DELL Technologies

Benefícios de segurança do Dell ThinOS

Trabalhe com confiança em qualquer lugar

com soluções projetadas para aumentar a segurança de seus desktops virtuais e ambientes Desktop "as a service".

Com o software Cloud Client Workspace e as soluções de thin client da Dell, você atende à evolução das necessidades da força de trabalho e aumenta a eficiência sem colocar a segurança em risco.

As soluções de thin client da Dell são endpoints de VDI otimizados e criados especificamente para fornecer um acesso seguro e sem interrupções a desktops virtualizados e Desktop "as a service" com gerenciamento moderno de TI.

Minimize a superfície de ataque e tenha tranquilidade com o exclusivo ThinOS da Dell, nosso sistema operacional para thin client mais seguro[1] desenvolvido especificamente para espaços de trabalho virtuais.

Saiba mais sobre o portfólio ->

Dell ThinOS: Pronto para o Zero Trust

Fortaleça as estratégias Zero Trust com o Dell ThinOS e o Wyse Management Suite

À medida que as ameaças cibernéticas evoluem, as organizações estão adotando modelos de segurança Zero Trust para a proteção contra violações de dados. A Dell Technologies ajuda os líderes de TI a fortalecer a segurança de endpoints em ambientes virtuais com o Dell ThinOS e o Wyse Management Suite (WMS), oferecendo uma solução segura, gerenciável e orientada por políticas.

Não confie em nenhum dispositivo

Em um modelo Zero Trust, mesmo os dispositivos ThinOS não devem ser automaticamente confiáveis. O Wyse Management Suite (WMS) permite a integração segura, colocando novos clientes em um grupo de políticas padrão, exigindo a aprovação do administrador antes de aplicar as configurações. Conexões seguras, como 802.1x ou EAP-TLS com certificados gerenciados por WMS ou um servidor SCEP, oferecem proteção aprimorada. Medidas adicionais, incluindo limitação de privilégios de conta, definição de senhas exclusivas do BIOS e uso de uma Device Security Deny List, reduzem ainda mais os riscos de segurança.

Não confie em aplicativos

No modo Appliance, o Dell ThinOS garante, por padrão, suporte seguro a aplicativos sem acesso ao shell, partições criptografadas com AES e inicialização segura para evitar adulteração. Somente pacotes de aplicativos aprovados pela Dell podem ser implementados via WMS por SSL, com validação de hash e assinatura para detectar corrupção ou alterações não autorizadas. Os administradores podem reduzir os riscos implementando apenas os componentes de software necessários e limitando o uso opcional de navegadores comerciais a fluxos de trabalho essenciais, minimizando a exposição e fortalecendo a segurança no nível do aplicativo.

Não confie em usuários

O acesso do usuário em ambientes ThinOS é estritamente gerenciado para se alinhar aos princípios de Zero Trust. A autenticação do agente virtual garante que os usuários possam acessar apenas os desktops ou aplicativos atribuídos a eles. A autenticação multifator adiciona uma camada crítica de proteção de identidade, enquanto a integração com plataformas como Imprivata OneSign ou Identity Automation fortalece o controle de sessão. Essas medidas combinadas ajudam a bloquear o acesso não autorizado e a manter a conformidade com os padrões de segurança da empresa.

Seguro por natureza

Proteja o dispositivo do usuário

Proteja os dados locais

Acesso seguro à sessão de VDI

Projeto seguro

O sistema operacional Dell ThinOS foi desenvolvido especificamente com a segurança em sua essência. Projetado como uma solução baseada em dispositivo com uma arquitetura fechada, ele ajuda a minimizar as vulnerabilidades. Somente aplicativos e drivers de terceiros que tenham sido rigorosamente testados, compactados e certificados pela Dell podem ser instalados, garantindo um ambiente controlado e seguro para suas operações essenciais.

Armazenamento seguro

Durante a operação no modo Appliance, não há shell de comando nem a capacidade de exibir, alterar ou excluir remotamente o sistema operacional, o aplicativo ou os arquivos de configuração armazenados no client. A segurança é ainda mais reforçada por meio da criptografia flash específica de dispositivo AES e da inicialização segura, fornecendo proteção robusta para componentes essenciais.

Superfícies reforçadas

Ao combinar a geração de imagens e o armazenamento seguros com APIs não disponíveis ao público, o Dell ThinOS cria uma superfície reforçada que protege contra vírus e malware que geralmente prejudicam dispositivos Windows e Linux.

Evite vulnerabilidades comuns

O Dell ThinOS foi projetado tendo em mente a segurança. Para uma proteção robusta contra ameaças comuns à segurança, ele pode se conectar facilmente a ambientes virtuais sem a necessidade de um navegador comercial. Para clientes com necessidades avançadas, ele oferece a opção de instalar um.

