DELL Technologies

Avantages de Dell ThinOS Security

Travailler en toute confiance, où que vous soyez

avec des solutions conçues pour renforcer la sécurité de vos postes de travail virtuels et de vos environnements Desktop as-a-service.

Répondez à l'évolution des besoins des collaborateurs et augmentez leur efficacité sans compromettre la sécurité avec le logiciel Cloud Client Workspace et les solutions de clients légers Dell.

Les solutions de client léger Dell sont des points de terminaison VDI optimisés, spécialement conçus pour fournir un accès sécurisé, en toute simplicité, aux postes de travail virtualisés et aux environnements Desktop-as-a-service, tout en offrant une gestion IT moderne.

Minimisez la surface d'attaque et gardez l'esprit tranquille avec ThinOS, le système d'exploitation Dell exclusif pour client léger le plus sûr[1], spécialement conçu pour les espaces de travail virtuels.

En savoir plus sur la gamme ->

Dell ThinOS : prêt pour le Zero-Trust

Renforcez les stratégies Zero-Trust avec Dell ThinOS et Wyse Management Suite

À mesure que les cybermenaces évoluent, les entreprises adoptent des modèles de sécurité Zero-Trust pour se protéger contre les violations de données. Dell Technologies aide les responsables IT à renforcer la sécurité des points de terminaison dans les environnements virtuels grâce à Dell ThinOS et Wyse Management Suite (WMS), qui offrent une solution sécurisée, facile à gérer et basée sur des règles.

Aucun appareil n'est présumé fiable

Dans un modèle Zero-Trust, même les appareils ThinOS ne doivent pas être approuvés automatiquement. Wyse Management Suite (WMS) permet une intégration sécurisée en plaçant les nouveaux clients dans un groupe de règles par défaut, nécessitant l'approbation de l'administrateur avant d'appliquer les configurations. Les connexions sécurisées, telles que 802.1x ou EAP-TLS avec des certificats gérés via WMS ou un serveur SCEP, offrent une meilleure protection. Des mesures supplémentaires, telles que la limitation des privilèges de compte, la définition de mots de passe du BIOS uniques et l'utilisation d'une liste d'exclusion des appareils non autorisés, contribuent à réduire encore davantage les risques en matière de sécurité.

Aucune application n'est présumée fiable

En mode Appliance, Dell ThinOS garantit, dès la conception, une prise en charge sécurisée des applications sans accès au shell, des partitions avec un chiffrement AES et un démarrage sécurisé pour empêcher toute altération. Seuls les packages d'application approuvés par Dell peuvent être déployés via WMS sur SSL, avec validation par hachage et signature pour détecter toute corruption ou modification non autorisée. Les administrateurs peuvent diminuer les risques en déployant uniquement les composants logiciels nécessaires et en limitant l'utilisation facultative d'un navigateur professionnel aux workflows essentiels. Cela permet de réduire l'exposition aux risques et de renforcer la sécurité au niveau des applications.

Aucun utilisateur n'est présumé fiable

L'accès des utilisateurs dans les environnements ThinOS est géré de manière stricte afin de respecter les principes Zero-Trust. L'authentification via un courtier virtuel garantit que les utilisateurs peuvent uniquement accéder aux bureaux ou applications qui leur sont affectés. L'authentification multifacteur ajoute une couche essentielle de protection des identités, tandis que l'intégration avec des plateformes comme Imprivata OneSign ou Identity Automation renforce le contrôle des sessions. Ces mesures combinées permettent de bloquer les accès non autorisés et de garantir la conformité aux normes de sécurité de l'entreprise.

Sécurité dès la conception

Protéger l'appareil utilisateur

Protéger les données locales

Accès sécurisé à la session VDI

Conception sécurisée

La sécurité du système d'exploitation Dell ThinOS est spécialement conçue. Basée sur des appliances avec une architecture fermée, cette solution permet de minimiser les failles de sécurité. Seuls les pilotes et applications tiers rigoureusement testés, packagés et certifiés par Dell peuvent être installés, ce qui garantit un environnement contrôlé et sécurisé pour vos opérations stratégiques.

