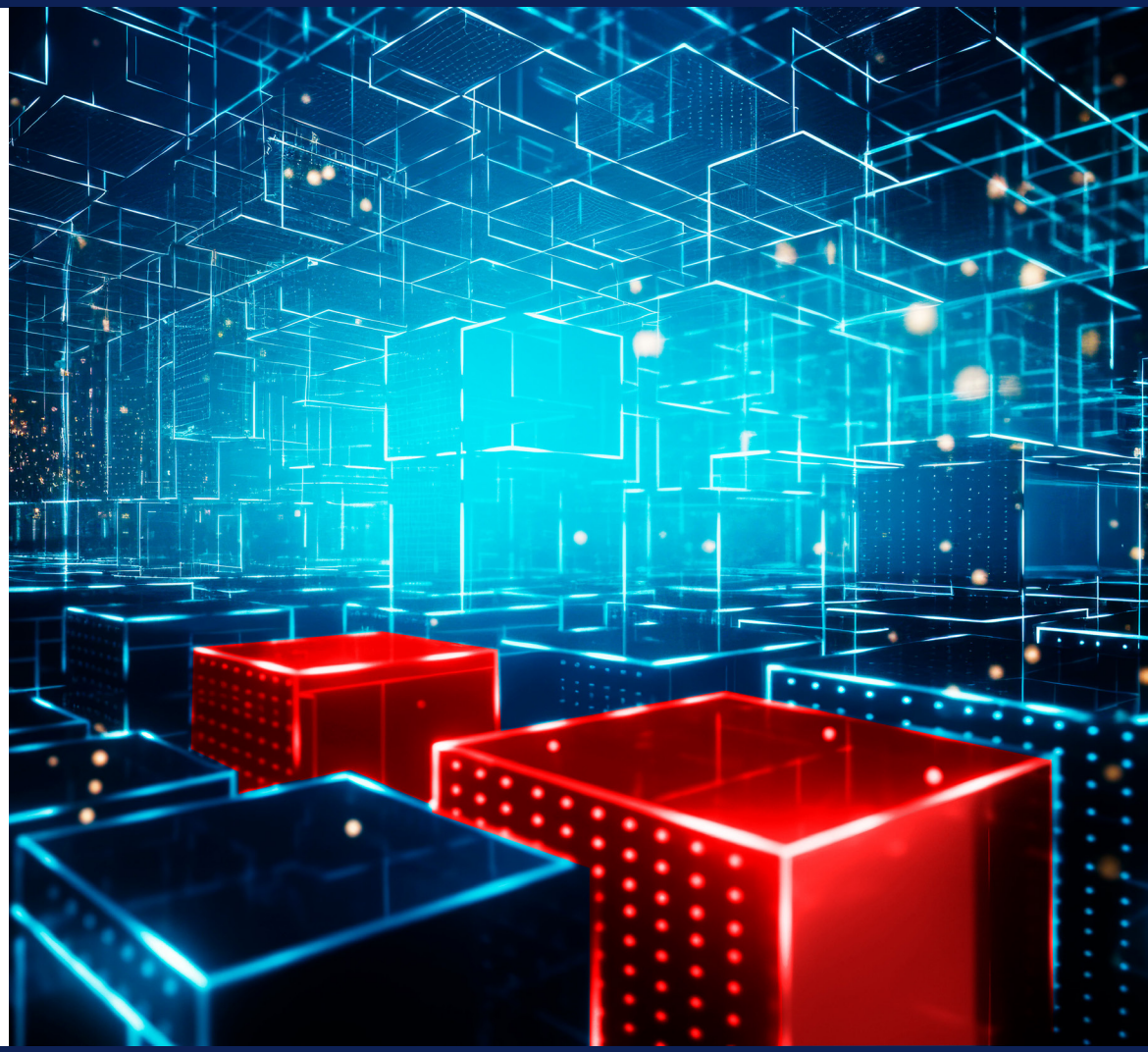
DELL Technologies

intel

Zabezpieczanie korzystania ze sztucznej inteligencji w punkcie końcowym

Chroń obciążenia robocze związane ze sztuczną inteligencją na urządzeniu dzięki bezpiecznym, nowoczesnym urządzeniom i nastawieniu na przeciwdziałanie zagrożeniom.

