POZNAWAJ

Dell Trusted Workspace

Bezpieczna praca w dowolnym miejscu

dzięki zabezpieczeniom sprzętowym i programowym stworzonym dla dzisiejszego świata opartego na chmurze.

Praca hybrydowa narażała organizacje na nowe wektory ataków. W czasach, gdy cyberprzestępcy stosują coraz bardziej zaawansowane techniki, skuteczne zabezpieczenia punktów końcowych wymagają wielu warstw ochrony, które chronią urządzenie, sieć i chmurę.

Ogranicz skalę ataku i wyprzedzaj współczesne zagrożenia dzięki kompleksowemu portfolio zabezpieczeń sprzętowych i programowych.

Dowiedz się więcej o portfolio →

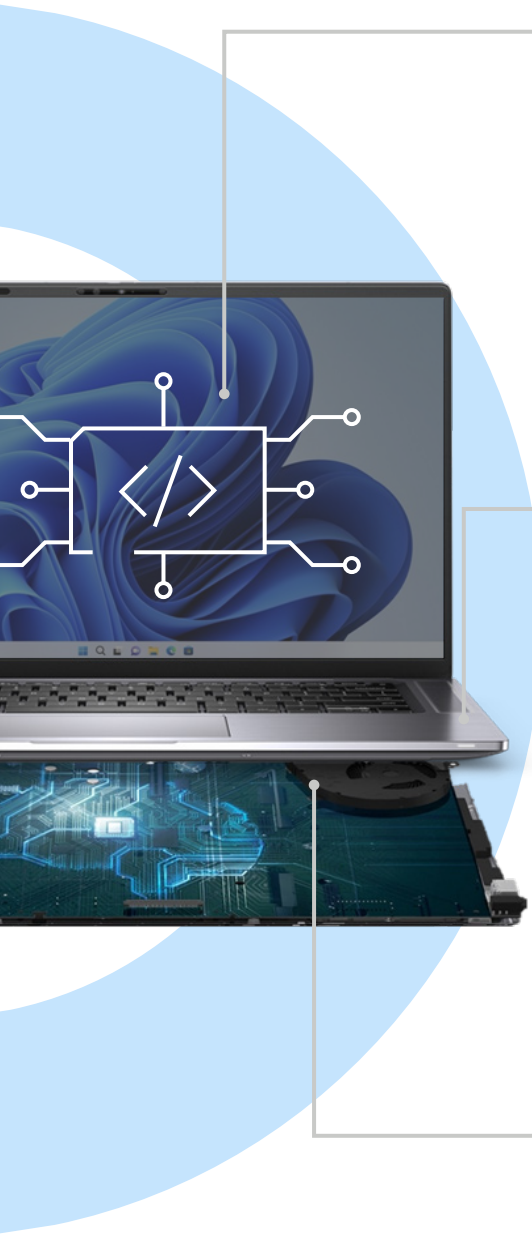
Najbezpieczniejsze komputery klasy komercyjnej z obsługą sztucznej inteligencji[1] →

Oprogramowanie zwiększające bezpieczeństwo każdej floty →

DELL Technologies

Dell Trusted Workspace

Wiele warstw ochrony



Zewnętrzne **zabezpieczenia oprogramowania**

Warstwa zaawansowanej ochrony przed zagrożeniami z oprogramowaniem od specjalistycznie dobranego ekosystemu partnerów. Wykorzystaj zalety i wzrost wydajności, które wynikają z konsolidacji zakupów zabezpieczeń.

Wbudowane **zabezpieczenia w sprzęcie i oprogramowaniu wewnętrznym**

Zapobiegaj atakom podstawowym i wykrywaj je dzięki najbezpieczniejszym w branży komputerom komercyjnym z obsługą sztucznej inteligencji[1]. Głębokie warstwy ochrony na poziomie systemu BIOS / oprogramowania wewnętrznego i sprzętu zapewniają ochronę urządzenia podczas użytkowania.

