DELL Technologies

Dell ThinOS 보안 이점

어디서나 안심하고 작업 가능

가상 데스크탑과 Desktop as-a-Service 환경의 보안을 강화하도록 설계된 솔루션입니다.

Cloud Client Workspace 소프트웨어와 Dell 씬 클라이언트 솔루션으로 보안을 유지하면서 인력의 변화하는 요구를 충족하고 효율성을 높여 보십시오.

Dell 씬 클라이언트 솔루션은 현대적인 IT 관리를 통해 가상화된 데스크탑과 DaaS(Desktop-as-a-Service) 환경에 안전하고 원활하게 액세스할 수 있도록 특별히 설계되어 있는 최적화된 VDI 엔드포인트입니다.

Dell에서 보안이 가장 뛰어난 씬 클라이언트 운영 체제[1]이며 가상 작업 공간을 위해 특별히 설계된 Dell 독점 ThinOS로 공격 표면을 최소화하여 안심하고 작업하십시오.

포트폴리오에 대한 자세한 정보 ->

Dell ThinOS: 제로 트러스트(Zero Trust) 지원

Dell ThinOS 및 Wyse Management Suite를 통해 제로 트러스트 전략 강화

사이버 위협이 진화함에 따라 조직은 데이터 침해로부터 보호하기 위해 제로 트러스트 보안 모델을 채택하고 있습니다. Dell Technologies는 안전하고 관리가 용이한 정책 기반 솔루션을 제공하는 Dell ThinOS 및 WMS(Wyse Management Suite)를 통해 IT 리더가 가상 환경에서 엔드포인트 보안을 강화할 수 있도록 지원합니다.

어떠한 디바이스도 신뢰하지 않음

제로 트러스트 모델에서는 ThinOS 디바이스라 해도 자동으로 신뢰해서는 안 됩니다. WMS(Wyse Management Suite)는 새 클라이언트를 기본 정책 그룹에 배치하여 구성을 적용하기 전에 관리자 승인을 받도록 함으로써 안전한 온보딩을 지원합니다. WMS 또는 SCEP 서버를 통해 관리되는 인증서를 사용하는 802.1x 또는 EAP-TLS와 같은 보안 연결은 보호를 강화합니다. 계정 권한 제한, 고유한 BIOS 비밀번호 설정, 디바이스 보안 거부 목록 사용 등의 추가 조치는 보안 위험을 더욱 낮춥니다.

어떠한 애플리케이션도 신뢰하지 않음

어플라이언스 모드에서 Dell ThinOS는 변조를 방지하기 위해 셸 액세스 없는 보안 애플리케이션 지원, AES 암호화 파티션 및 보안 부팅을 보장하도록 되어 있습니다. Dell Technologies에서 승인한 애플리케이션 패키지만 WMS over SSL을 통해 배포할 수 있으며, 손상이나 무단 변경을 탐지하기 위한 해시 및 서명 검증을 거치게 됩니다. 관리자는 필요한 소프트웨어 구성 요소만 배포하고 선택 사항인 브라우저는 필수 워크플로에만 사용하도록 제한함으로써 노출을 최소화하고 애플리케이션 수준 보안을 강화하여 위험을 낮출 수 있습니다.

어떠한 사용자도 신뢰하지 않음

ThinOS 환경의 사용자 액세스는 제로 트러스트 원칙에 부합하도록 엄격하게 관리됩니다. 가상 브로커 인증은 사용자가 본인에게 할당된 데스크탑 또는 애플리케이션에만 액세스할 수 있도록 합니다. 다단계 인증은 중요한 ID 보호 계층을 추가하고, Imprivata OneSign 또는 Identity Automation과 같은 플랫폼과의 통합은 세션 제어를 강화합니다. 이러한 조치가 결합되면 무단 액세스를 차단하고 엔터프라이즈 보안 표준을 준수하는 데 도움이 됩니다.

보안을 고려한 설계

사용자 디바이스 보호

로컬 데이터 보호

VDI 세션에 대한 보안 액세스

보안 설계

Dell ThinOS 운영 체제는 보안을 핵심에 두고 특별히 설계되었습니다. 폐쇄형 아키텍처를 갖춘 어플라이언스 기반 솔루션으로 설계되어 취약성을 최소화하는 데 도움이 됩니다. Dell Technologies에서 엄격하게 테스트하고 패키징하고 인증한 타사 애플리케이션과 드라이버만 설치할 수 있으므로 미션 크리티컬 운영을 위한 제어되고 안전한 환경이 보장됩니다.