CROWDSTRIKE ABSOLUTE®



Streszczenie dla kierownictwa

Sztuczna inteligencja na urządzeniu przynosi ogromne korzyści, ale wiąże się też z cyberzagrożeniami. W tym e-booku przedstawimy, ak bezpiecznie przygotować swoją organizację do wykorzystania innowacji w zakresie sztucznej inteligencji w punkcie końcowym.

Spis treści

Powierzchnia ataku na sztuczną inteligencję na urządzeniu

Co może być celem

Wszystkie nowe technologie wiążą się z ryzykiem dla cyberbezpieczeństwa z jednego powodu: to nowe terytorium. Masz do czynienia z czymś nieznanym. Widzieliśmy to w przypadku chmury obliczeniowej, blockchainu i wielu innych technologii. To samo dotyczy sztucznej inteligencji na urządzeniu. Kluczem do ograniczenia tego ryzyka jest, jak zawsze, przyjrzenie się nieznanemu.

Zanim opowiemy o tym, jakie zabezpieczenia są potrzebne, aby zminimalizować obszar narażony na ataki, warto wspomnieć, co zabezpieczamy i dlaczego. Pomyśl o tym jak o systemie rur w budynku, w którym mieści się wiele firm. Rury te transportują po całym budynku wodę, gaz itp. do różnych zastosowań. Jeśli materia przepływająca przez rury jest zanieczyszczona lub przepływ jest zakłócony, nie może wykonać swojej pracy. Jeśli rury przenoszące materię są zużyte lub uszkodzone, nie mogą wykonywać swoich zadań. Zarówno rury, jak i ich zawartość muszą być w dobrym stanie technicznym, aby spełnić potrzeby odpowiednich zastosowań.►

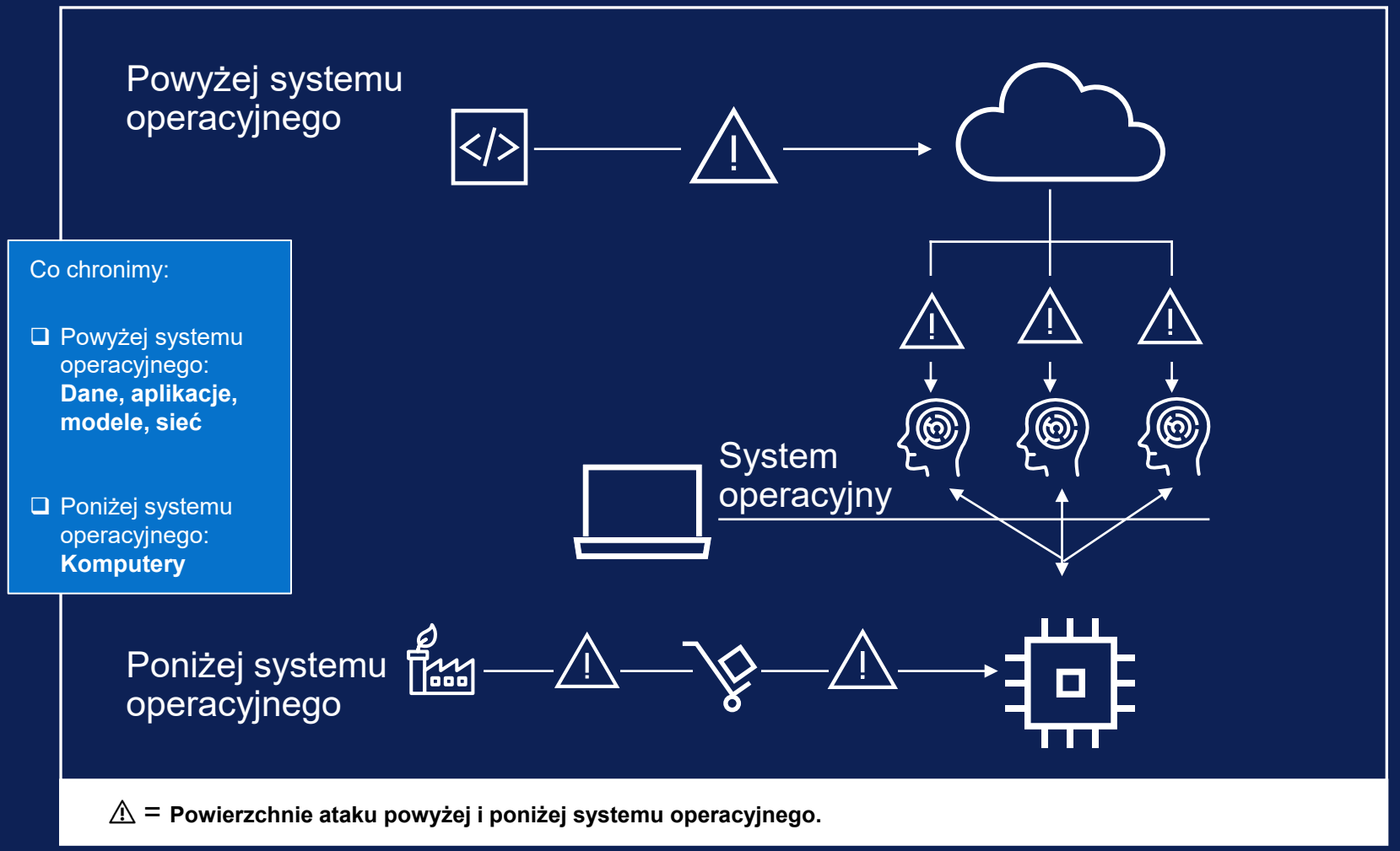
Powierzchnia ataku na sztuczną inteligencję na urządzeniu — ciąg dalszy

