DELL Technologies

Vantaggi in termini di sicurezza di Dell ThinOS

Lavora ovunque in tutta tranquillità

grazie a soluzioni progettate per aumentare la sicurezza dei desktop virtuali e degli ambienti desktop as-a-Service.

Per soddisfare le esigenze in continua evoluzione della forza lavoro e aumentare l'efficienza senza compromettere la sicurezza con il software Cloud Client Workspace e le soluzioni thin client Dell.

Le soluzioni thin client Dell sono endpoint VDI ottimizzati, progettati appositamente per offrire accesso semplice e sicuro ai desktop virtualizzati e agli ambienti Desktop-as-a-Service con gestione IT moderna.

Riduci al minimo la superficie di attacco e goditi la tranquillità con l'esclusivo ThinOS di Dell, il nostro sistema operativo thin client più sicuro[1] appositamente progettato per gli ambienti di lavoro virtuali.

Ulteriori informazioni sul portafoglio ->

Dell ThinOS: predisposizione per Zero Trust

Rafforza le strategie Zero Trust con Dell ThinOS e Wyse Management Suite

Con l'evoluzione delle minacce informatiche, le organizzazioni stanno adottando modelli di sicurezza Zero Trust per proteggersi dalle violazioni dei dati. Dell Technologies aiuta i leader IT a rafforzare la sicurezza degli endpoint in ambienti virtuali con Dell ThinOS e Wyse Management Suite (WMS) che offrono una soluzione sicura, gestibile e basata su policy.

Nessun dispositivo è affidabile

In un modello Zero Trust, nemmeno i dispositivi ThinOS devono essere considerati automaticamente affidabili. Wyse Management Suite (WMS) consente l'onboarding sicuro inserendo nuovi client in un gruppo di policy predefinito, che richiede l'approvazione dell'amministratore prima dell'applicazione delle configurazioni. Le connessioni protette, ad esempio 802.1x o EAP-TLS con certificati gestiti tramite WMS o un server SCEP, forniscono una protezione avanzata. Ulteriori misure, tra cui la limitazione dei privilegi dell'account, l'impostazione di password BIOS univoche e l'utilizzo di un elenco di negazione della sicurezza dei dispositivi, riducono ulteriormente i rischi per la sicurezza.

Nessuna applicazione è affidabile

In modalità Appliance, Dell ThinOS garantisce, per progettazione, il supporto sicuro delle applicazioni senza accesso shell, con partizioni crittografate AES e avvio sicuro per evitare manomissioni. Solo i pacchetti di applicazioni approvati da Dell possono essere implementati tramite WMS su SSL, con convalida di hash e firma per rilevare il danneggiamento o le modifiche non autorizzate. Gli amministratori possono ridurre i rischi implementando solo i componenti software necessari e limitando l'utilizzo opzionale del browser commerciale ai flussi di lavoro essenziali, riducendo al minimo l'esposizione e rafforzando la sicurezza a livello di applicazione.

Nessun utente è affidabile

L'accesso degli utenti negli ambienti ThinOS è rigorosamente gestito per allinearsi ai principi Zero Trust. L'autenticazione del broker virtuale garantisce che gli utenti possano accedere solo a desktop o applicazioni loro assegnati. L'autenticazione a più fattori aggiunge un livello critico di protezione delle identità, mentre l'integrazione con piattaforme come Imprivata OneSign o Identity Automation rafforza il controllo delle sessioni. Queste misure combinate aiutano a bloccare l'accesso non autorizzato e supportano la conformità agli standard di sicurezza aziendali.

Sicurezza nativa

Protezione del dispositivo utente

Protezione dei dati locali

Accesso protetto alla sessione VDI

Progettazione mirata alla sicurezza

Il sistema operativo Dell ThinOS è progettato appositamente con la sicurezza come elemento centrale. Progettata come soluzione basata su appliance con architettura chiusa, contribuisce a ridurre al minimo le vulnerabilità. È possibile installare solo le applicazioni e i driver di terze parti rigorosamente testati, creati e certificati da Dell, garantendo così un ambiente controllato e sicuro per le operazioni mission-critical.

