DELL Technologies

# Korzyści z zabezpieczeń systemu Dell ThinOS

## Wydajna praca z dowolnego miejsca

dzięki rozwiązaniom zaprojektowanym w celu zwiększenia bezpieczeństwa wirtualnych pulpitów i środowisk „pulpit jako usługa”.

Sprostaj zmieniającym się potrzebom pracowników i zwiększ wydajność bez uszczerbku dla bezpieczeństwa dzięki oprogramowaniu Cloud Client Workspace i rozwiązaniom Dell dla terminali klienckich.

Rozwiązania Dell dla terminali klienckich to zoptymalizowane punkty końcowe VDI zaprojektowane z myślą o zapewnieniu bezpiecznego i płynnego dostępu do wirtualnych pulpitów i środowisk „pulpit jako usługa” przy użyciu nowoczesnych narzędzi do zarządzania IT.

Zminimalizuj powierzchnię ataku i zachowaj spokój dzięki wyjątkowemu systemowi operacyjnemu ThinOS firmy Dell, naszemu najbezpieczniejszemu systemowi operacyjnemu dla terminali klienckich[1] stworzonemu specjalnie z myślą o wirtualnych przestrzeniach roboczych.

Dowiedz się więcej o portfolio ->

# Dell ThinOS: gotowy na model „zero trust”

## Wzmocnienie strategii modelu „zero trust” systemami Dell ThinOS i Wyse Management Suite

Wraz z rozwojem cyberzagrożeń organizacje przyjmują model „zero trust”, aby chronić się przed naruszeniami danych. Firma Dell Technologies pomaga liderom IT wzmocnić bezpieczeństwo punktów końcowych w środowiskach wirtualnych dzięki rozwiązaniom Dell ThinOS i Wyse Management Suite (WMS), które zapewniają bezpieczne, łatwe w zarządzaniu i oparte na regułach rozwiązanie.

### Brak zaufania do urządzeń

W modelu „zero trust” nawet urządzenia z systemem ThinOS nie powinny być automatycznie uznawane za godne zaufania. Pakiet Wyse Management Suite (WMS) umożliwia bezpieczne wdrażanie nowych klientów poprzez umieszczenie ich w domyślnej grupie zasad, wymagającej zatwierdzenia przez administratora przed zastosowaniem konfiguracji. Bezpieczne połączenia, takie jak 802.1x lub EAP-TLS z certyfikatami zarządzanymi za pośrednictwem WMS lub serwera SCEP, zapewniają lepszą ochronę. Dodatkowe środki, w tym ograniczenie uprawnień do konta, ustawienie unikalnych haseł BIOS i stosowanie listy blokowanych urządzeń, jeszcze bardziej zmniejszają ryzyko związane z bezpieczeństwem.

### Brak zaufania do aplikacji

W trybie urządzenia system Dell ThinOS zapewnia z założenia bezpieczne wsparcie dla aplikacji — bez dostępu do powłoki systemowej, z partycjami szyfrowanymi algorytmem AES oraz bezpiecznym rozruchem, który zapobiega manipulacjom. Tylko pakiety aplikacji zatwierdzone przez firmę Dell mogą być wdrażane za pośrednictwem WMS przez protokół SSL, z weryfikacją skrótu i podpisu w celu wykrycia uszkodzeń lub nieautoryzowanych zmian. Administratorzy mogą zmniejszyć ryzyko, wdrażając tylko niezbędne komponenty oprogramowania i ograniczając opcjonalne korzystanie z komercyjnych przeglądarek do niezbędnych procesów roboczych, minimalizując ekspozycję na ryzyko i wzmacniając bezpieczeństwo na poziomie aplikacji.