Stockage sécurisé

En mode Appliance, il n'y a pas de shell de commande ni la possibilité d'afficher, de modifier ou de supprimer à distance les fichiers de système d'exploitation, d'application ou de configuration stockés sur le client. La sécurité est renforcée par Secure Boot et le chiffrement Flash AES spécifique à l'appareil, ce qui offre une protection robuste pour les composants stratégiques.

Surfaces renforcées

En combinant des images et un stockage sécurisés avec des API non accessibles au public, Dell ThinOS crée une surface renforcée qui protège contre les virus et les logiciels malveillants qui affectent souvent les appareils Windows et Linux.

Prévention des failles de sécurité courantes

Dell ThinOS est conçu dans un souci de sécurité. Pour une protection robuste contre les menaces de sécurité courantes, le département IT peut se connecter facilement aux environnements virtuels sans avoir besoin d'un navigateur professionnel. Pour les clients ayant des besoins avancés, il offre la possibilité d'en installer un.

Gestion sécurisée

Protéger l'appareil utilisateur

Protéger les données locales

Accès sécurisé à la session VDI

Sécurité du BIOS et CMOS

ThinOS facilite la sécurisation à distance de votre BIOS lors de l'utilisation d'un appareil client Dell. En quelques clics, Wyse Management Suite Pro Edition vous permet de déployer en masse sur plusieurs appareils des mises à niveau et des paramètres du BIOS, tels que les mots de passe du BIOS.

Gestion automatisée des certificats

Les certificats globaux peuvent être facilement déployés à l'aide de Wyse Management Suite. En outre, ThinOS prend en charge le protocole SCEP (Simple Certificate Enrollment Protocol), qui simplifie la gestion des certificats d'appareils uniques.

Connexions sécurisées

Wyse Management Suite peut gérer et mettre à niveau en toute sécurité les appareils ThinOS à l'aide de connexions HTTPS sécurisées et chiffrées sur les réseaux publics et privés.

Création d'images sécurisée

Les images ThinOS sont spécialement conçues pour être installées exclusivement sur des appareils clients Dell spécifiques, ce qui garantit une compatibilité et des performances optimales. Pour éviter toute altération, ces images intègrent des mesures de sécurité avancées lorsqu'elles sont déployées via Wyse Management Suite ou Dell OS Recovery Tool.

Principales protections :

- Somme de contrôle pour vérifier l'intégrité des données
- Validation de signature numérique pour authentifier la source d'image
- Plateformes uniques pour garantir la compatibilité avec le matériel client et le système d'exploitation préinstallé

Communications sécurisées

Protéger l'appareil utilisateur

Protéger les données locales

Accès sécurisé à la session VDI

Connexions SSL

Toutes les communications entre les courtiers et les protocoles peuvent être effectuées via des connexions sécurisées. Des stratégies de communication ThinOS peuvent être définies à un niveau global ou individuel pour appliquer le niveau de sécurité souhaité. Les trois niveaux « pris en charge » sont les suivants :

- Élevé : la validation du certificat est requise
- Avertissement : acceptation de l'utilisateur requise si la vérification de validation du certificat échoue
- Faible : aucune validation de certificat requise

Sécurité filaire et sans fil

Toutes les communications d'entreprise 802.1x filaires et sans fil peuvent être sécurisées à l'aide de WPA/WPA2 PSK/Enterprise avec EAP-PEAP, EAP-LEAP, EAP-TLS ou EAP-FAST.

Sécurité du protocole de courtier

À l'instar des ordinateurs de bureau Windows et Linux, ThinOS offre des fonctionnalités de chiffrement et de compression lors de la connexion à des courtiers et des serveurs d'environnement virtuel à l'aide des protocoles RDP, HDX, BLAST, DCV et PCoIP. En outre, ThinOS est compatible avec FIPS 140-2 pour garantir des communications sécurisées dans les environnements sensibles.