Co może być celem — ciąg dalszy

Odnieśmy to teraz do sztucznej inteligencji w punkcie końcowym:

- Rury to Twoja infrastruktura — Twoje komputery, sieci firmowe. Sposób i miejsce pracy.
- Materiał przepływający przez rury to dane, aplikacje i modele, które napędzają różne zastosowania AI. Narzędzia i zasoby niezbędne do wykonywania pracy.

Dobrze myślisz. Cyberprzestępcy atakują oba aspekty. Mogą wykraść własność intelektualną w celu otrzymania okupu albo zainfekować dane lub modele, aby wpłynąć na ich działanie. Konsekwencje mogą być poważne, co prowadzi do szkód finansowych i uszczerbku na reputacji i/lub może wywołać kontrole regulacyjne.►



Zagrożenia bezpieczeństwa w punkcie końcowym

Taktyki, których atakujący używają, aby uzyskać dostęp

Teraz omówimy metody, których atakujący mogą użyć do uzyskania dostępu do obu celów.

Naruszenie bezpieczeństwa urządzeń. Jak wynika z badań przeprowadzonych przez firmę Forrester Research w marcu 2025 r. („Endpoint Security Market Insights"), komputery należą do głównych celów współczesnych cyberzagrożeń. Ten rodzaj ataku może nastąpić na długo przed rozpoczęciem pracy nad sztuczną inteligencją na urządzeniu, tj. **atak na łańcuch dostaw sprzętu lub oprogramowania**. W łańcuchu dostaw występują dziesiątki, jeśli nie setki, punktów, w których złośliwy podmiot może manipulować komponentami — np. obwodami, oprogramowaniem wewnętrznym — w celu powstania słabych ogniw, które będzie mógł później wykorzystać. Wyobraź sobie nadchodzącą katastrofę firmy inwestycyjnej, która otrzymała zupełnie nową przesyłkę komputerów z podrobionymi elementami.

Naruszenie tożsamości. Naruszenia związane ze skradzionymi lub naruszonymi poświadczeniami są jednym z najszybciej rozwijających się wektorów ataków. Nic dziwnego. Osoby atakujące korzystające z prawidłowych poświadczeń mogą zalogować się do komputera, swobodnie poruszać się w sieci korporacyjnej i pozostać niewykryte przez długi czas. Według najnowszego raportu Cost of a Data Breach firmy IBM wykrywanie i eliminowanie tych naruszeń trwało średnio 292 dni, co było najdłuższym spośród wszystkich badanych wektorów ataków. Ten poziom dostępu jest zbyt cenny, aby podmioty atakujące mogły go zignorować. Jak wynika z badania firmy Zscaler, złośliwe podmioty intensyfikują swoje działania polegające na kradzieży poświadczeń poprzez usprawnianie i zwiększanie skali ataków phishingowych za pomocą generatywnej sztucznej inteligencji. Ten nieupoważniony dostęp do wrażliwych danych służących do szkolenia lub wnioskowania albo nawet bezpośrednio do modeli jest klasyfikowany jako **atak na łańcuch dostaw modelu**.