Storage sicuro

Operando in modalità Appliance, non è presente una shell di comando o la possibilità di visualizzare, modificare o eliminare file di sistema, applicazioni o configurazioni archiviati sul client. La sicurezza viene ulteriormente implementata tramite Secure Boot e la crittografia flash specifica del dispositivo AES, fornendo una solida protezione per i componenti critici.

Superfici rinforzate

Combinando imaging e storage sicuri con API non pubblicamente disponibili, Dell ThinOS crea una superficie rinforzata che protegge dai virus e malware che spesso affliggono i dispositivi Windows e Linux.

Prevenzione delle vulnerabilità comuni

Dell ThinOS è progettato pensando alla sicurezza. Per una protezione robusta contro le minacce di sicurezza più comuni, può connettersi senza problemi ad ambienti virtuali senza dover utilizzare un browser commerciale. Per i clienti con esigenze avanzate, offre la possibilità di installarne una.

Gestione sicura

Protezione del dispositivo utente

Protezione dei dati locali

Accesso protetto alla sessione VDI

Sicurezza del BIOS e del CMOS

ThinOS semplifica la protezione remota del BIOS quando si utilizza un dispositivo client Dell. In pochi clic è possibile implementare in massa gli aggiornamenti e le impostazioni del BIOS, ad esempio le password del BIOS, su più dispositivi utilizzando Wyse Management Suite Pro Edition.

Gestione automatizzata dei certificati

Grazie all'utilizzo di Wyse Management Suite, è possibile implementare con assoluta semplicità i certificati globali. Inoltre, ThinOS supporta SCEP (Simple Certificate Enrollment Protocol), semplificando la gestione dei certificati univoci dei dispositivi.

Connessioni protette

Wyse Management Suite è in grado di gestire e aggiornare in modo sicuro i dispositivi ThinOS utilizzando connessioni HTTPS protette e crittografate su reti pubbliche e private.

Immagini protette

Le immagini ThinOS sono progettate appositamente per l'installazione esclusivamente su specifici dispositivi client Dell, garantendo compatibilità e prestazioni ottimali. Per evitare manomissioni, tali immagini incorporano misure di sicurezza avanzate quando implementate tramite Wyse Management Suite o Dell OS Recovery Tool.

Le principali protezioni includono:

- Convalida del checksum per verificare l'integrità dei dati
- Convalida della firma digitale per autenticare la fonte delle immagini
- Chiavi univoche della piattaforma per garantire la compatibilità con l'hardware client e il sistema operativo preinstallato

Comunicazioni protette

Protezione del dispositivo utente

Protezione dei dati locali

Accesso protetto alla sessione VDI

Collegamenti SSL

Tutte le comunicazioni con broker e protocollo possono essere completate tramite connessioni sicure. Le policy di comunicazione ThinOS possono essere definite a livello globale o individuale per applicare il livello di sicurezza desiderato. I tre livelli "supportati" sono:

- Alto: richiesta la convalida del certificato
- Avvertenza: richiesta l'accettazione dell'utente se il controllo di validazione del certificato non riesce
- Basso: non è richiesta alcuna convalida del certificato

Sicurezza cablata e wireless

Tutte le comunicazioni aziendali cablate e wireless 802.1x possono essere protette utilizzando WPA/WPA2 PSK/ Enterprise con EAP-PEAP, EAP-LEAP, EAP-TLS o EAP-FAST.

Sicurezza del protocollo broker

Come i desktop Windows e Linux, ThinOS abilita funzionalità di crittografia e compressione quando si collega a broker e server di ambienti virtuali utilizzando protocolli RDP, HDX, BLAST, DCV e PCoIP. Inoltre, ThinOS è compatibile con FIPS 140-2 per offrire comunicazioni sicure in ambienti sensibili.