Sécurité des utilisateurs locaux

Protéger les données des utilisateurs finaux et contrôler l'accès des utilisateurs locaux

Protéger l'appareil utilisateur

Protéger les données locales

Accès sécurisé à la session VDI

Protection contre l'altération

Les paramètres de privilèges ThinOS offrent une sécurité renforcée du poste de travail en limitant l'accès des utilisateurs aux menus, empêchant ainsi l'affichage ou les modifications non autorisés. Les administrateurs IT disposent d'un accès complet à l'interface utilisateur pour garantir un contrôle total et des opérations rationalisées. En outre, ThinOS est conçu pour se connecter à un environnement virtuel sans avoir besoin d'installer un navigateur local.

Tokens et authentification avancés

Prise en charge de l'authentification basée sur des tokens à l'aide de cartes à puce CAC et PIV avec les middlewares 90Meter et ActiveIdentity, et d'appareils Yubikey avec FIDO2.

Informations d'identification sécurisées des utilisateurs finaux

Par défaut, les appareils ThinOS stockent les informations d'identification SignOn et les objets de cache d'application (tels que les bitmaps de session) exclusivement dans la RAM jusqu'à la fin de la session. Aucune information d'identification SignOn ou aucun objet de protocole n'est écrit sur le système de fichiers Flash de l'appareil. En revanche, les appareils Windows et Linux utilisent souvent le cache de disque pour préserver les informations d'identification et le cache d'application, ce qui les rend plus vulnérables aux violations de données ou au piratage.

Sécurité des disques USB et locaux

Tous les fichiers système d'image ThinOS, les fichiers de package, les configurations mises en cache et les objets de référentiel mis en miroir stockés sur le système de fichiers Flash local du client sont chiffrés AES afin de minimiser le risque de compromission des données.

Pour les unités équipées d'un module TPM (Trusted Platform Module), une partie des clés de hachage est stockée dans ce composant. Par conséquent, même si les modules Flash sont retirés des appareils, les données de ces modules restent inaccessibles. En outre, les certificats utilisés pour établir des connexions SSL sécurisées, une fois chargés et stockés sur la mémoire Flash de l'appareil, ne peuvent pas être exportés.

- **Toute la mise en cache est effectuée sur la RAM et est non persistante**
- **Le chiffrement AES est appliqué à toutes les partitions/tous les fichiers**
- **La restauration des paramètres d'usine par défaut restaure l'appareil à l'état de configuration expédié en usine**
- **Chiffrement Flash spécifique à l'appareil et démarrage sécurisé**

Dell ThinOS vous offre un contrôle précis sur les périphériques de stockage de masse USB. Vous pouvez définir les utilisateurs qui ont accès et la façon exacte dont ils peuvent utiliser ces appareils, ce qui garantit à la fois la sécurité et la flexibilité.

1 Flexible controls for IT support

Des privilèges d'administration peuvent être utilisés pour contrôler le dépannage du client. Les journaux client peuvent être exportés vers WMS ou une clé USB locale.

Les configurations des appareils clients sont stockées sur une partition Flash sécurisée non basée sur le système d'exploitation. Ces configurations peuvent être effacées à l'aide d'une réinitialisation des paramètres par défaut.

Les certificats clients et les fichiers image sont stockés dans une partition de stockage sécurisée non liée au système d'exploitation. Ces certificats peuvent être effacés à l'aide d'une réinitialisation des paramètres par défaut.

2 Contrôles flexibles pour l'accès à l'environnement virtuel de stockage de masse USB

BIOS ThinOS

Les ports USB peuvent être activés/désactivés via les configurations du BIOS, localement sur l'appareil ou via la console Wyse Management Suite. La désactivation des ports USB s'applique à toutes les classes d'appareils USB.

Confidentialité et sécurité

La sécurité des appareils autorise ou refuse l'accès aux appareils USB en fonction de VID/PID ou de la classe USB. Elle permet de restreindre de manière sélective l'accès à n'importe quel périphérique connecté à l'appareil client ThinOS.