Zagrożenie wewnętrzne. Z ostatnich badań wynika, że w porównaniu z innymi wektorami ataków **złośliwe ataki wewnętrzne** spowodowały najwyższe koszty, średnio 4,99 mln USD. Należy pamiętać, że ataki wewnętrzne mogą wystąpić w całym łańcuchu dostaw sprzętu, oprogramowania i modelu.►

Mediana czasu, w jakim użytkownik końcowy może paść ofiarą ataku z zastosowaniem wiadomości e-mail służącej do **phishingu**: <60 sekund*

Średnio 292 dni na wykrycie i wyeliminowanie **naruszenia poświadczeń** **

Złośliwe ataki wewnętrzne kosztują średnio 4,99 mln USD**

** Źródło: Verizon DBIR, 2024 r.*
*** Źródło: IBM Cost of a Data Breach, 2024 r.*

Środki zaradcze, którymi należy dysponować

Co zmniejsza ryzyko

Żaden z tych celów ataku nie jest zasadniczo nowy. Cele końcowe ataków też nie. Jak zawsze, chcemy skupić się na zapewnieniu bezpieczeństwa i odporności floty. **Warstwowe stosowanie środków zaradczych** może pomóc zmniejszyć obszar narażony na ataki i natychmiast zwracać uwagę na wszelkie podejrzane działania.

Podejście „zero trust” pozwoli zminimalizować ryzyko w całej flocie. Zasady te — nigdy nie ufaj, zawsze weryfikuj i ciągle monitoruj — pomagają wyprzedzić atakujących. Nie da się zablokować 100% ataków. Aby zapewnić wysoki poziom bezpieczeństwa, potrzebujesz **widoczności i kontroli** w całym ekosystemie IT.

Mając to na uwadze, ponownie oceń swoją infrastrukturę, zwłaszcza systemy i procesy, które wchodzą w interakcję z AI. Jakie środki zaradcze minimalizują ryzyko naruszenia bezpieczeństwa urządzeń, naruszenia tożsamości i zagrożeń wewnętrznych?►

Zasady modelu „zero trust” pomagają się bronić przed ryzykiem i zmniejszać zasięg cyberzagrożeń

Środki zaradcze, którymi należy dysponować — ciąg dalszy

Co zmniejsza ryzyko — ciąg dalszy

Istnieją dwie ogólne kategorie środków zaradczych.

Zabezpieczenia „poniżej poziomu systemu operacyjnego" chronią urządzenia AI, na których pracujesz. Można podzielić to na dwie części:

- Ochrona floty dzięki urządzeniom **zbudowanym**
- **w bezpieczny sposób**. Oznacza to korzystanie
- z komputerów ze sztuczną inteligencją, które są z założenia bezpieczne, tj. zostały skonstruowane zgodnie z zasadami bezpiecznego projektowania i w ramach bezpiecznego łańcucha dostaw.
- Ochrona floty dzięki urządzeniom z **wbudowanymi zabezpieczeniami**. Bezpieczne komputery ze sztuczną inteligencją są wyposażone w warstwy wbudowanej ochrony, które zapewniają fabrycznie wgląd aż do poziomu systemu BIOS i warstw układów scalonych.