### Brak zaufania do użytkowników

Dostęp użytkowników w środowiskach ThinOS jest ściśle zarządzany zgodnie z zasadami modelu „zero trust”. Wirtualne uwierzytelnianie u brokera gwarantuje, że użytkownicy mają dostęp tylko do przypisanych im pulpitów lub aplikacji. Uwierzytelnianie wieloskładnikowe zapewnia dodatkową warstwę ochrony tożsamości, a integracja z platformami takimi jak Imprivata OneSign lub Identity Automation wzmacnia kontrolę sesji. Połączenie tych środków pomaga blokować nieautoryzowany dostęp i zapewnia zgodność z korporacyjnymi standardami bezpieczeństwa.

# Bezpieczne z założenia

**Chroń urządzenie użytkownika**

**Chroń dane lokalne**

**Bezpieczny dostęp do sesji VDI**

## Zaprojektowany z myślą o bezpieczeństwie

System operacyjny Dell ThinOS został zaprojektowany z myślą o bezpieczeństwie. Zaprojektowany jako rozwiązanie oparte na urządzeniach o zamkniętej architekturze pomaga zminimalizować luki w zabezpieczeniach. Można instalować tylko aplikacje i sterowniki innych firm, które zostały rygorystycznie przetestowane, przygotowane i certyfikowane przez firmę Dell — co zapewnia kontrolowane i bezpieczne środowisko dla operacji o znaczeniu krytycznym.

## Bezpieczne przechowywanie

Podczas pracy w trybie urządzenia nie ma powłoki poleceń ani możliwości zdalnego przeglądania, zmieniania ani usuwania plików systemu operacyjnego, aplikacji ani konfiguracji przechowywanych na kliencie. Bezpieczeństwo jest dodatkowo wzmacniane przez Bezpieczny rozruch i szyfrowanie flash AES specyficzne dla urządzenia, zapewniając solidną ochronę krytycznych komponentów.

## Wzmocniona ochrona

Łącząc bezpieczne obrazowanie i pamięć masową z niedostępnymi publicznie interfejsami API, system operacyjny Dell ThinOS zapewnia wzmocnioną ochronę przed wirusami i złośliwym oprogramowaniem, które często nękają urządzenia z systemem Windows i Linux.

## Zapobieganie typowym lukom w zabezpieczeniach

System operacyjny Dell ThinOS zaprojektowano z myślą o bezpieczeństwie. Aby zapewnić solidną ochronę przed typowymi zagrożeniami bezpieczeństwa, może bezproblemowo łączyć się ze środowiskami wirtualnymi bez konieczności korzystania z komercyjnej przeglądarki. Dla klientów z zaawansowanymi potrzebami umożliwia jej instalację.

# Bezpieczne zarządzanie


**Chroń urządzenie użytkownika**

**Chroń dane lokalne**

**Bezpieczny dostęp do sesji VDI**

## Zabezpieczenia systemu BIOS i pamięci CMOS

System ThinOS ułatwia zdalne zabezpieczanie systemu BIOS podczas korzystania z urządzenia klienckiego firmy Dell. Wystarczy kilka kliknięć, aby masowo wdrożyć aktualizacje i ustawienia systemu BIOS, takie jak hasła systemu BIOS, na wielu urządzeniach za pomocą pakietu Wyse Management Suite Pro.

## Zautomatyzowane zarządzanie certyfikatami

Certyfikaty globalne można łatwo wdrażać za pomocą pakietu Wyse Management Suite. Ponadto system operacyjny ThinOS obsługuje protokół SCEP (Simple Certificate Enrollment Protocol), co upraszcza zarządzanie unikatowymi certyfikatami urządzeń.

## Bezpieczne połączenia

Pakiet Wyse Management Suite umożliwia bezpieczne zarządzanie urządzeniami z systemem ThinOS i uaktualnianie ich przy użyciu bezpiecznych, szyfrowanych połączeń HTTPS zarówno w sieciach publicznych, jak i prywatnych.

## Bezpieczne obrazowanie

Obrazy systemu ThinOS są przeznaczone do instalacji wyłącznie na określonych urządzeniach klienckich firmy Dell, co zapewnia optymalną zgodność i wydajność. Aby uniemożliwić ingerencję, obrazy te są wyposażone w zaawansowane środki bezpieczeństwa, gdy są wdrażane za pomocą pakietu Wyse Management Suite lub narzędzia Dell OS Recovery Tool.