Sicurezza degli utenti locali

Proteggi i dati degli utenti finali e controlla l'accesso degli utenti locali

Protezione del dispositivo utente

Protezione dei dati locali

Accesso protetto alla sessione VDI

Protezione dalle manomissioni

Le impostazioni dei privilegi ThinOS offrono una solida protezione del desktop limitando l'accesso degli utenti ai menu del desktop, impedendo la visualizzazione o le modifiche non autorizzate. Gli amministratori IT hanno accesso completo all'interfaccia utente per il controllo completo e operazioni semplificate. Inoltre, ThinOS è progettato per connettersi a un ambiente virtuale senza la necessità di installare un browser locale.

Credenziali degli utenti finali protette

Per impostazione predefinita, i dispositivi ThinOS archiviano le credenziali SignOn e gli oggetti cache delle applicazioni (ad esempio bitmap di sessione) esclusivamente nella RAM fino al termine della sessione. Non vengono scritte credenziali SignOn o oggetti di protocollo nel file system flash del dispositivo. Al contrario, i dispositivi basati su Windows e Linux utilizzano spesso la cache del disco per conservare le credenziali e la cache delle applicazioni, rendendoli più vulnerabili a violazioni di dati o attacchi hacker.

Autenticazione avanzata e token

Supporto per l'autenticazione basata su token tramite smart card CAC e PIV con middleware 90Meter e ActiveIdentity e dispositivi Yubikey con FIDO2.

Protezione USB e disco locale

Tutti i file del sistema di immagini ThinOS, i file dei pacchetti, le configurazioni memorizzate nella cache e gli oggetti del repository con mirroring archiviati nel file system flash locale del client sono crittografati AES per ridurre al minimo il rischio di compromissione dei dati.

Per le unità dotate di Trusted Platform Module (TPM), una parte delle chiavi hash viene archiviata all'interno di questo componente. Di conseguenza, anche se i moduli flash vengono rimossi dai dispositivi, i dati su questi moduli rimangono inaccessibili. Inoltre, i certificati utilizzati per stabilire connessioni SSL protette, una volta caricati e archiviati nella memoria flash del dispositivo, non possono essere esportati.

- **Tutto il caching è nella RAM ed è non persistente**
- **La crittografia AES viene applicata a tutte le partizioni o a tutti i file**
- **Il ripristino delle impostazioni predefinite di fabbrica riporta il dispositivo allo stato di configurazione iniziale, quello di uscita dalla fabbrica**
- **Crittografia flash specifica del dispositivo e avvio protetto**

Dell ThinOS offre un controllo preciso sui dispositivi di storage di massa USB. È possibile definire quali utenti godano dell'accesso e in che modo possono utilizzare questi dispositivi, garantendo sicurezza e flessibilità.

1 Flexible controls for IT support

È possibile utilizzare il privilegio amministrativo per controllare la risoluzione dei problemi del client. I registri del client possono essere esportati in WMS o in una chiavetta USB locale.

Le configurazioni del dispositivo del cliente vengono salvate in una partizione flash protetta e non correlata al sistema operativo. Queste configurazioni possono essere cancellate utilizzando un ripristino delle impostazioni predefinite.

I certificati client e i file di immagine vengono archiviati in una partizione di storage sicura e non del sistema operativo. Tali certificati possono essere cancellati utilizzando un ripristino delle impostazioni predefinite.

2 Controlli flessibili per l'accesso all'ambiente virtuale di storage di massa USB

ThinOS BIOS

Le porte USB possono essere abilitate/disabilitate tramite le configurazioni del BIOS, localmente sul dispositivo o tramite la console Wyse Management Suite. La disabilitazione delle porte USB si applica a tutte le classi di dispositivi USB.

Privacy e sicurezza

La sicurezza del dispositivo consente o nega l'accesso ai dispositivi USB in base al VID/PID o alla classe USB. Consente di limitare selettivamente l'accesso a qualsiasi dispositivo collegato al dispositivo client ThinOS.