안전한 스토리지

어플라이언스 모드에서 작동하는 동안에는 클라이언트에 저장된 운영 체제, 애플리케이션 또는 구성 파일을 원격으로 보거나 변경하거나 삭제할 수 있는 명령 셸이나 기능이 없습니다. 보안 부팅 및 AES 디바이스별 플래시 암호화를 통해 보안이 더욱 강화되어 주요 구성 요소를 강력히 보호합니다.

강화된 표면

Dell ThinOS는 보안 이미징 및 스토리지를 비공개로 제공되는 API와 결합하여 Windows 및 Linux 디바이스에서 종종 문제를 일으키는 바이러스와 멀웨어로부터 보호하는 강화된 표면을 제공합니다.

일반 취약점 방지

Dell ThinOS는 안전을 염두에 두고 설계되었습니다. 일반적인 보안 위협에 대한 강력한 보호를 위해 커머셜 브라우저 없이도 가상 환경에 원활하게 연결할 수 있습니다. 고급 요구 사항이 있는 고객들에게는 설치 옵션을 제공합니다.

보안 관리

사용자 디바이스 보호

로컬 데이터 보호

VDI 세션에 대한 보안 액세스

BIOS 및 CMOS 보안

ThinOS를 사용하면 Dell 클라이언트 디바이스를 사용할 때 BIOS를 원격으로 쉽게 보호할 수 있습니다. Wyse Management Suite Pro Edition을 사용하면 몇 번의 클릭만으로 BIOS 비밀번호와 같은 BIOS 업그레이드 및 설정을 여러 디바이스에 대량 배포할 수 있습니다.

자동화된 인증서 관리

Wyse Management Suite를 사용하여 글로벌 인증서를 쉽게 배포할 수 있습니다. 또한 ThinOS는 SCEP(Simple Certificate Enrollment Protocol)를 지원함으로써 고유한 디바이스 인증서의 관리를 간소화합니다.

보안 연결

Wyse Management Suite는 퍼블릭 네트워크와 프라이빗 네트워크 모두에서 암호화된 보안 HTTPS 연결을 사용하여 ThinOS 디바이스를 안전하게 관리하고 업그레이드할 수 있습니다.

보안 이미징

ThinOS 이미지는 지정된 Dell 클라이언트 디바이스에만 설치하도록 특별히 제작되어 최적의 호환성과 성능을 보장합니다. 변조를 방지하기 위해 이러한 이미지는 Wyse Management Suite 또는 Dell OS Recovery Tool을 통해 배포될 때 고급 보안 조치를 통합합니다.

주요 보호 기능은 다음과 같습니다.

- 데이터 무결성을 확인하기 위한 체크섬 검증
- 이미지 소스를 인증하기 위한 디지털 서명 검증
- 클라이언트 하드웨어 및 사전 설치된 운영 체제와의 호환성을 보장하기 위한 고유한 플랫폼 키

보안 통신

사용자 디바이스 보호

로컬 데이터 보호

VDI 세션에 대한 보안 액세스

SSL 연결

모든 브로커 및 프로토콜 통신은 보안 연결을 통해 완료할 수 있습니다. 원하는 보안 수준을 적용하기 위해 ThinOS 통신 정책은 글로벌 또는 개별 수준에서 정의될 수 있습니다. 세 가지 "지원" 수준은 다음과 같습니다.

- 높음 - 인증서 검증 필요
- 경고 - 인증서 검증에 실패한 경우 사용자 수락 필요
- 낮음 - 인증서 검증이 필요하지 않음

유선 및 무선 보안

모든 유선 및 무선 802.1x 엔터프라이즈 통신은 EAP-PEAP, EAP-LEAP, EAP-TLS 또는 EAP-FAST를 포함하는 WPA/WPA2 PSK/Enterprise를 사용하여 보호할 수 있습니다.

브로커 프로토콜 보안

Windows 및 Linux 데스크탑과 마찬가지로 ThinOS는 RDP, HDX, BLAST, DCV 및 PCoIP 프로토콜을 사용하여 가상 환경 브로커 및 서버에 연결할 때 암호화 및 압축 기능을 활성화합니다. 또한 ThinOS는 FIPS 140-2를 지원하므로 보안에 민감한 환경에서 안전한 통신을 보장합니다.