Tylko firma Dell integruje telemetrię komputerów PC z wiodącym w branży oprogramowaniem w celu poprawy bezpieczeństwa całej floty.[1]

Ochrona **sprzętu w łańcuchu dostaw**

Pracuj bez obaw, wiedząc, że Twoje urządzenie jest bezpieczne od pierwszego uruchomienia. Bezpieczne projektowanie, opracowywanie i testowanie komputerów PC pomaga zmniejszyć ryzyko wystąpienia luk w zabezpieczeniach produktów. Rygorystyczne kontrole łańcucha dostaw zmniejszają ryzyko manipulacji produktem.

Zapobieganie zagrożeniom, wykrywanie ich w dowolnym miejscu i reagowanie na nie

Dell SafeGuard and Response

Dell SafeData

Ochrona przed coraz poważniejszymi zagrożeniami

Dell SafeBIOS

Dell SafeID

Podczas dostawy upewnij się, że sprzęt jest nienaruszony

Dell SafeSupply Chain

Dell Trusted Workspace — rozwiązanie z wbudowanymi zabezpieczeniami

Najbezpieczniejsze komercyjne komputery PC z obsługą sztucznej inteligencji na świecie[1]

Bezpieczeństwo od pierwszego uruchomienia komputera

Rygorystyczne, najnowocześniejsze kontrole łańcucha dostaw i opcjonalne dodatki, takie jak unikalna dla firmy Dell funkcja **zabezpieczonej weryfikacji komponentów**, zapewniają integralność komputera. Więcej informacji →

Weryfikacja integralności oprogramowania sprzętowego

Ekskluzywna dla firmy Dell **weryfikacja oprogramowania wewnętrznego**, sprzętowe zabezpieczenie stosowane w procesorach Intel, chroni przed nieautoryzowanym dostępem i manipulowaniem wysoce uprzywilejowanym oprogramowaniem wewnętrznym. Więcej informacji →

Bezpieczne dane uwierzytelniające użytkowników końcowych

Weryfikacja dostępu użytkownika za pomocą unikalnego dla firmy Dell **SafeID**, dedykowanego układu zabezpieczającego, który ukrywa dane uwierzytelniające użytkownika przed złośliwym oprogramowaniem. Więcej informacji →

Utrzymaj integralność systemu BIOS

Wyłapuj i odpieraj zagrożenia dzięki unikalnej weryfikacji systemu BIOS firmy Dell **SafeBIOS**. Można tu ocenić uszkodzenia systemu BIOS, naprawić go i pozyskać przydatne informacje, dzięki którym można ograniczyć podatność na przyszłe zagrożenia. Więcej informacji →

Wykrywanie zagrożeń

Wskaźniki ataku (oferowana tylko przez Dell funkcja wczesnego alarmu) skanują system pod kątem zachowań wskazujących na zagrożenie, zanim dojdzie do powstania szkód. Więcej informacji→

Wyłapywanie znanych luk w zabezpieczeniach

Unikalna funkcja **Common Vulnerabilities and Exposures (CVE) Detection** firmy Dell monitoruje publicznie zgłaszane luki w zabezpieczeniach systemu BIOS i zaleca aktualizacje w celu zmniejszenia ryzyka. Więcej informacji →

Principled Technologies® *Wiodąca pozycja w branży potwierdzona przez Principled Technologies**

Zmniejsz lukę w zabezpieczeniach IT dzięki telemetrii komputera

Wzbogać rozwiązania programowe o informacje poniżej poziomu systemu operacyjnego. Tylko firma Dell integruje telemetrię komputerów PC z wiodącymi w branży dostawcami oprogramowania w celu poprawy bezpieczeństwa całej floty[1]. Dowiedz się więcej →

Więcej informacji o Dell Trusted Devices

Notebooki →

Komputery stacjonarne →

Stacje robocze →

Wyniki opublikowanych badań obejmują tylko urządzenia z procesorami Intel.

DELL Technologies

Dell Trusted Workspace — wbudowane zabezpieczenia

Oprogramowanie zwiększające bezpieczeństwo każdej floty

Udaremnij zaawansowane cyberataki dzięki funkcjom Dell SafeGuard and Response

Zapobieganie zagrożeniom, wykrywanie ich w dowolnym miejscu i reagowanie na nie. Sztuczna inteligencja i uczenie maszynowe proaktywnie wykrywają i blokują ataki na punkty końcowe, podczas gdy eksperci ds. bezpieczeństwa pomagają wyszukiwać i usuwać zidentyfikowane zagrożenia w punktach końcowych, sieci i chmurze.