Gerenciamento seguro

Proteja o dispositivo do usuário

Proteja os dados locais

Acesso seguro à sessão de VDI

Segurança do BIOS e do CMOS

O ThinOS facilita a proteção remota do BIOS ao usar um dispositivo client da Dell. Com apenas alguns cliques, é possível implementar upgrades e configurações do BIOS em massa, como senhas do BIOS, em vários dispositivos usando o Wyse Management Suite Pro Edition.

Gerenciamento automatizado de certificados

Certificados globais podem ser facilmente implementados usando o Wyse Management Suite. Além disso, o ThinOS é compatível com o Simple Certificate Enrollment Protocol (SCEP), simplificando o gerenciamento de certificados exclusivos de dispositivo.

Conexões seguras

O Wyse Management Suite pode gerenciar e fazer upgrade de dispositivos ThinOS com segurança utilizando conexões HTTPS criptografadas e seguras em redes públicas e privadas.

Geração de imagens segura

As imagens do ThinOS são desenvolvidas especificamente para instalação exclusiva em dispositivos client da Dell especificados, garantindo a compatibilidade e o desempenho ideais. Para a proteção contra adulteração, essas imagens incorporam medidas de segurança avançadas quando implementadas por meio do Wyse Management Suite ou do Dell OS Recovery Tool.

As principais proteções incluem:

- Validação de checksum para verificar a integridade dos dados
- Validação de assinatura digital para autenticar a fonte da imagem
- Chaves de plataforma exclusivas para garantir a compatibilidade com o hardware do client e o sistema operacional pré-instalado

Comunicações seguras

Proteja o dispositivo do usuário

Proteja os dados locais

Acesso seguro à sessão de VDI

Conexões SSL

Todas as comunicações de agente e protocolo podem ser concluídas por meio de conexões seguras. As políticas de comunicação do ThinOS podem ser definidas em um nível global ou individual para aplicar o nível de segurança desejado. Os três níveis "compatíveis" são:

- Alto: validação de certificados obrigatória
- Aviso: aceitação do usuário necessária se a verificação da validação de certificados falhar
- Baixo: nenhuma validação de certificados exigida

Segurança com e sem fio

Todas as comunicações corporativas com fio e sem fio 802.1x podem ser protegidas utilizando WPA/WPA2 PSK/ Enterprise com EAP-PEAP, EAP-LEAP, EAP-TLS ou EAP-FAST.

Segurança do protocolo de agente

Como os desktops Windows e Linux, o ThinOS permite recursos de criptografia e compactação ao se conectar a agentes e servidores de ambiente virtual utilizando protocolos RDP, HDX, BLAST, DCV e PCoIP. Além disso, o ThinOS é compatível com FIPS 140-2 para garantir comunicações seguras em ambientes sensíveis.

Segurança do usuário local

Proteja os dados do usuário final
e controle o acesso do usuário local

Proteja o dispositivo do usuário

Proteja os dados locais

Acesso seguro à sessão de VDI

Proteção contra violações

As configurações de privilégio do ThinOS fornecem segurança robusta de desktop, restringindo o acesso do usuário aos menus de desktop, impedindo a visualização ou alterações não autorizadas. Os administradores de TI têm acesso completo à interface do usuário para garantir controle completo e operações otimizadas. Além disso, o ThinOS foi projetado para se conectar a um ambiente virtual sem a necessidade de instalar um navegador local.

Credenciais seguras dos usuários finais

Por padrão, os dispositivos ThinOS armazenam credenciais de log-on e objetos de cache de aplicativos (como bitmaps de sessão) exclusivamente na RAM até que a sessão termine. Nenhum objeto de protocolo ou credencial de log-on é gravado no file system flash do dispositivo. Por outro lado, os dispositivos baseados em Windows e Linux geralmente usam cache de disco para preservar credenciais e cache de aplicativos, tornando-os mais vulneráveis a violações de dados ou invasões.

Autenticação avançada e tokens

Suporte para autenticação baseada em token utilizando smart cards CAC e PIV com middleware 90Meter e ActiveIdentity e dispositivos Yubikey com FIDO2.

Segurança de disco local e USB

Todos os file systems de imagem do ThinOS, arquivos do pacote, configurações armazenadas em cache e objetos em repositório espelhados armazenados no file system flash local do cliente são criptografados com AES para minimizar o risco de comprometimento de dados.

Para unidades equipadas com um Trusted Platform Module (TPM), uma parte das chaves hash é armazenada nesse componente. Consequentemente, mesmo se os módulos flash forem removidos dos dispositivos, os dados nesses módulos permanecerão inacessíveis. Além disso, os certificados usados para estabelecer conexões SSL seguras, uma vez carregados e armazenados no flash do dispositivo, não podem ser exportados.