로컬 사용자 보안

최종 사용자 데이터 보호 및 로컬 사용자 액세스 제어

사용자 디바이스 보호

로컬 데이터 보호

VDI 세션에 대한 보안 액세스

변조 방지

ThinOS 권한 설정은 데스크탑 메뉴에 대한 사용자 액세스를 제한하여 강력한 데스크탑 보안을 제공함으로써 무단 보기 또는 변경을 방지합니다. IT 관리자는 완전한 사용자 인터페이스 액세스 권한을 통해 완벽한 제어와 간소화된 운영을 보장할 수 있습니다. 또한 ThinOS는 로컬 브라우저를 설치할 필요 없이 가상 환경에 연결하도록 설계되었습니다.

최종 사용자 자격 증명 보안

기본적으로 ThinOS 디바이스는 세션이 종료될 때까지 SignOn 자격 증명 및 애플리케이션 캐시 오브젝트(예: 세션 비트맵)를 RAM에 단독으로 저장합니다. 어떠한 SignOn 자격 증명 또는 프로토콜 오브젝트도 디바이스의 플래시 파일 시스템에 기록되지 않습니다. 반면 Windows 및 Linux 기반 디바이스는 디스크 캐시를 사용하여 자격 증명과 애플리케이션 캐시를 보존하는 경우가 많기 때문에 데이터 침해나 해킹에 더 취약합니다.

고급 인증 및 토큰

90Meter 및 ActiveIdentity 미들웨어를 사용하는 CAC 및 PIV 스마트 카드와 FIDO2를 사용하는 Yubikey 디바이스를 통해 토큰 기반 인증을 지원합니다.

USB 및 로컬 디스크 보안

클라이언트의 로컬 플래시 파일 시스템에 저장된 모든 ThinOS 이미지 시스템 파일, 패키지 파일, 캐싱된 구성 및 미러링된 리포지토리 오브젝트는 데이터 손상 위험을 최소화하기 위해 AES로 암호화되어 있습니다.

TPM(Trusted Platform Module)이 탑재된 장치의 경우 해시 키의 일부가 이 구성 요소 내에 저장됩니다. 따라서 플래시 모듈을 디바이스에서 제거하더라도 해당 모듈의 데이터는 액세스 불가능한 상태로 유지됩니다. 또한 보안 SSL 연결을 설정하는 데 사용되는 인증서는 디바이스의 플래시에 로드되고 저장된 후에는 내보낼 수 없습니다.

- **모든 캐싱은 RAM에 저장되며 비영구적임**
- **AES 암호화는 모든 파티션/파일에 적용됨**
- **출고 시 기본값으로 재설정하면 디바이스가 출고 시 상태로 복원됨**
- **디바이스별 플래시 암호화 및 보안 부팅**

Dell ThinOS를 사용하면 USB 대용량 스토리지 디바이스를 정밀하게 제어할 수 있습니다. 액세스 권한이 있는 사용자와 해당 사용자가 이러한 디바이스를 사용하는 방법을 정확하게 정의함으로써 보안과 유연성을 모두 보장할 수 있습니다.

1 Flexible controls for IT support

관리 권한은 클라이언트 문제 해결을 제어하는 데 사용할 수 있습니다. 클라이언트 로그는 WMS 또는 로컬 USB 키로 내보낼 수 있습니다.

클라이언트 디바이스 구성은 OS가 아닌 보안 플래시 파티션에 저장됩니다. 이러한 구성은 출고 시 기본값으로 재설정하여 지울 수 있습니다.

클라이언트 인증서 및 이미지 파일은 OS가 아닌 보안 스토리지 파티션에 저장됩니다. 이러한 인증서는 출고 시 기본값으로 재설정하여 지울 수 있습니다.

2 USB 대용량 스토리지 가상 환경 액세스를 위한 유연한 제어

ThinOS BIOS

USB 포트는 BIOS 구성을 통해 활성화/비활성화할 수 있습니다. 디바이스에서 로컬로 수행하거나 Wyse Management Suite 콘솔을 통해 수행할 수 있습니다. USB 포트를 비활성화하면 모든 USB 디바이스 클래스에 적용됩니다.

