. Dell Technologies ayuda a los líderes de TI a reforzar la seguridad de los puntos finales en entornos virtuales con Dell ThinOS y Wyse Management Suite (WMS), que ofrecen una solución segura, fácil de gestionar y basada en políticas.

No confíe en ningún dispositivo

En un modelo de confianza cero, no se debería confiar automáticamente ni siquiera en los dispositivos con ThinOS. Wyse Management Suite (WMS) permite la incorporación segura mediante la colocación de nuevos clientes en un grupo de políticas predeterminado, lo que requiere la aprobación del administrador antes de aplicar configuraciones. Las conexiones seguras, como 802.1x o EAP-TLS con certificados gestionados a través de WMS o un servidor SCEP, proporcionan una protección mejorada. Medidas adicionales, como la limitación de privilegios de cuentas, la configuración de contraseñas únicas del BIOS y el uso de una lista de denegación de seguridad de dispositivos, reducen aún más los riesgos de seguridad.

No confíe en ninguna aplicación

En el modo de dispositivo, Dell ThinOS garantiza, por diseño, la compatibilidad con aplicaciones seguras sin acceso al shell, particiones cifradas con AES y arranque seguro para prevenir manipulaciones. Solo los paquetes de aplicaciones aprobados por Dell pueden implementarse a través de WMS sobre SSL, con validación de hash y firma para detectar daños o cambios no autorizados. Los administradores pueden reducir el riesgo implementando solo los componentes de software necesarios y limitando el uso opcional de navegadores comerciales a los flujos de trabajo esenciales, lo que minimiza la exposición y refuerza la seguridad en el nivel de las aplicaciones.

No confíe en ningún usuario

El acceso de los usuarios en entornos de ThinOS se gestiona estrictamente para que se ajuste a los principios de confianza cero. La autenticación de agentes virtuales garantiza que los usuarios solo puedan acceder a los equipos de sobremesa o las aplicaciones que se les hayan asignado. La autenticación multifactor aporta una capa crítica de protección de identidad, al tiempo que se integra con plataformas como Imprivata OneSign o Identity Automation para reforzar el control de las sesiones. Estas medidas combinadas ayudan a bloquear el acceso no autorizado y respaldan el cumplimiento normativo de los estándares de seguridad empresariales.

Diseño seguro

Protección del dispositivo del usuario

Protección de los datos locales

Acceso seguro a la sesión de VDI

Diseño seguro

El sistema operativo Dell ThinOS se ha diseñado a medida con la seguridad en el núcleo. Diseñado como una solución basada en dispositivo con una arquitectura cerrada, ayuda a minimizar las vulnerabilidades. Solo las aplicaciones y los controladores de otros fabricantes probados, empaquetados y certificados rigurosamente por Dell se pueden instalar, lo que garantiza un entorno seguro y controlado para sus operaciones de misión crítica.

Almacenamiento seguro

Mientras funciona en el modo de dispositivo, no hay shell de comandos ni capacidad para visualizar, modificar o eliminar de forma remota el sistema operativo, las aplicaciones o los archivos de configuración almacenados en el cliente. La seguridad se aplica aún más a través de arranque seguro y cifrado flash específico del dispositivo AES, lo que ofrece una protección sólida de los componentes críticos.

Superficies reforzadas

Mediante la combinación de imágenes y almacenamiento seguros con API no disponibles públicamente, Dell ThinOS crea una superficie reforzada que protege contra los virus y el malware que a menudo afectan a los dispositivos con Windows y Linux.

Prevención de vulnerabilidades comunes

Dell ThinOS se ha diseñado teniendo en cuenta la seguridad. Para disfrutar de una protección sólida contra las amenazas de seguridad comunes, se puede conectar perfectamente con entornos virtuales sin necesidad de un navegador comercial. Para los clientes con necesidades avanzadas, ofrece la opción de instalar uno.

Gestión segura

Protección del dispositivo del usuario

Protección de los datos locales

Acceso seguro a la sesión de VDI

Seguridad de BIOS y CMOS

ThinOS facilita la protección remota de su BIOS cuando se utiliza un dispositivo de cliente de Dell. Con tan solo unos clics, puede implementar masivamente actualizaciones y configuraciones del BIOS, como contraseñas del BIOS, en varios dispositivos mediante Wyse Management Suite Pro Edition.

Gestión automatizada de certificados

Los certificados globales se pueden implementar fácilmente con Wyse Management Suite. Además, ThinOS es compatible con Simple Certificate Enrollment Protocol (SCEP), lo que simplifica la gestión de certificados de dispositivos únicos.

Conexiones seguras

Wyse Management Suite puede gestionar y actualizar de forma segura los dispositivos con ThinOS mediante conexiones HTTPS seguras y cifradas tanto en redes públicas como privadas.