Periferiche

Le impostazioni di reindirizzamento USB possono essere utilizzate per forzare il supporto del driver del dispositivo USB da un host virtuale anziché dal dispositivo client ThinOS.

Impostazioni di sessione

Le politiche di partner globali e specifiche per il fornitore possono essere utilizzate per controllare la mappatura e il reindirizzamento dei dispositivi USB.

Thin client estremamente sicuri con Dell ThinOS[1]

Sicurezza fin dal primo avvio

L'esclusivo sistema operativo thin client Dell è sicuro in termini nativi per ridurre al minimo i rischi e proteggere desktop virtuali e sessioni Desktop as-a-Service.

Gestione sicura

Il controllo centralizzato granulare di Wyse Management Suite offre la possibilità di applicare policy di sicurezza, configurare le impostazioni di conformità dei dispositivi e gestire il BIOS.

Protezione delle credenziali degli utenti finali

Lo storage delle credenziali utente nella RAM aiuta a proteggerle da malware e le cancella al riavvio, riducendo il rischio di accesso non autorizzato.

Endpoint affidabile

Supporto per i metodi di autenticazione più diffusi, gli standard di conformità e le informazioni non persistenti per proteggere i dati delle sessioni e connettersi in tutta sicurezza da ovunque.

Architettura chiusa

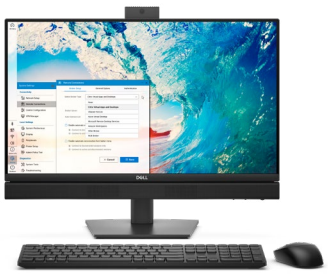
Nessun dato sensibile o informazione personale viene esposto sul dispositivo locale. Consolidamento del sistema per limitare le superfici di attacco, a un'API non pubblicata e a file e dati crittografati forniti in pacchetto da Dell per prevenire virus e malware.

Protezione DELLE COMUNICAZIONI

ThinOS offre comunicazioni sicure supportando connessioni SSL per tutti i protocolli broker e metodi di crittografia avanzati per l'accesso sicuro alle reti aziendali cablate e wireless.