개인 정보 보호 및 보안

디바이스 보안은 VID/PID 또는 USB 클래스를 기반으로 USB 디바이스에 대한 액세스를 허용하거나 거부합니다. ThinOS 클라이언트 디바이스에 연결된 모든 디바이스에 대한 액세스를 선택적으로 제한할 수 있습니다.

주변 장치

USB 리디렉션 설정을 사용하여 ThinOS 클라이언트 디바이스 대신 가상 호스트에서 USB 디바이스 드라이버 지원을 강제할 수 있습니다.

세션 설정

글로벌 및 공급업체별 파트너 정책을 사용하여 USB 디바이스 매핑 및 리디렉션을 제어할 수 있습니다.

Dell ThinOS[1]를 사용하여 최고 수준의 보안을 자랑하는 씬 클라이언트

처음 부팅하는 순간부터 보안 유지

Dell 독점 씬 클라이언트 운영 체제는 위험을 최소화하고 가상 데스크탑과 DaaS(Desktop-as-a-Service) 세션을 보호하도록 설계되었기 때문에 안전합니다.

보안 관리

Wyse Management Suite의 세분화된 중앙 집중식 제어를 통해 보안 정책을 적용하고, 디바이스 규정 준수 설정을 구성하고, BIOS를 관리할 수 있습니다.

최종 사용자 자격 증명 보안

RAM에 사용자 자격 증명을 저장하면 멀웨어로부터 안전하게 보호하고 재부팅 시 지울 수 있으므로 무단 액세스 위험이 줄어듭니다.

신뢰할 수 있는 엔드포인트

널리 사용되는 인증 방법, 규정 준수 표준 및 비영구적 정보를 지원하여 세션 데이터를 보호하고 어디서든 확실하게 연결할 수 있습니다.

폐쇄형 아키텍처

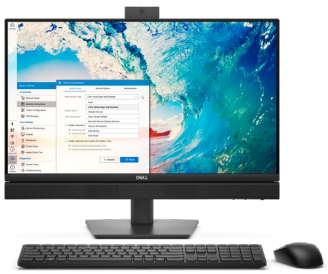
로컬 디바이스에서 기밀 데이터나 개인 정보가 노출되지 않습니다. 공격 표면을 제한하는 시스템 강화, 게시되지 않는 API, 암호화된 데이터, Dell에서 독점적으로 패키징하는 파일은 바이러스와 멀웨어를 방지하는 데 도움이 됩니다.

보안 통신

ThinOS는 모든 브로커 프로토콜에 대해 SSL 연결을 지원하고 보안 유무선 엔터프라이즈 네트워크 액세스를 위한 고급 암호화 방법을 지원함으로써 보안 통신을 보장합니다.