Imágenes seguras

Las imágenes de ThinOS se han diseñado a medida para su instalación exclusiva en dispositivos de cliente de Dell específicos, lo que garantiza una compatibilidad y un rendimiento óptimos. Para ofrecer protección contra la manipulación, estas imágenes incorporan medidas avanzadas de seguridad cuando se implementan a través de Wyse Management Suite o Dell OS Recovery Tool.

Las protecciones clave incluyen:

- Validación de la suma de comprobación para verificar la integridad de los datos
- Validación de firma digital para autenticar el origen de la imagen
- Claves de plataforma únicas para garantizar la compatibilidad con el hardware de cliente y el sistema operativo preinstalado

Comunicaciones seguras

Protección del dispositivo del usuario

Protección de los datos locales

Acceso seguro a la sesión de VDI

Conexiones SSL

Todas las comunicaciones de intermediarios y protocolos se pueden completar a través de conexiones seguras. Las políticas de comunicación de ThinOS se pueden definir en un nivel global o individual para imponer el nivel de seguridad deseado. Los tres niveles "compatibles" son:

- Alto: requiere validación del certificado
- Advertencia: requiere aceptación del usuario si la comprobación de validación del certificado falla
- Bajo: no requiere validación del certificado

Seguridad inalámbrica y con cable

Todas las comunicaciones empresariales inalámbricas y con cable 802.1x se pueden proteger mediante WPA/WPA2 PSK/Enterprise con EAP-PEAP, EAP-LEAP, EAP-TLS o EAP-FAST.

Seguridad de protocolos de intermediarios

Al igual que los equipos de escritorio con Windows y Linux, ThinOS permite funciones de cifrado y compresión cuando se conecta a intermediarios de entornos virtuales y servidores mediante los protocolos RDP, HDX, BLAST, DCV y PCoIP. Además, ThinOS es compatible con FIPS 140-2 para garantizar comunicaciones seguras en entornos confidenciales.

Seguridad de los usuarios locales

Protección de los datos de los usuarios finales y control de acceso de los usuarios locales

Protección del dispositivo del usuario

Protección de los datos locales

Acceso seguro a la sesión de VDI

Protección frente a manipulaciones

La configuración de privilegios de ThinOS ofrece una seguridad sólida de los equipos de escritorio mediante la restricción del acceso de usuario al menú del escritorio, con lo que se evitan la visualización o los cambios no autorizados. Los administradores de TI cuentan con acceso completo a la interfaz de usuario para garantizar un control total y operaciones optimizadas. Además, ThinOS se ha diseñado para conectarse a un entorno virtual sin necesidad de instalar un navegador local.

Autenticación y tokens avanzados

Se ofrece compatibilidad con autenticación basada en tokens mediante tarjetas inteligentes CAC y PIV con middleware 90Meter y ActiveIdentity, además de dispositivos Yubikey con FIDO2.

Protección de las credenciales de los usuarios finales

De forma predeterminada, los dispositivos con ThinOS almacenan las credenciales de inicio de sesión y los objetos de la caché de aplicaciones (como los mapas de bits de sesiones) exclusivamente en la RAM hasta que finaliza la sesión. No se escriben credenciales de inicio de sesión ni objetos de protocolos en el sistema de archivos flash del dispositivo. Por el contrario, los dispositivos basados en Windows y Linux a menudo utilizan la caché de disco para conservar las credenciales y la caché de aplicaciones, lo que hace que sean más vulnerables a las vulneraciones de datos o la piratería.

Seguridad de USB y discos locales

Todos los archivos del sistema de imágenes de ThinOS, los archivos de paquetes, las configuraciones almacenadas en caché y los objetos del repositorio reflejados que se almacenen en el sistema de archivos flash local del cliente se cifran mediante AES para minimizar el riesgo de comprometer los datos.

En el caso de las unidades equipadas con un módulo de plataforma de confianza (TPM), una parte de las claves hash se almacena dentro de este componente. En consecuencia, incluso si los módulos flash se retiran de los dispositivos, los datos de estos módulos siguen siendo inaccesibles. Además, los certificados utilizados para establecer conexiones SSL seguras, una vez cargados y almacenados en la memoria flash del dispositivo, no se pueden exportar.

- **Todo el almacenamiento en caché se realiza en la RAM y no es persistente**
- **El cifrado AES se aplica a todas las particiones y archivos**
- **El restablecimiento de los valores de fábrica restaura el dispositivo al estado de configuración en el que se envió desde la fábrica**
- **Arranque seguro y cifrado flash específico del dispositivo**

Dell ThinOS le ofrece un control preciso de los dispositivos de almacenamiento masivo USB. Puede definir qué usuarios tienen acceso y cómo pueden usar exactamente estos dispositivos, lo que garantiza la seguridad y flexibilidad.

