DELL Technologies

Dell ThinOS Security Benefits

Work confidently from anywhere

with solutions designed to augment the security of your virtual desktops and Desktop-as-a-Service environments.

Meet the evolving needs of the workforce and increase efficiency without compromising on security with Cloud Client Workspace software and Dell thin client solutions.

Dell thin client solutions are optimized VDI endpoints purposefully designed to deliver secure and seamless access to virtualized desktops and Desktop-as-a-Service environments with modern IT management.

Minimize the attack surface and experience peace of mind with Dell's exclusive ThinOS, our most secure thin client operating system[1] purpose-built for virtual workspaces.

Learn more about the portfolio ->

Dell ThinOS: Zero Trust ready

Strengthen Zero Trust strategies with Dell ThinOS and Wyse Management Suite

As cyber threats evolve, organizations are adopting Zero Trust security models to protect against data breaches. Dell Technologies helps IT leaders strengthen endpoint security in virtual environments with Dell ThinOS and Wyse Management Suite (WMS) delivering a secure, manageable and policy-driven solution.

Trust No Devices

In a Zero Trust model, even ThinOS devices should not be automatically trusted. Wyse Management Suite (WMS) enables secure onboarding by placing new clients in a default policy group, requiring admin approval before applying configurations. Secure connections, such as 802.1x or EAP-TLS with certificates managed through WMS or a SCEP server, provide enhanced protection. Additional measures, including limiting account privileges, setting unique BIOS passwords and using a Device Security Deny List, further reduce security risks.

Trust No Applications

In appliance mode, Dell ThinOS ensures, by design, secure application support with no shell access, AES-encrypted partitions and secure boot to prevent tampering. Only Dell-approved application packages can be deployed via WMS over SSL, with hash and signature validation to detect corruption or unauthorized changes. Administrators can reduce risk by deploying only necessary software components and limiting the optional commercial browser use to essential workflows, minimizing exposure and strengthening application-level security.

Trust No Users

User access in ThinOS environments is strictly managed to align with Zero Trust principles. Virtual broker authentication ensures users can only access the desktops or applications assigned to them. Multifactor authentication adds a critical layer of identity protection, while integration with platforms like Imprivata OneSign or Identity Automation to strengthen session control. These combined measures help block unauthorized access and support compliance with enterprise security standards.

Secure by design

Protect the user device

Protect the local data

Secure access to the VDI session

Secure Design

The Dell ThinOS operating system is purpose-built with security at its core. Designed as an appliance-based solution with a closed architecture, it helps to minimize vulnerabilities. Only third-party applications and drivers that have been rigorously tested, packaged and certified by Dell can be installed, ensuring a controlled and secure environment for your mission-critical operations.

Secure Storage

While operating in Appliance Mode, there is no command shell or the ability to remotely view, alter or delete operating system, application or configuration files stored on the client. Security is further enforced through Secure Boot and AES device-specific flash encryption, providing robust protection for critical components.

Hardened Surfaces

By combining secure imaging and storage with non-publicly available APIs, Dell ThinOS creates a hardened surface that protects against viruses and malware that often plague Windows and Linux devices.

Prevent Common Vulnerabilities

Dell ThinOS is designed with safety in mind. For robust protection against common security threats, it can seamlessly connect to virtual environments without needing a commercial browser. For customers with advanced needs, it offers the option to install one.

Secure Management

Protect the user device

Protect the local data

Secure access to the VDI session

BIOS and CMOS Security

ThinOS makes it easy to remotely secure your BIOS when using a Dell client device. In just a few clicks you can mass-deploy BIOS upgrades and settings, such as BIOS passwords, across multiple devices using Wyse Management Suite Pro Edition.

Automated Certificate Management

Global certificates can easily be deployed using Wyse Management Suite. Additionally, ThinOS supports Simple Certificate Enrollment Protocol (SCEP), simplifying the management of unique device certificates.