Kluczowe zabezpieczenia obejmują:

- Walidację sumy kontrolnej w celu sprawdzenia integralności danych
- Walidację podpisu cyfrowego w celu uwierzytelnienia źródła obrazu
- Unikalne klucze platformy zapewniające kompatybilność ze sprzętem klienta i preinstalowanym systemem operacyjnym

# Bezpieczna komunikacja

**Chroń urządzenie użytkownika**

**Chroń dane lokalne**

**Bezpieczny dostęp do sesji VDI**

## Złącza SSL

Cała komunikacja brokera i protokołu może być realizowana za pośrednictwem bezpiecznych połączeń. Zasady komunikacji systemu ThinOS można definiować na poziomie globalnym lub indywidualnym w celu narzucenia żądanego poziomu zabezpieczeń. Trzy „obsługiwane” poziomy to:

- Wysoki — wymagana walidacja certyfikatu
- Ostrzeżenie — akceptacja użytkownika jest wymagana, jeśli sprawdzanie poprawności certyfikatu zakończy się niepowodzeniem
- Niski — nie jest wymagana walidacja certyfikatu

## Zabezpieczenia przewodowe i bezprzewodowe

Cała komunikacja przewodowa i bezprzewodowa 802.1x w przedsiębiorstwie może być zabezpieczona za pomocą WPA/WPA2 PSK/Enterprise z protokołami EAP-PEAP, EAP-LEAP, EAP-TLS lub EAP-FAST.

## Zabezpieczenia protokołu brokera

Podobnie jak komputery stacjonarne z systemami Windows i Linux, system ThinOS umożliwia korzystanie z funkcji szyfrowania i kompresji podczas dołączania do brokerów i serwerów środowiska wirtualnego przy użyciu protokołów RDP, HDX, BLAST, DCV i PCoIP. Ponadto system operacyjny ThinOS jest zgodny ze standardem FIPS 140-2, co zapewnia bezpieczną komunikację w środowiskach narażonych na ataki.

# Zabezpieczenia użytkowników lokalnych

Ochrona danych użytkowników końcowych i kontrolowanie dostępu użytkowników lokalnych

**Chroń urządzenie użytkownika**

**Chroń dane lokalne**

**Bezpieczny dostęp do sesji VDI**

## Ochrona przed ingerencją

Ustawienia uprawnień systemu ThinOS zapewniają solidne zabezpieczenia pulpitu, ograniczając dostęp użytkownika do menu pulpitu, zapobiegając nieautoryzowanemu wyświetlaniu lub wprowadzaniu zmian. Administratorzy IT mają pełny dostęp do interfejsu użytkownika, aby zapewnić całkowitą kontrolę i usprawnić operacje. Ponadto system ThinOS został zaprojektowany tak, aby łączyć się ze środowiskiem wirtualnym bez konieczności instalowania lokalnej przeglądarki.

## Zaawansowane uwierzytelnianie i tokeny

Obsługa uwierzytelniania opartego na tokenach przy użyciu kart inteligentnych CAC i PIV z oprogramowaniem pośredniczącym 90Meter i Activeldentity oraz urządzeń Yubikey z FIDO2.

## Bezpieczne dane uwierzytelniające użytkowników końcowych

Domyślnie urządzenia z systemem ThinOS przechowują poświadczenia logowania i obiekty pamięci podręcznej aplikacji (takie jak mapy bitowe sesji) wyłącznie w pamięci RAM do momentu zakończenia sesji. W systemie plików flash urządzenia nie są zapisywane żadne poświadczenia logowania ani obiekty protokołu. Natomiast urządzenia z systemem Windows i Linux często używają pamięci podręcznej dysku do przechowywania poświadczeń i pamięci podręcznej aplikacji, co czyni je bardziej podatnymi na naruszenia danych lub włamania.