Périphériques

Les paramètres de redirection USB peuvent être utilisés pour forcer la prise en charge du pilote de périphérique USB à partir d'un hôte virtuel au lieu de l'appareil client ThinOS.

Paramètres de la session

Des politiques de partenariat globales et spécifiques au fournisseur peuvent être utilisées pour contrôler le mappage et la redirection des périphériques USB.

Les clients légers les plus sécurisés avec Dell ThinOS[1]

Protection assurée dès le premier démarrage

Le client léger exclusif Dell est conçu dès le départ pour être sécurisé et réduire les risques. Il protège les postes de travail virtuels et les sessions Desktop as-a-service.

Gestion sécurisée

Le contrôle centralisé granulaire de Wyse Management Suite permet d'appliquer les politiques de sécurité, de configurer les paramètres de conformité des appareils et de gérer le BIOS.

Informations d'Identification sécurisées des Utilisateurs Finaux

Stocker les informations d'identification des utilisateurs dans la RAM permet de les protéger contre les logiciels malveillants et de les effacer au redémarrage, ce qui réduit le risque d'accès non autorisé.

Point de terminaison de confiance

La prise en charge des méthodes d'authentification courantes, des normes de conformité et des informations non persistantes permet de protéger les données des sessions et de se connecter en toute confiance, partout.

Architecture fermée

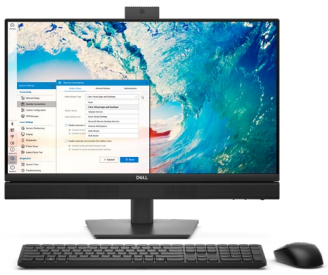
Aucune donnée sensible ni information personnelle n'est exposée sur l'appareil local. Le renforcement de la protection système pour limiter les surfaces d'attaque, les API non publiées, les données chiffrées et les fichiers exclusivement packagés par Dell permet de résister aux virus et aux logiciels malveillants.

Communications sécurisées

ThinOS garantit des communications sécurisées en prenant en charge les connexions SSL pour tous les protocoles de courtier et les méthodes avancées de chiffrage pour un accès sécurisé aux réseaux d'entreprise filaires et sans fil.