Secure Connections

Wyse Management Suite can securely manage and upgrade ThinOS devices using secure, encrypted HTTPS connections on both public and private networks.

Secure Imaging

ThinOS images are purpose-built for installation exclusively on specified Dell client devices, ensuring optimal compatibility and performance. To safeguard against tampering, these images incorporate advanced security measures when deployed through Wyse Management Suite or the Dell OS Recovery Tool.

Key protections include:

- Checksum validation to verify data integrity
- Digital signature validation to authenticate the image source
- Unique platform keys to ensure compatibility with the client hardware and pre-installed operating system

Secure Communications

Protect the user device

Protect the local data

Secure access to the VDI session

SSL Connections

All broker and protocol communications can be completed over secure connections. ThinOS communication policies can be defined at a global or individual level to enforce the desired security level. The three "supported" levels are:

- High – Certificate validation required
- Warning – User acceptance required if the certificate validation check fails
- Low – No certificate validation require

Wired and Wireless Security

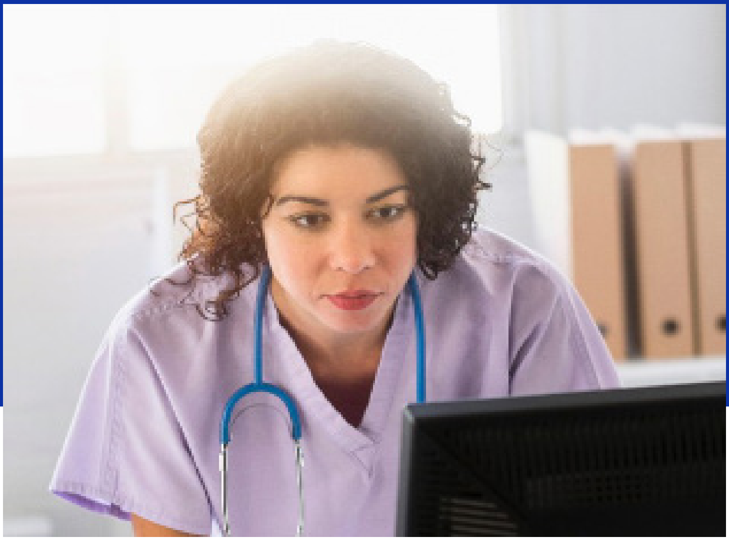
All wired and wireless 802.1x enterprise communications can be secured using WPA/WPA2 PSK/Enterprise with EAP-PEAP, EAP-LEAP, EAP-TLS,or EAP-FAST.

Broker Protocol Security

Like Windows and Linux desktops, ThinOS enables encryption and compression features when attaching to virtual environment brokers and servers using RDP, HDX, BLAST, DCV and PCoIP protocols. Additionally, ThinOS is FIPS 140-2 capable to ensure secure communications in sensitive environments.

Local User Security

Protect end user data and control local user access



Protect the user device

Protect the local data

Secure access to the VDI session

Tamper protection

ThinOS privilege settings provide robust desktop security by restricting user access to desktop menus, preventing unauthorized viewing or changes. IT administrators have full user interface access to ensure complete control and streamlined operations. Additionally, ThinOS is designed to connect to a virtual environment without the need to install a local browser.

Secure End user credentials

By default, ThinOS devices store SignOn credentials and application cache objects (such as session bitmaps) exclusively in RAM until the session ends. No SignOn credentials or protocol objects are written to the device's flash file system. In contrast, Windows and Linux-based devices often use disk cache to preserve credentials and application cache, making them more vulnerable to data breaches or hacking.

Advanced Authentication and Tokens

Support for token-based authentication using CAC and PIV smartcards with 90Meter and ActiveIdentity middleware, and Yubikey devices with FIDO2.

USB and Local Disk Security

All ThinOS image system files, package files, cached configurations and mirrored repository objects stored on the client's local flash file system are AES encrypted to minimize the risk of data compromise.