# Zabezpieczenia USB i dysku lokalnego

**Wszystkie systemowe pliki obrazów ThinOS, pliki pakietów, konfiguracje w pamięci podręcznej i dublowane obiekty repozytorium przechowywane w lokalnym systemie plików flash klienta są szyfrowane za pomocą AES w celu zminimalizowania ryzyka naruszenia bezpieczeństwa danych.**

W przypadku jednostek wyposażonych w moduł TPM (Trusted Platform Module, Moduł zaufanej platformy) część kluczy skrótu jest przechowywana w tym komponencie. W związku z tym, nawet jeśli moduły flash zostaną usunięte z urządzeń, dane na tych modułach pozostają niedostępne. Ponadto nie można eksportować certyfikatów używanych do nawiązywania bezpiecznych połączeń SSL, które zostały załadowane i zapisane w pamięci flash urządzenia.

- **Całe buforowanie odbywa się w pamięci RAM i jest nietrwałe**
- **Szyfrowanie AES jest stosowane do wszystkich partycji/plików**
- **Przywrócenie domyślnych ustawień fabrycznych przywraca urządzenie do stanu konfiguracji dostarczonego fabrycznie**
- **Specyficzne dla urządzenia szyfrowanie flash i bezpieczny rozruch**

**System operacyjny Dell ThinOS zapewnia precyzyjną kontrolę nad urządzeniami pamięci masowej USB. Możesz określić, którzy użytkownicy mają dostęp i jak konkretnie mogą korzystać z tych urządzeń, zapewniając zarówno bezpieczeństwo, jak i elastyczność.**

## 1 Flexible controls for IT support

Uprawnienia administracyjne mogą służyć do kontrolowania rozwiązywania problemów z klientem. Dzienniki klienta można eksportować do usługi WMS lub lokalnej pamięci USB.

Konfiguracje urządzeń klienckich są przechowywane na bezpiecznej partycji flash innej niż system operacyjny. Konfiguracje te można wyczyścić, przywracając ustawienia fabryczne.

Certyfikaty klienta i pliki obrazów są przechowywane na bezpiecznej partycji magazynu innej niż system operacyjny. Certyfikaty te można wyczyścić, przywracając ustawienia fabryczne.

## 2 Elastyczna kontrola dostępu do wirtualnego środowiska pamięci masowej USB

### ThinOS BIOS

Porty USB można włączać/wyłączać za pomocą konfiguracji systemu BIOS, lokalnie na urządzeniu lub za pomocą konsoli pakietu Wyse Management Suite. Wyłączenie portów USB dotyczy wszystkich klas urządzeń USB.

### Prywatność i bezpieczeństwo

Zabezpieczenia urządzenia zezwalają lub odmawiają dostępu do urządzeń USB w oparciu o VID/PID lub klasę USB. Pozwala to na selektywne ograniczanie dostępu do dowolnego urządzenia podłączonego do urządzenia klienckiego ThinOS.

### Urządzenia peryferyjne

Ustawienia przekierowania USB mogą służyć do wymuszania obsługi sterownika urządzenia USB z hosta wirtualnego, a nie z urządzenia klienckiego ThinOS.

### Ustawienia sesji

Globalne i specyficzne dla dostawcy zasady partnerów mogą być używane do kontrolowania mapowania i przekierowywania urządzeń USB.

# Najbezpieczniejsze terminale klienckie z systemem Dell ThinOS[1]

### Bezpieczeństwo od pierwszego uruchomienia komputera

Wyjątkowy system operacyjny terminala klienckiego firmy Dell jest bezpieczny z założenia w celu zminimalizowania ryzyka i ochrony pulpitów wirtualnych oraz sesji „pulpitu jako usługi".

### Bezpieczne Zarządzanie

Szczegółowa, scentralizowana kontrola z poziomu pakietu Wyse Management Suite pomaga egzekwować zasady zabezpieczeń, konfigurować ustawienia zgodności urządzeń i zarządzać systemem BIOS.