- **Todo o armazenamento em cache fica na RAM e não é persistente**
- **A criptografia AES é aplicada a todas as partições/arquivos**
- **Redefinir para os padrões de fábrica restaura o dispositivo para o estado de configuração enviado da fábrica**
- **Criptografia flash específica do dispositivo e inicialização segura**

O Dell ThinOS oferece controle preciso sobre dispositivos USB de armazenamento em massa. É possível definir quais usuários têm acesso e exatamente como eles podem utilizar esses dispositivos, garantindo segurança e flexibilidade.

1 Flexible controls for IT support

O privilégio administrativo pode ser usado para controlar a solução de problemas de client. Os logs de client podem ser exportados para o WMS ou para uma chave USB local.

As configurações do dispositivo client são armazenadas em uma partição flash segura e sem sistema operacional. Essas configurações podem ser apagadas usando uma redefinição para os padrões de fábrica.

Os certificados de client e os arquivos de imagem são armazenados em uma partição de armazenamento segura e sem sistema operacional. Esses certificados podem ser apagados usando uma redefinição para os padrões de fábrica.

2 Controles flexíveis para acesso ao ambiente virtual de armazenamento USB em massa

BIOS do ThinOS

As portas USB podem ser ativadas/desativadas por meio das configurações do BIOS, localmente no dispositivo ou pelo console do Wyse Management Suite. A desativação das portas USB aplica-se a todas as classes de dispositivos USB.

Privacidade e segurança

A segurança do dispositivo permite ou proíbe o acesso a dispositivos USB com base em VID/PID ou classe USB. Permite restringir seletivamente o acesso a qualquer dispositivo conectado ao dispositivo client ThinOS.

Periféricos

As configurações de redirecionamento de USB podem ser usadas para forçar o suporte do driver de dispositivo USB a vir de um host virtual em vez do dispositivo client ThinOS.

Configurações de sessão

Políticas de parceiros globais e específicas de fornecedores podem ser usadas para controlar o mapeamento e o redirecionamento de dispositivos USB.

Os thin clients mais seguros com o Dell ThinOS[1]

Tenha segurança desde a primeira inicialização

O sistema operacional thin client exclusivo da Dell é seguro e projetado para minimizar os riscos e proteger desktops virtuais e sessões de Desktop "as a service".

Gerenciamento SEGURO

O controle centralizado granular do Wyse Management Suite ajuda a impor políticas de segurança, definir configurações de conformidade do dispositivo e gerenciar o BIOS.

Credenciais SEGURAS dos USUÁRIOS FINAIS

O armazenamento de credenciais do usuário na RAM ajuda a mantê-las protegidas contra malware e remove-as na reinicialização, reduzindo o risco de acesso não autorizado.

Endpoint confiável

O suporte para métodos populares de autenticação, padrões de conformidade e informações não persistentes ajudam a proteger os dados da sessão e se conectar com confiança em qualquer lugar.

Arquitetura fechada

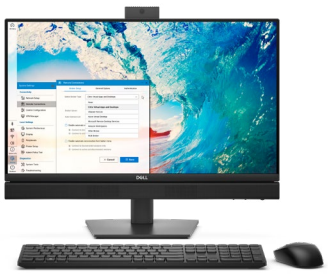
Não há exposição de dados confidenciais nem de informações pessoais no dispositivo local. O fortalecimento do sistema para limitar superfícies de ataque, APIs não publicadas, dados e arquivos criptografados e exclusivamente compactados pela Dell ajudam a prevenir vírus e malware.

Comunicações SEGURAS

O ThinOS garante comunicações seguras ao oferecer suporte a conexões SSL para todos os protocolos de agente e métodos avançados de criptografia para acesso seguro a redes corporativas com e sem fio.