1 Flexible controls for IT support

El privilegio administrativo se puede usar para controlar la solución de problemas del cliente. Los registros del cliente se pueden exportar a WMS o a una llave USB local.

Las configuraciones del dispositivo de cliente se almacenan en una partición flash segura que no es del sistema operativo. Estas configuraciones se pueden borrar mediante un restablecimiento de los valores de fábrica.

Los certificados y los archivos de imagen del cliente se almacenan en una partición de almacenamiento segura que no es del sistema operativo. Estos certificados se pueden borrar mediante un restablecimiento de los valores de fábrica.

2 Controles flexibles para el acceso a entornos virtuales de almacenamiento masivo USB

BIOS de ThinOS

Los puertos USB se pueden activar/desactivar a través de las configuraciones del BIOS, ya sea localmente en el dispositivo o a través de la consola de Wyse Management Suite. La desactivación de los puertos USB se aplica todas las clases de dispositivos USB.

Privacidad y seguridad

La seguridad del dispositivo permite o rechaza el acceso a los dispositivos USB en función del VID/PID o la clase de USB. Permite restringir selectivamente el acceso a cualquier dispositivo conectado al dispositivo de cliente ThinOS.

Periféricos

La configuración de redireccionamiento de USB se puede usar para forzar que la compatibilidad con controladores de dispositivos USB provenga de un host virtual, en lugar del dispositivo de cliente ThinOS.

Configuración de la sesión

Las políticas de partners globales y específicas de proveedores se pueden usar para controlar la asignación y el redireccionamiento de dispositivos USB.

Los clientes ligeros más seguros con Dell ThinOS[1]

Esté protegido desde el primer arranque

El sistema operativo de cliente ligero exclusivo de Dell es seguro por diseño para minimizar los riesgos y proteger los escritorios virtuales y las sesiones de escritorio como servicio.

Administración segura

El control granular centralizado desde Wyse Management Suite ayuda a imponer las políticas de seguridad, configurar los ajustes de cumplimiento normativo de los dispositivos y gestionar el BIOS.

Credenciales De Usuarios Finales seguras

El almacenamiento de las credenciales de usuario en la RAM ayuda a mantenerlas a salvo del malware y las elimina al reiniciar, lo que reduce el riesgo de acceso no autorizado.

Punto final de confianza

La compatibilidad con métodos de autenticación populares, estándares de cumplimiento normativo e información no persistente ayuda a proteger los datos de las sesiones y conectarse con confianza desde cualquier lugar.

Arquitectura cerrada

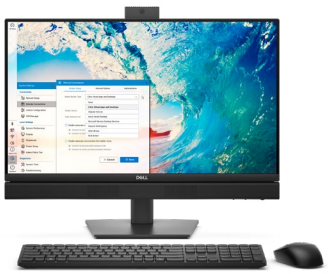
No se exponen datos confidenciales ni información personal en el dispositivo local. El reforzamiento del sistema para limitar las superficies de ataque, las API no publicadas, los datos cifrados y los archivos empaquetados exclusivamente por Dell ayudan a prevenir los virus y el malware.

Comunicaciones seguras

ThinOS garantiza comunicaciones seguras a través de la compatibilidad con conexiones SSL para todos los protocolos de intermediarios y los métodos de cifrado avanzados, para un acceso seguro a las redes empresariales inalámbricas y con cable.