### Bezpieczne DAne UWierzytelniające Użytkowników końcowych

Przechowywanie poświadczeń użytkownika w pamięci RAM pomaga chronić je przed złośliwym oprogramowaniem i czyści je po ponownym uruchomieniu, zmniejszając ryzyko nieautoryzowanego dostępu.

### Zaufany punkt końcowy

Obsługa popularnych metod uwierzytelniania, standardów zgodności i nietrwałych informacji pomaga chronić dane sesji i zapewnia pewne połączenia z dowolnego miejsca.

### Zamknięta architektura

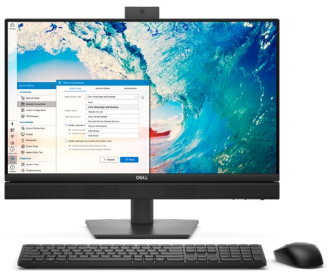
Brak danych wrażliwych i osobowych na urządzeniu lokalnym. Utwardzanie systemu w celu ograniczenia powierzchni narażenia na atak, nieopublikowane interfejsy API, szyfrowanie danych i pakiety plików przygotowywane wyłącznie przez firmę Dell chronią przed wirusami i złośliwym oprogramowaniem.

### Bezpieczna Komunikacja

System ThinOS zapewnia bezpieczną komunikację, obsługując połączenia SSL dla wszystkich protokołów brokera i zaawansowane metody szyfrowania w celu zapewnienia bezpiecznego dostępu do przewodowych i bezprzewodowych sieci przedsiębiorstwa.