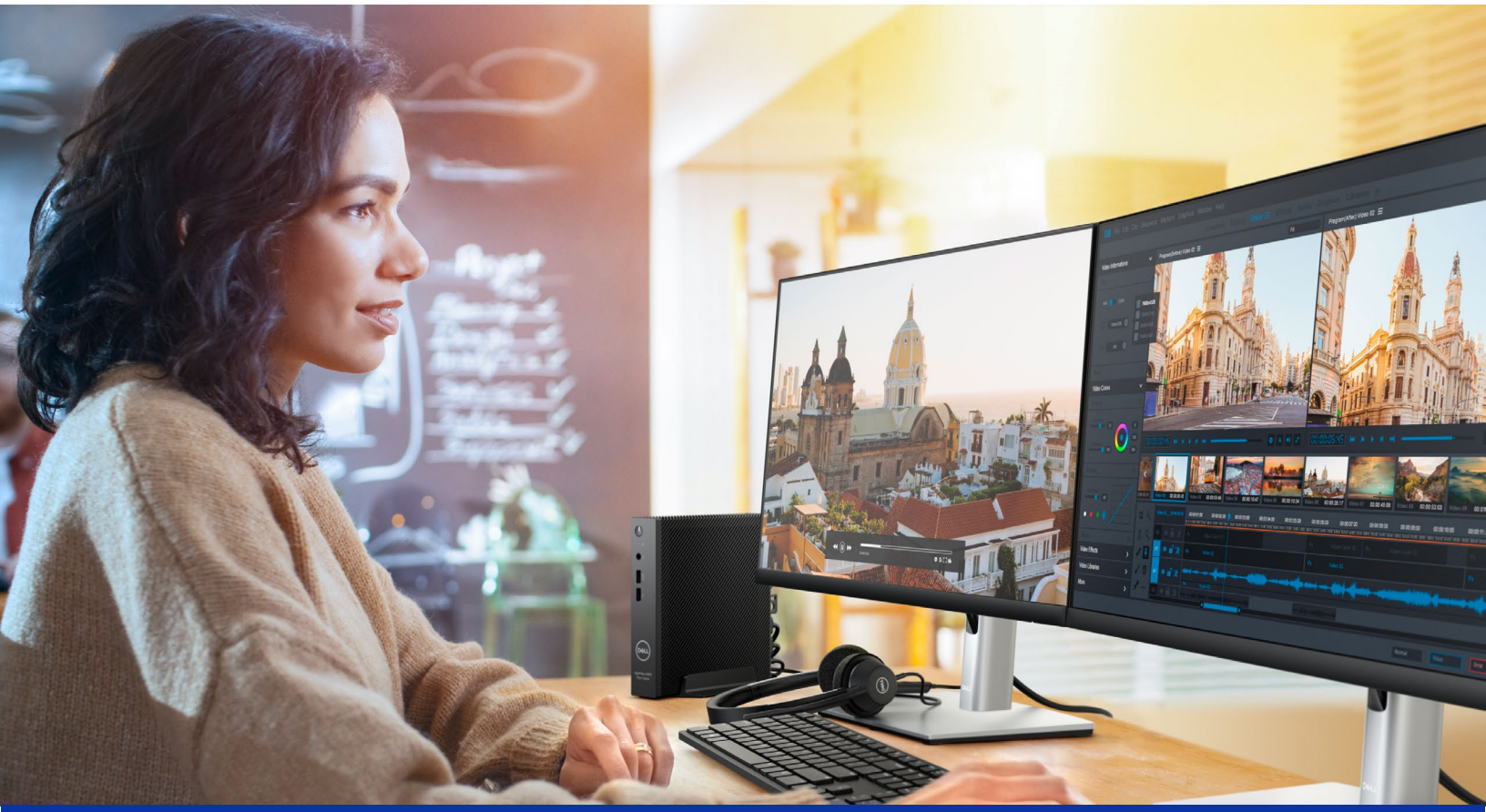
Dell 씬 클라이언트 솔루션 살펴보기

OptiPlex 3000 씬 클라이언트 - >



Dell Pro 올인원 35W - >

Dell Pro 14 노트북 - >



Dell ThinOS 및 Dell 씬 클라이언트 솔루션으로 어디서나 안심하고 작업 가능

Virtual Desktop Infrastructure 및 Desktop as-a-Service 솔루션을 위한 최적화되고 안전한 VDI 엔드포인트입니다.

웹사이트
dell.com/CloudClientWorkspace

자세한 정보
IT 환경 간소화 블로그 -->

대화에 참여
LinkedIn / X

출처 및 법적 고지 사항

[1]어플라이언스 모드의 Dell ThinOS와 경쟁 제품을 비교한 Dell 분석 기준, 2025년 1월.

[2]Dell ThinOS 어플라이언스 모드는 Dell ThinOS의 기본 작동 상태로, 처음부터 강력한 보안 태세를 적용하도록 설계되었습니다. 버전 2508 이상에서 ThinOS는 IT 관리자에게 더 큰 유연성을 제공하여 브라우저 옵션을 설치하고 타사 소프트웨어 구성 요소를 배포할 수 있도록 합니다. ThinOS 10과의 호환성을 보장하려면 타사 애플리케이션이 Ubuntu 24.04 x86_64와 호환되고, Debian 설치 패키지를 포함해야 하며, App Builder 툴에서 모든 OS 종속성 검사를 성공적으로 통과해야 합니다(클라이언트 디바이스의 기능에 따라 다름). 배포하려면 격리 모드와 네이티브 모드 중에서 선택해야 합니다. 네이티브 모드에서 실행되는 애플리케이션은 작동 동작에 따라 제한될 수 있습니다. 배포하기 전에 성공적인 설치 및 기능을 확인하기 위해 철저한 테스트를 수행하는 것이 좋습니다. 지원되는 애플리케이션 및 배포 지침에 대한 자세한 내용은 Dell.com/support에서 제공하는 고객 설치 가이드를 참조하십시오.