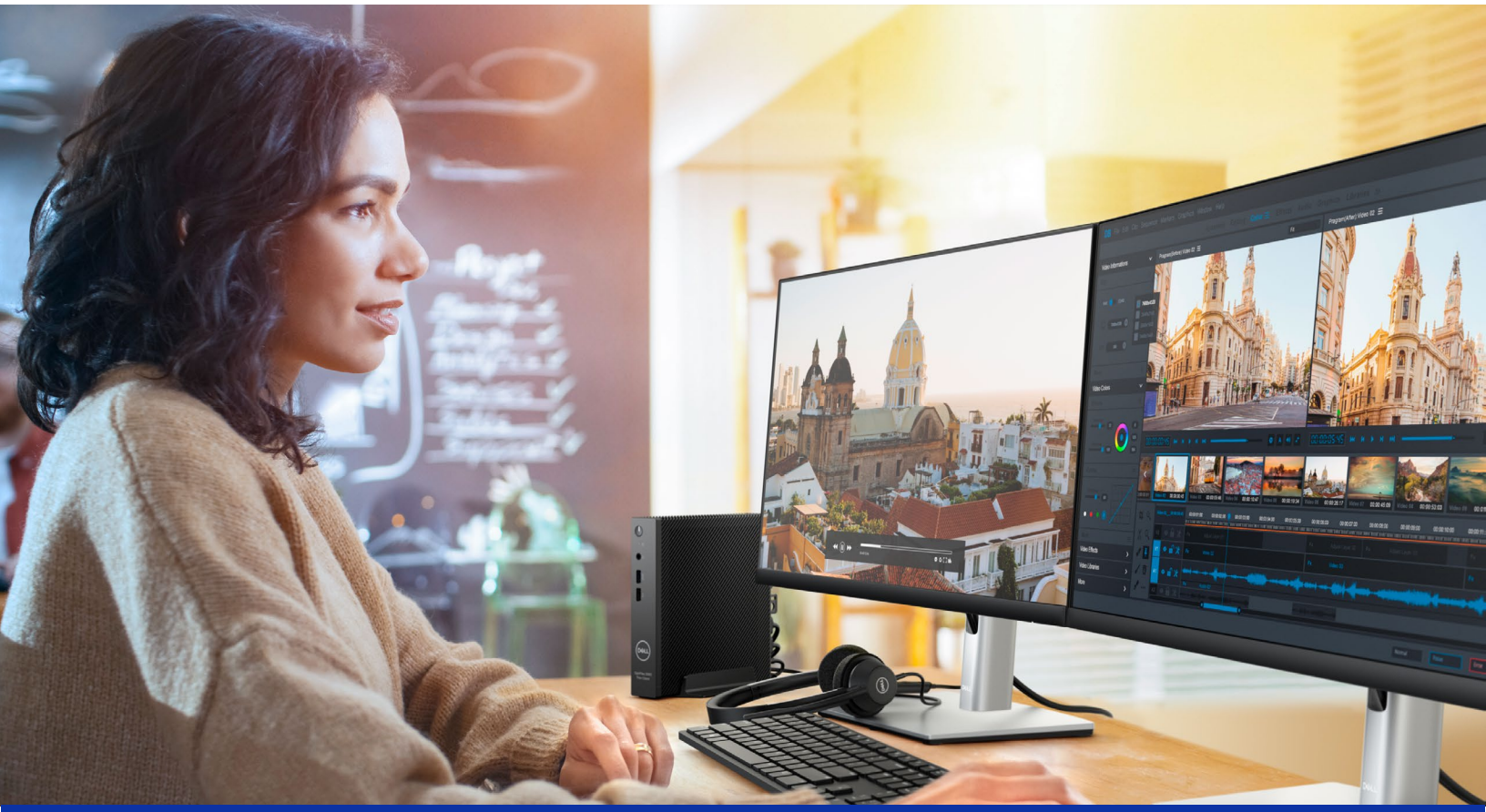
Explore as soluções de thin client da Dell

Thin Client OptiPlex 3000 - >



Dell Pro all in one de 35 W - >

Notebook Dell Pro 14 - >



Mais confiança para trabalhar em qualquer lugar com as **soluções de thin client da Dell e o Dell ThinOS**

Um endpoint VDI otimizado e seguro para suas soluções de infraestrutura de desktop virtual e de Desktop "as a service".

Visite-nos
dell.com/CloudClientWorkspace

Leia mais
Blog Simplifique a TI -->

Participe da conversa
LinkedIn/X

Fontes e isenções de responsabilidade

[1]Com base em uma análise da Dell sobre o Dell ThinOS no modo Appliance em comparação com produtos da concorrência, de janeiro de 2025.

[2]O modo Appliance do Dell ThinOS é o estado operacional padrão do Dell ThinOS, projetado para impor uma postura de segurança robusta desde o início. Com a versão 2508 e posteriores, o ThinOS oferece maior flexibilidade para administradores de TI, permitindo a instalação de opções de navegadores comerciais e a implementação de componentes de software de terceiros. Para garantir a compatibilidade com o ThinOS 10, os aplicativos de terceiros devem ser compatíveis com o Ubuntu 24.04 x86_64, incluir um pacote de instalação Debian e passar com sucesso em todas as verificações de dependência do SO na ferramenta App Builder, conforme a capacidade do dispositivo client. A implementação requer a escolha entre o modo isolado ou nativo. Os aplicativos em execução no modo Nativo podem estar sujeitos a restrições com base em seu comportamento operacional. É altamente recomendável realizar testes completos para confirmar a instalação e a funcionalidade bem-sucedidas antes da implementação. Para obter detalhes completos sobre os aplicativos compatíveis e diretrizes de implementação, consulte o Guia de instalação pelo cliente disponível em Dell.com/support.