## Odkryj terminale klienckie Dell

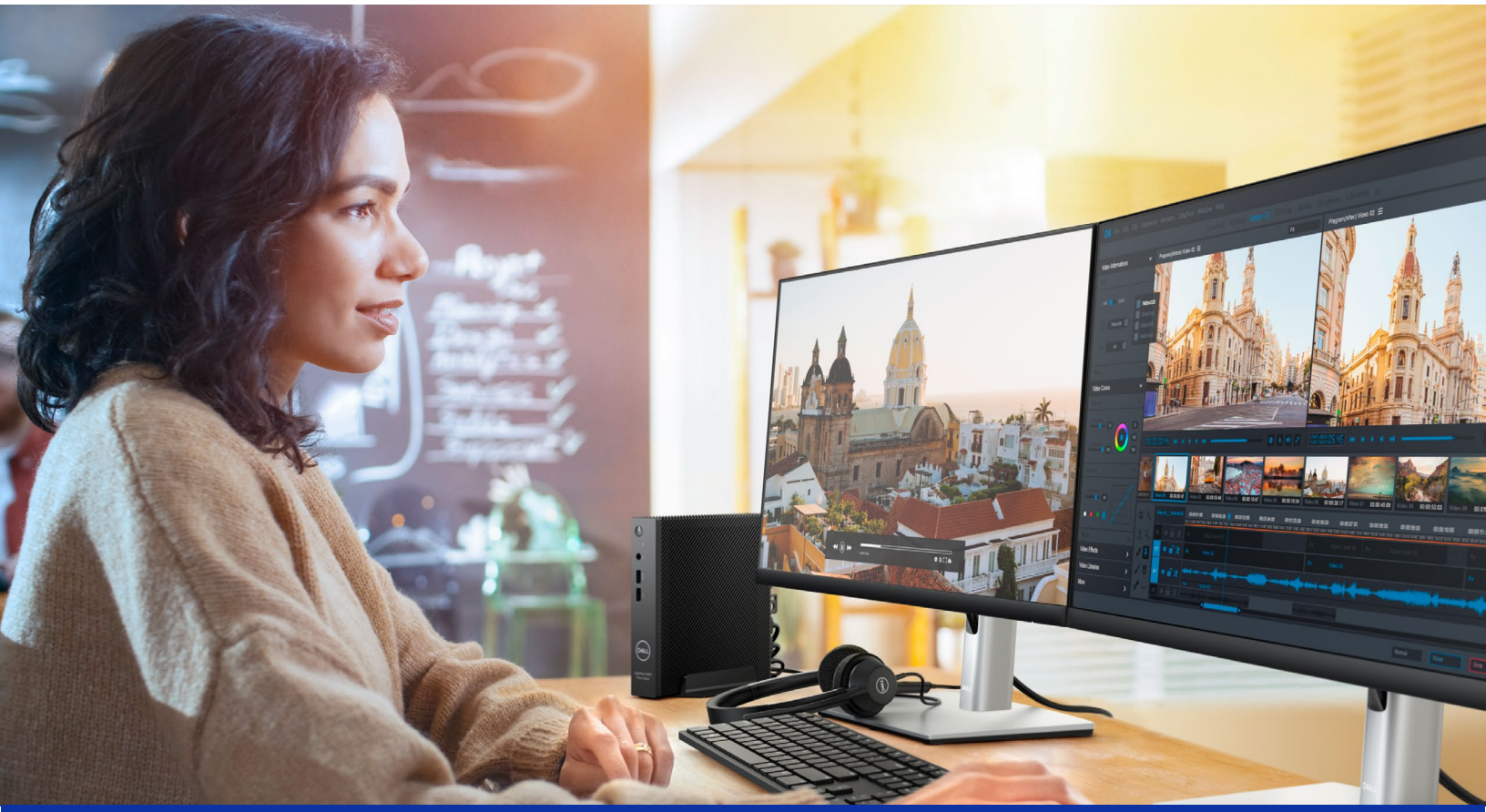
Terminal kliencki OptiPlex 3000 - >



Dell Pro All-in-One 35 W - >

Notebook Dell Pro 14 - >

KORZYŚCI Z ZABEZPIECZEŃ SYSTEMU
DELL THINOS W TRYBIE URZĄDZENIA



# Pracuj bez obaw z dowolnego miejsca dzięki **rozwiązaniom Dell ThinOS i terminali klienckich firmy Dell**

**Zoptymalizowany i bezpieczny punkt końcowy VDI z infrastrukturą pulpitów wirtualnych i rozwiązaniami „pulpit jako usługa”.**

Odwiedź nas
dell.com/CloudClientWorkspace

Więcej informacji
Blog o upraszczaniu infrastruktury IT -->

Dołącz do dyskusji
LinkedIn / X

**Źródła i zastrzeżenia**

[1]Na podstawie wyników analizy przeprowadzonej przez Dell w celu porównania systemu ThinOS w trybie urządzenia z konkurencyjnymi produktami, styczeń 2025 r.

[2] Tryb urządzenia Dell ThinOS to domyślny stan działania systemu Dell ThinOS, zaprojektowany w celu wymuszenia wysokiego stanu bezpieczeństwa od samego początku. W wersji 2508 i nowszych ThinOS zapewnia administratorom IT większą elastyczność, umożliwiając instalację komercyjnych przeglądarek internetowych i wdrażanie komponentów oprogramowania innych firm. Aby zapewnić zgodność z systemem ThinOS 10, aplikacje innych firm muszą być zgodne z systemem Ubuntu 24.04 x86_64, zawierać pakiet instalacyjny Debian i pomyślnie przejść wszystkie kontrole zależności systemu operacyjnego przeprowadzone przy użyciu narzędzia Kreator aplikacji (w zależności od możliwości urządzenia klienckiego). Wdrożenie wymaga wybranie trybu izolowanego lub natywnego. Aplikacje działające w trybie natywnym mogą podlegać ograniczeniom w zależności od ich działania. Zdecydowanie zaleca się przeprowadzenie dokładnych testów w celu potwierdzenia pomyślnej instalacji i funkcjonalności przed wdrożeniem. Pełne informacje na temat obsługiwanych aplikacji i wytycznych dotyczących wdrażania można znaleźć w przewodniku instalacji dla klientów dostępnym na stronie Dell.com/support.