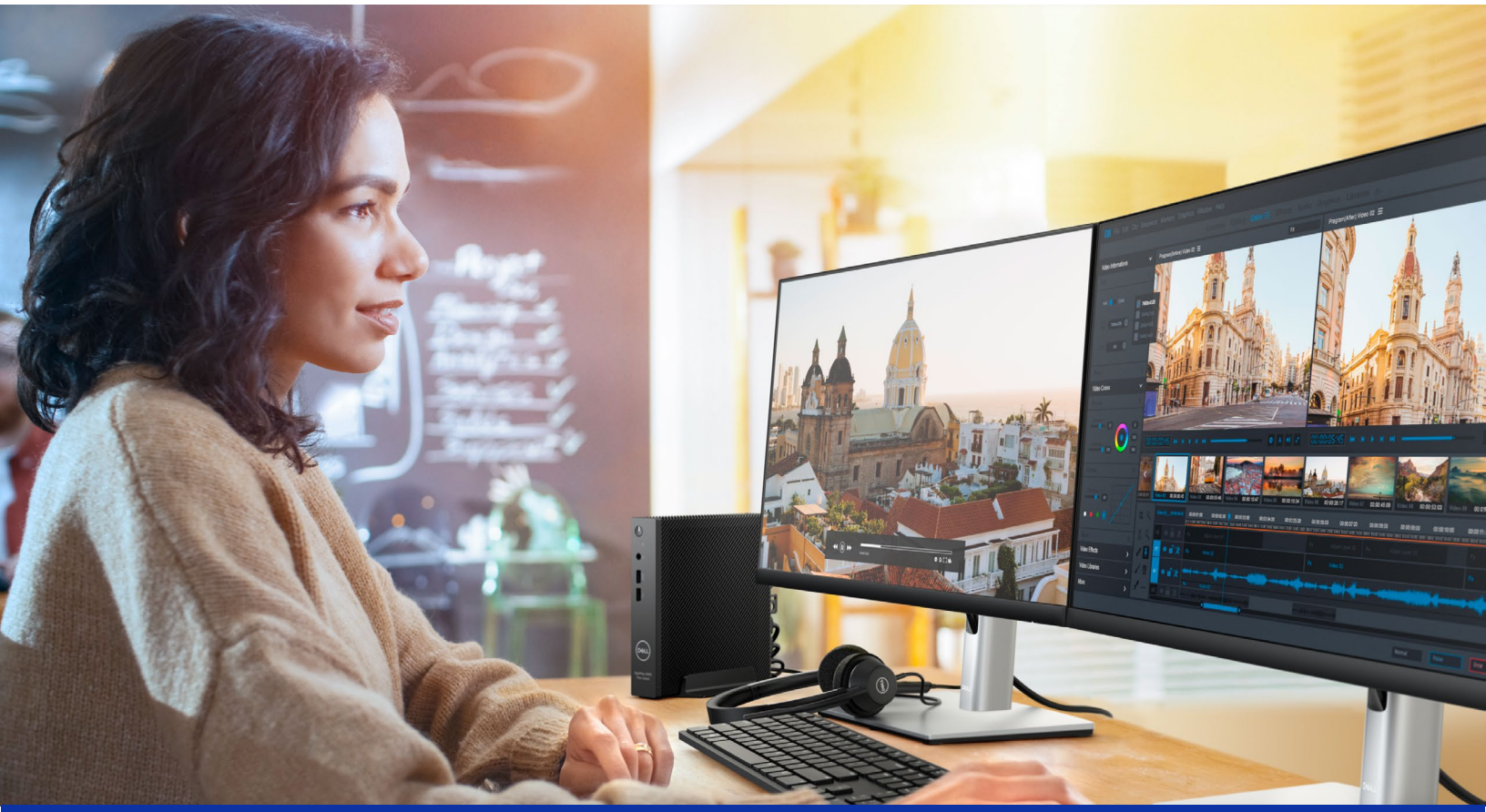
Scopri le soluzioni thin client Dell

Thin client OptiPlex 3000 - >



Dell Pro All-in-One 35 W - >

Notebook Dell Pro 14 - >



Lavora ovunque in tutta sicurezza con **le soluzioni thin client Dell ThinOS e Dell**

Endpoint VDI ottimizzato e protetto con soluzioni per Virtual Desktop Infrastructure e Desktop as-a-Service.

Visitaci
dell.com/CloudClientWorkspace

Ulteriori informazioni
Blog IT semplificata -->

Partecipa alla conversazione
LinkedIn / X

Fonti e dichiarazioni di non responsabilità

[1]Dati basati su un'analisi condotta da Dell su Dell ThinOS rispetto ai prodotti della concorrenza, gennaio 2025.

[2]Dell ThinOS in modalità Appliance è lo stato operativo predefinito di Dell ThinOS, progettato per applicare un solido profilo di sicurezza fin dall'inizio. Con la versione 2508 e più recenti, ThinOS introduce una maggiore flessibilità per gli amministratori IT, consentendo l'installazione di opzioni del browser commerciale e il deployment di componenti software di terze parti. Per garantire la compatibilità con ThinOS 10, le applicazioni di terze parti devono essere compatibili con Ubuntu 24.04 x86_64, includere un pacchetto di installazione Debian e superare correttamente tutti i controlli delle dipendenze del sistema operativo nello strumento App Builder (in base alla funzionalità del dispositivo client). Il deployment richiede la scelta tra modalità isolata o nativa. Le applicazioni in esecuzione in modalità nativa possono essere soggette a restrizioni in base al loro comportamento operativo. Si consiglia vivamente di eseguire test approfonditi per confermare la corretta installazione e la funzionalità del sistema prima del deployment. Per i dettagli completi sulle applicazioni supportate e sulle linee guida per il deployment, fai riferimento alla guida all'installazione per il cliente disponibile su Dell.com/support.