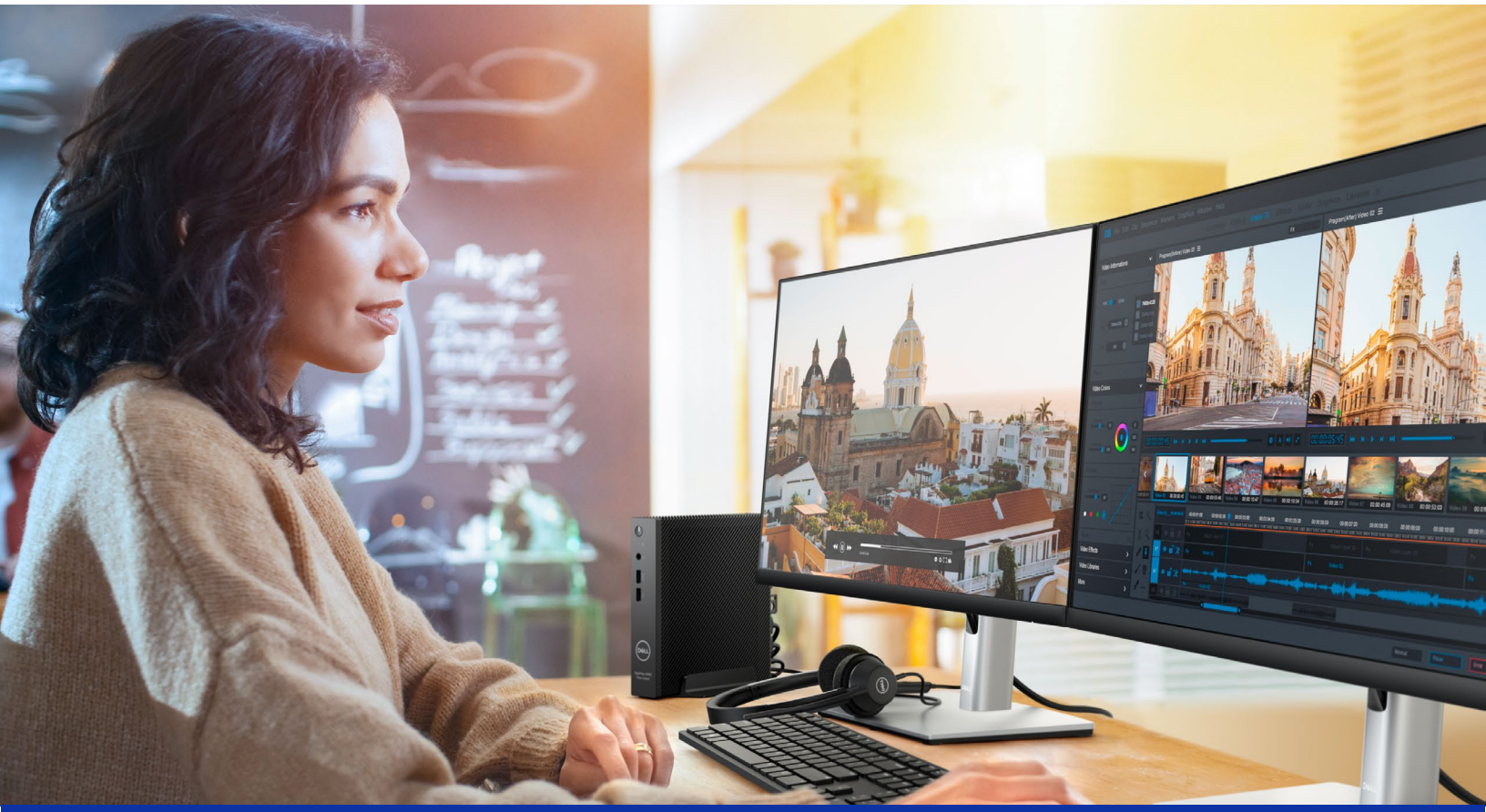
Découvrez les solutions de clients légers Dell

Client léger OptiPlex 3000 - >



Dell Pro tout-en-un 35 W - >

Ordinateur portable Dell Pro 14 - >



Travaillez en toute confiance, où que vous soyez, avec les **solutions ThinOS et de client léger Dell**

Point de terminaison VDI optimisé et sécurisé pour vos solutions d'infrastructure de bureau virtuel et de bureau as-a-service.

Venez-nous voir
dell.com/CloudClientWorkspace

En savoir plus
Blog Simplify IT -->

Rejoindre la discussion
LinkedIn/X

Sources et mentions légales

[1]D'après une analyse réalisée par Dell en janvier 2025, comparant Dell ThinOS en mode appliance et des produits concurrents.

[2] Le mode Appliance de Dell ThinOS est l'état de fonctionnement par défaut de Dell ThinOS, conçu pour appliquer une posture de sécurité robuste dès le départ. À partir de la version 2508, ThinOS offre une plus grande flexibilité aux administrateurs IT, leur permettant d'installer des options de navigateur professionnel et de déployer des composants logiciels tiers. Pour garantir la compatibilité avec ThinOS 10, les applications tierces doivent être compatibles avec Ubuntu 24.04 x86_64, inclure un package d'installation Debian et passer toutes les vérifications de dépendance du système d'exploitation dans l'outil App Builder (sous réserve de la capacité de l'appareil client). Le déploiement nécessite de choisir entre le mode Isolé ou Natif. Les applications exécutées en mode Natif peuvent être soumises à des restrictions en fonction de leur comportement de fonctionnement. Il est vivement recommandé d'effectuer des tests approfondis pour confirmer la réussite de l'installation et le bon fonctionnement avant le déploiement. Pour obtenir plus d'informations sur les applications prises en charge ainsi que des instructions de déploiement, voir le Guide d'installation client disponible sur Dell.com/support.