For units equipped with a Trusted Platform Module (TPM), a portion of the hash keys is stored within this component. Consequently, even if flash modules are removed from the devices, the data on these modules remains inaccessible. Additionally, certificates used to establish secure SSL connections, once loaded and stored on the device's flash, cannot be exported.

- **All caching is to RAM and is non-persistent**
- **AES encryption is applied to all partitions/files**
- **Reset to factory defaults restores the device to the configuration state shipped from the factory**
- **Device specific flash encryption and secure boot**

Dell ThinOS gives you precise control over USB mass storage devices. You can define which users have access and exactly how they can use these devices, ensuring both security and flexibility.

1 Flexible controls for IT support

Administrative privilege can be used to control client troubleshooting. Client logs can be exported to WMS or a local USB key.

Client device configurations are stored to a secure, non-OS flash partition. These configurations can be cleared using a reset to factory defaults.

Client certificates and image files are stored in a secure, non-OS storage partition. These certificates can be cleared using a reset to factory defaults.

2 Flexible controls for USB mass storage virtual environment access

ThinOS BIOS

USB ports can be enabled/disabled via BIOS configurations, either locally on the device or through the Wyse Management Suite console. Disabling USB ports applies to all USB device classes.

Privacy & Security

Device security allows or denies access to USB devices based on VID/PID or USB Class. It allows to selectively restrict access to any device attached to the ThinOS client device.

Peripherals

USB redirection settings can be used to force USB device driver support to come from a virtual host instead of the ThinOS client device.

Session Settings

Global and vendor specific partner policies can be used to control USB device mapping and redirection.

The most secure thin clients with Dell ThinOS[1]

Be secure from first boot

Dell-exclusive thin client operating system is secure by design to minimize risks and protect virtual desktops and Desktop-as-a-Service sessions.

Secure Management

Granular centralized control from Wyse Management Suite helps to enforce security policies, configure device compliance settings and manage BIOS.

Secure End User Credentials

Storing user credentials in RAM helps to keep them safe from malware and clears them on reboot, reducing the risk of unauthorized access.

Trusted Endpoint

Support for popular authentication methods, compliance standards and non-persistent information helps to protect session data and connect confidently from anywhere.

Closed architecture

No sensitive data or personal information is exposed on the local device. System hardening to limit attack surfaces, unpublished APIs, encrypted data and files exclusively packaged by Dell help to prevent viruses and malware.