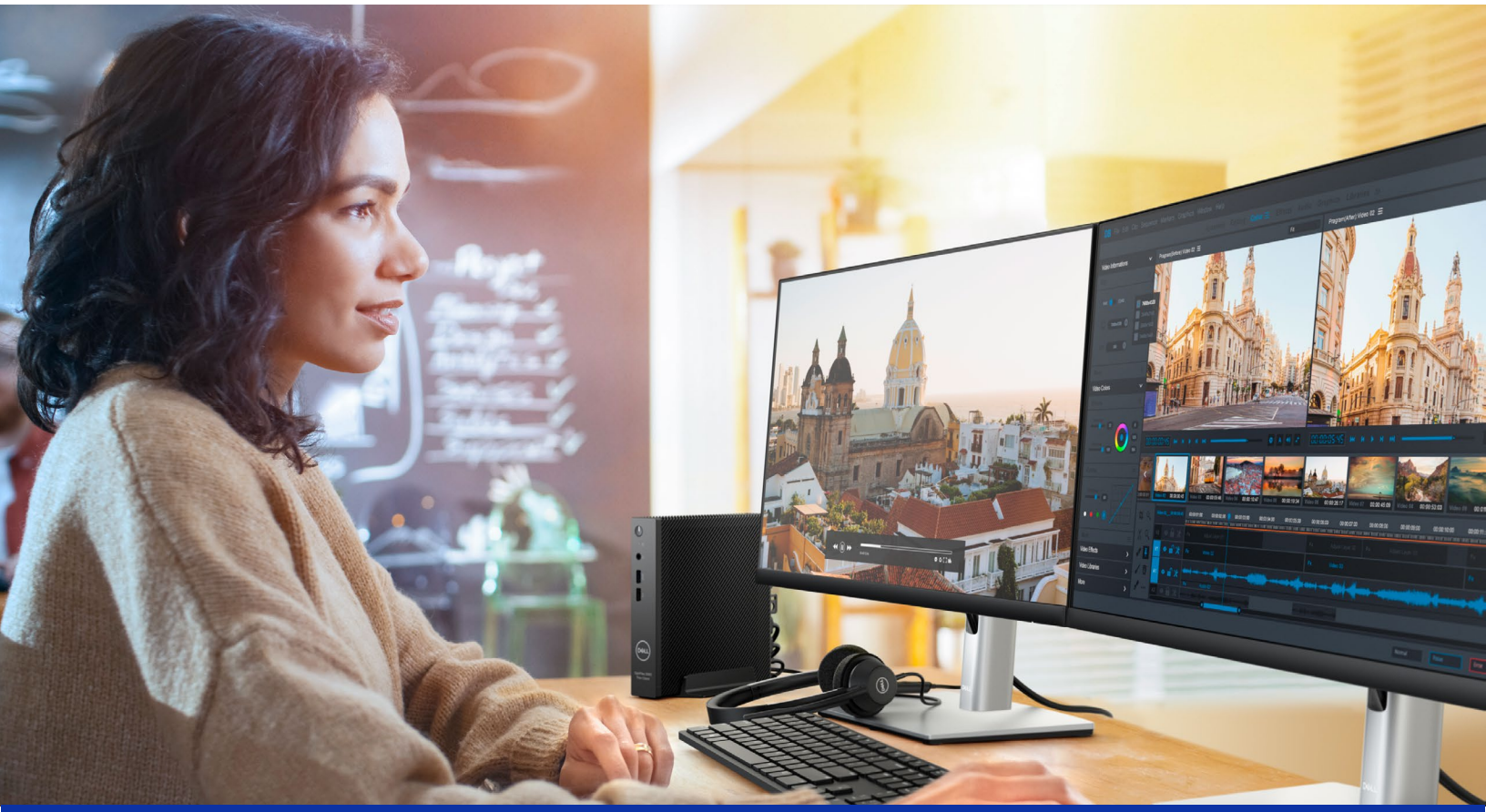
Explorar soluciones para clientes ligeros de Dell

Cliente ligero OptiPlex 3000 - >



Dell Pro All-in-One 35 W - >

Portátil Dell Pro 14 - >



Trabaje con confianza desde cualquier lugar con **Dell ThinOS y las soluciones para clientes ligeros de Dell**

Un punto final de VDI optimizado y seguro para su infraestructura de escritorio virtual y sus soluciones de escritorio como servicio.

Visítenos
dell.com/CloudClientWorkspace

Más información
Blog Simplifique la TI -->

Participe en la conversación
LinkedIn / X

Fuentes y renuncias:

[1] Según análisis de Dell comparando Dell ThinOS en el modo de dispositivo frente a productos de la competencia de enero de 2025.

[2]El modo de dispositivo de Dell ThinOS es el estado operativo predeterminado de Dell ThinOS, diseñado para aplicar un estado de seguridad sólido desde el principio. Con la versión 2508 y posteriores, ThinOS presenta una mayor flexibilidad para los administradores de TI, lo que permite instalar opciones de navegadores comerciales e implementar componentes de software de otros fabricantes. Para garantizar la compatibilidad con ThinOS 10, las aplicaciones de otros fabricantes deben ser compatibles con Ubuntu 24.04 x86_64, incluir un paquete de instalación de Debian y superar correctamente todas las comprobaciones de dependencia del sistema operativo utilizando la herramienta App Builder (dependiendo de las capacidades del dispositivo de cliente). La implementación requiere seleccionar entre el modo aislado o nativo. Las aplicaciones que se ejecutan en modo nativo pueden estar sujetas a restricciones en función de su comportamiento operativo. Se recomienda encarecidamente realizar pruebas exhaustivas para confirmar la instalación y la funcionalidad correctas antes de la implementación. Para obtener información completa sobre las aplicaciones compatibles y las directrices de implementación, consulte la guía de instalación para clientes disponible en Dell.com/support.