Partnerzy

CrowdStrike Falcon® →

Sophos | Secureworks® Taegis™ XDR →

Chroń dane na urządzeniu i w chmurze dzięki Dell SafeData

Zapewnij użytkownikom możliwość bezpiecznej współpracy z dowolnego miejsca. Netskope przyjmuje podejście do bezpieczeństwa i dostępu do chmury skoncentrowane na danych, chroniąc dane i użytkowników wszędzie, podczas gdy usługa Absolute zapewnia IT widoczność, ochronę i trwałość poza korporacyjną zaporą ogniową.

Partnerzy

Mechanizm autonaprawy w zakresie punktów końcowych, aplikacji i sieci dzięki Absolute →

Poznaj rozwiązania Security Service Edge z Netskope →

Poznaj Dell Security Services

Dzięki firmie Dell klienci mogą samodzielnie zarządzać bezpieczeństwem lub zlecić to specjalistom. Skorzystaj z naszego w pełni zarządzanego rozwiązania SecOps 360°, zaprojektowanego w celu zapobiegania zagrożeniom bezpieczeństwa w środowisku IT, reagowania na nie i odzyskiwania danych.

Dowiedz się więcej o usłudze Managed Detection and Response Pro Plus →

Dell Trusted Workspace – zabezpieczenia wspomagane sprzętowo

Zintegrowane zabezpieczenia

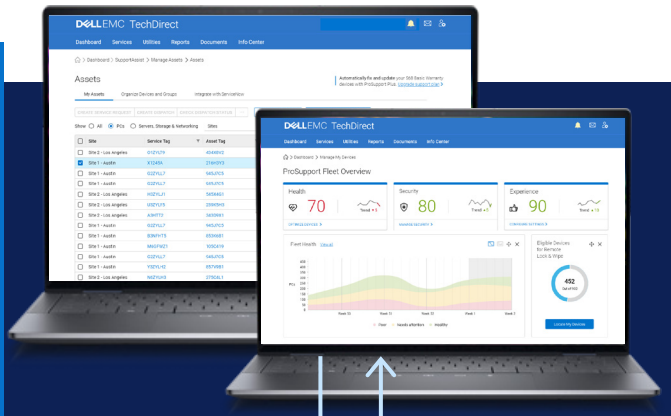
Ewoluujące cyberzagrożenia omijają zabezpieczenia oparte wyłącznie na oprogramowaniu. Pomóż zmniejszyć powierzchnię ataku punktów końcowych za pomocą zabezpieczeń wspomaganych sprzętowo.

Aby zapewnić ochronę przed nowoczesnymi zagrożeniami, zabezpieczenia sprzętowe i programowe muszą ze sobą współpracować. W tym zakresie pomocą może służyć firma Dell. Współpracujemy z wiodącymi w branży partnerami w zakresie bezpieczeństwa, łącząc bogatą telemetrię na poziomie urządzeń z najnowocześniejszym wykrywaniem zagrożeń w celu poprawy bezpieczeństwa Twojej floty.

- ✓ **Zmniejszenie obszaru narażonego na ataki**
- ✓ **Poprawa wykrywania zagrożeń**
- ✓ **Zaufanie do urządzeń**
- ✓ **Konsolidacja dostawców**

Zewnętrzne zabezpieczenia oprogram

Tylko firma Dell integruje telemetrię komputerów PC z wiodącym w branży oprogramowaniem w celu poprawy bezpieczeństwa całej floty[1] [2]



SYSTEM OPERACYJNY

Wbudowane zabezpieczenia sprzętowe i w oprogramowaniu wewnętrznym

Dell SafeBIOS

Aplikacja Dell Trusted Device

Weryfikacja systemu BIOS | Wykrywanie typowych luk w zabezpieczeniach i podatności | Oznaki ataku