Secure Communications

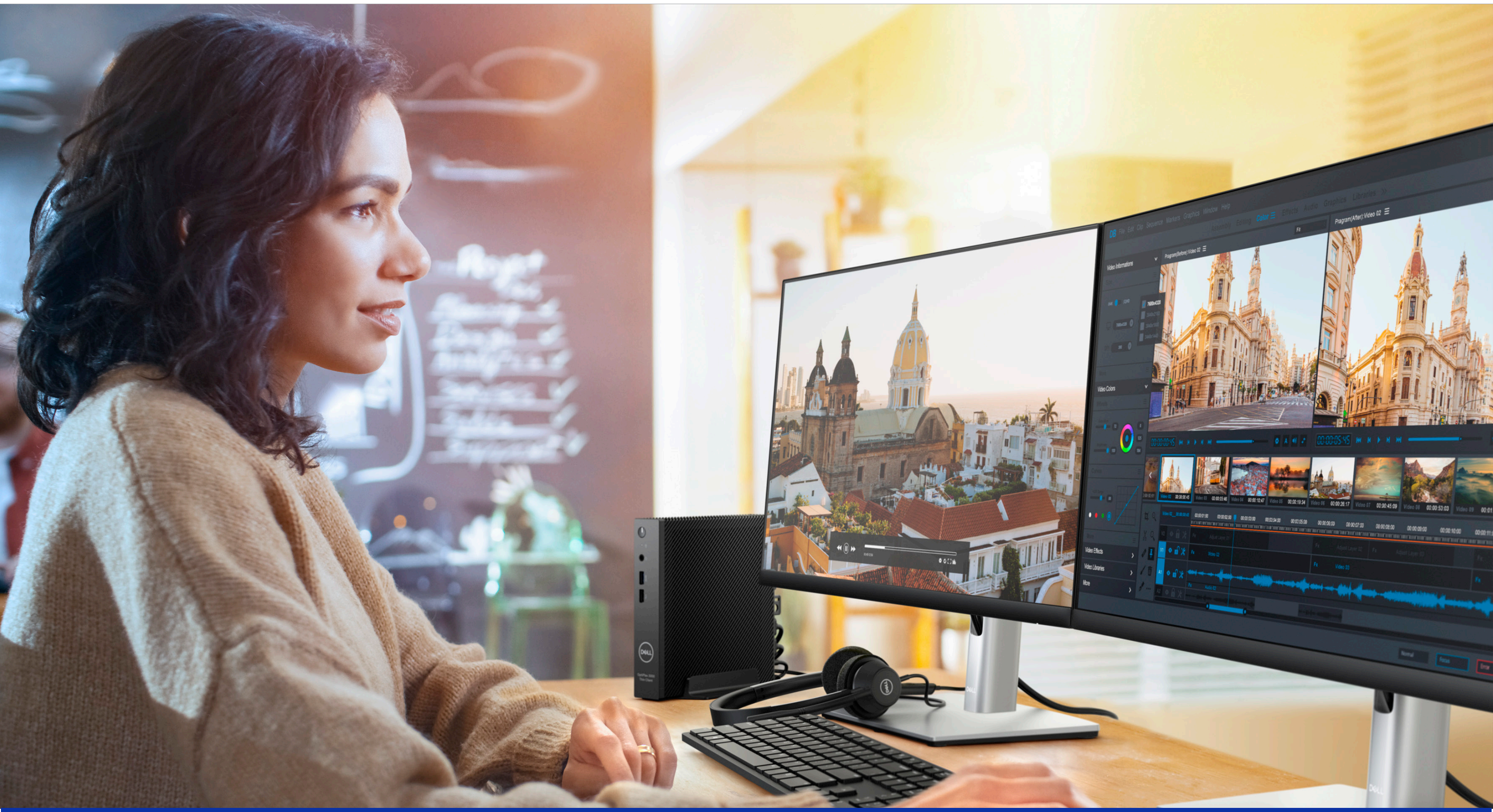
ThinOS ensures secure communications by supporting SSL connections for all broker protocol and advanced encryption methods for secure wired and wireless enterprise networks access.

Explore Dell Thin Client Solutions

[OptiPlex 3000 Thin Client - >](#)

[Dell Pro All-in-One 35 W - >](#)

[Dell Pro 14 laptop - >](#)



Work confidently from anywhere with

Dell ThinOS and Dell thin client solutions

An optimized and secure VDI endpoint with for your Virtual Desktop Infrastructure and Desktop-as-a-Service solutions.

Visit us
dell.com/CloudClientWorkspace

Read more
Simplify IT Blog -->

Join the conversation
LinkedIn / X

Sources and disclaimers

[1] Based on Dell analysis of Dell ThinOS in Appliance Mode vs. competitive products, January 2025.

[2] Dell ThinOS Appliance Mode is the default operating state of Dell ThinOS, designed to enforce a robust security posture from the start. With version 2508 and above, ThinOS introduces greater flexibility for IT administrators, allowing the installation of commercial browser options and deployment of third-party software components. To ensure compatibility with ThinOS 10, third-party applications must be compatible with Ubuntu 24.04 x86_64, include a Debian installation package and successfully pass all OS dependency checks using the App Builder tool—subject to the capabilities of the client device. Deployment requires selecting between Isolated or Native mode. Applications running in Native mode may be subject to restrictions based on their operating behavior. Thorough testing is strongly recommended to confirm successful installation and functionality before deployment. For full details on supported applications and deployment guidelines, refer to the Customer Install Guide available on Dell.com/support.