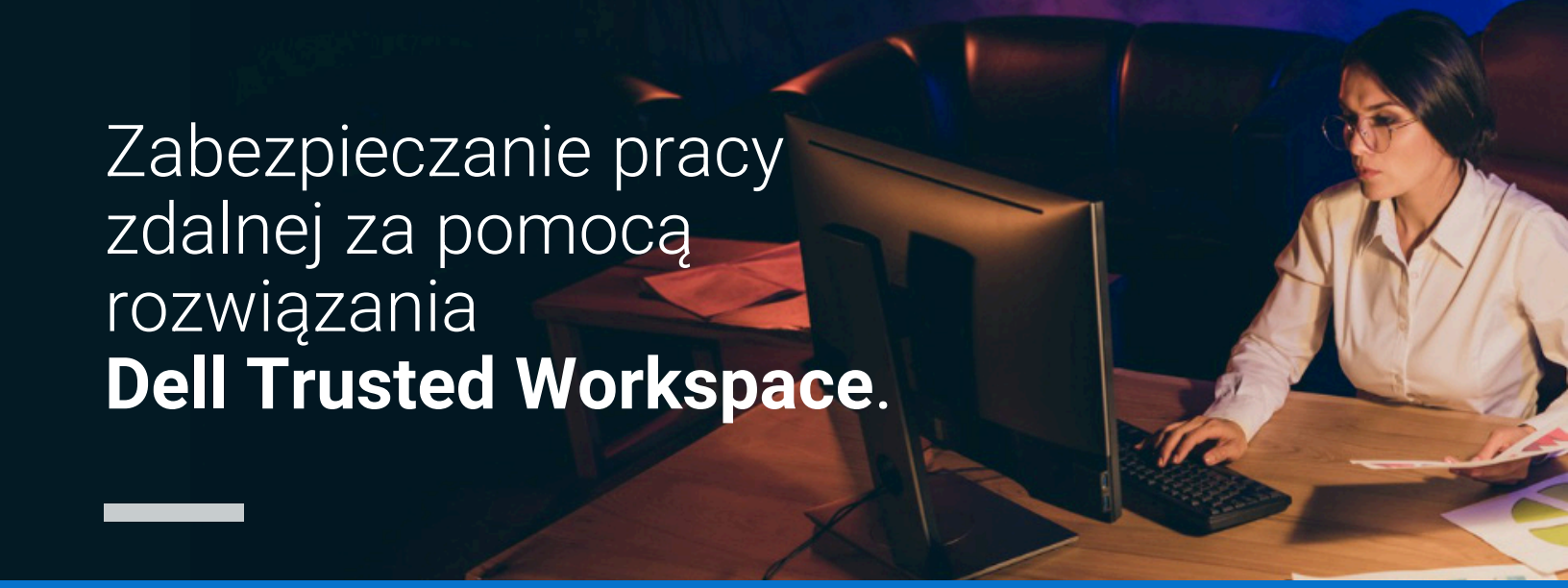
Funkcje układów scalonych „poniżej systemu operacyjnego”

Kooperacyjne zabezpieczenia łańcucha dostaw

Dell SafeSupply Chain[3]

Zabezpieczona weryfikacja komponentów na urządzeniu • w chmurze

DELL Technologies



Zabezpieczanie pracy zdalnej za pomocą rozwiązania **Dell Trusted Workspace**.

Zabezpieczenia wbudowane i sprzętowe

Zewnętrzne zabezpieczenia oprogramowania

Zmniejsz powierzchnię ataku i popraw długoterminową odporność cybernetyczną dzięki wielu warstwom obrony.

Odwiedź nas
dell.com/endpoint-security

Kontakt
global.security.sales@dell.com

Więcej informacji
Zabezpieczenia punktów końcowych — blogi →

Dołącz do dyskusji
LinkedIn /delltechnologies

X @delltech

Źródła i zastrzeżenia

[1] Na podstawie wewnętrznej analizy przeprowadzonej przez firmę Dell, październik 2024 r. (Intel) i marzec 2025 r. (AMD). Dotyczy komputerów z procesorami Intel i AMD. Nie wszystkie funkcje są dostępne na wszystkich komputerach osobistych. W przypadku niektórych funkcji wymagany jest dodatkowy zakup. Komputery z procesorami Intel zostały zweryfikowane przez Principled Technologies. Porównanie zabezpieczeń, kwiecień 2024 r. [2] Integracje dostępne dla CrowdStrike Falcon Insight XDR i Absolute. [3] Dostępność zależy od regionu.

DELL Technologies