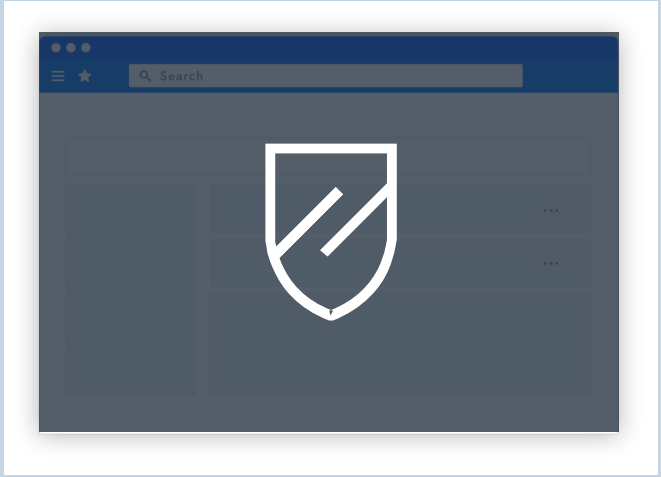
Zabezpieczenia „powyżej poziomu systemu operacyjnego" chronią dostęp do modeli sztucznej inteligencji. Chroń dane i modele, *z którymi* pracujesz, oraz sieci firmowe, *w których* pracujesz, dzięki **zabezpieczeniom oprogramowania**. Ochrona operacji bezpieczeństwa uczenia maszynowego i monitorowanie ruchu sieciowego wdrożonych obciążeń roboczych związanych ze sztuczną inteligencją są niezbędne.►

Ochrona poniżej poziomu systemu operacyjnego

Bezpieczne komputery AI PC

Bezpieczeństwo sprzętu i oprogramowania wewnętrznego, bezpieczeństwo łańcucha dostaw, podstawowe układy scalone

Powyżej poziomu zabezpieczeń systemu operacyjnego



Zabezpieczenie programowe

Dodatkowa warstwa zabezpieczeń punktów końcowych, sieci i środowisk chmurowych

Usługi w zakresie bezpieczeństwa i wiedza ekspercka umożliwiają połączenie wszystkich elementów.

Stosowanie najlepszych praktyk we flocie

W jaki sposób komputery Dell AI PC zapewniają podstawowe bezpieczeństwo Twojej floty

Tutaj może pomóc Dell Trusted Workspace. Nasi technolodzy opracowują i projektują zabezpieczenia naszych komercyjnych komputerów AI PC z głębokim zrozumieniem nastawienia na przeciwdziałanie zagrożeniom.

Poniżej systemu operacyjnego bezpieczna konstrukcja, solidne mechanizmy kontroli łańcucha dostaw i opcjonalna gwarancja łańcucha dostaw pomagają zapewnić bezpieczeństwo komputerów od pierwszego uruchomienia. Wbudowane zabezpieczenia sprzętu i oprogramowania wewnętrznego chronią komputer podczas użytkowania, np. występujące wyłącznie w komputerach firmy Dell wykrywanie manipulacji na poziomie systemu BIOS (Dell SafeBIOS) i zabezpieczenia poświadczeń bez użycia hasła (Dell SafeID) w celu ochrony przed nieupoważnionym dostępem. Ponadto technologie krzemowe firmy Intel® pomagają stworzyć podstawę do ochrony różnych aspektów sztucznej inteligencji w ramach jej użytkowania przez klientów AI PC. Firma Intel pomaga np. zabezpieczać dane sztucznej inteligencji w spoczynku na komputerze klienckim dzięki akceleracji szyfrowania modelu na dysku.►

Stosowanie najlepszych praktyk we flocie — ciąg dalszy

W jaki sposób komputery Dell AI PC zapewniają podstawowe bezpieczeństwo Twojej floty — ciąg dalszy

Aby uzupełnić tę ochronę poniżej poziomu systemu operacyjnego, technologia Persistence naszego partnera Absolute może zostać wbudowana fabrycznie, co zapewni jeszcze lepszy wgląd i pełniejszą kontrolę przez cały cykl życia komputera. Umożliwi np. geolokalizację urządzeń na trasie i działanie mechanizmu autonaprawy krytycznych aplikacji w najgorszym przypadku.

Warto zaznaczyć, że firma Dell opracowała ekosystem rozwiązań dla partnerów w zakresie oprogramowania, w tym CrowdStrike Falcon XDR i Absolute Secure Access, które stosują zasady modelu „zero trust" w celu ochrony łańcucha dostaw modelu przed nieupoważnionym dostępem **powyżej systemu operacyjnego**. Korzystając z tych rozwiązań, można tworzyć i egzekwować zasady ze szczegółową kontrolą dostępu (np. kontrolą dostępu opartą na rolach), aby ograniczać ryzyko, że złośliwe osoby wewnętrzne uzyskają dostęp do modeli sztucznej inteligencji lub je zmodyfikują.►

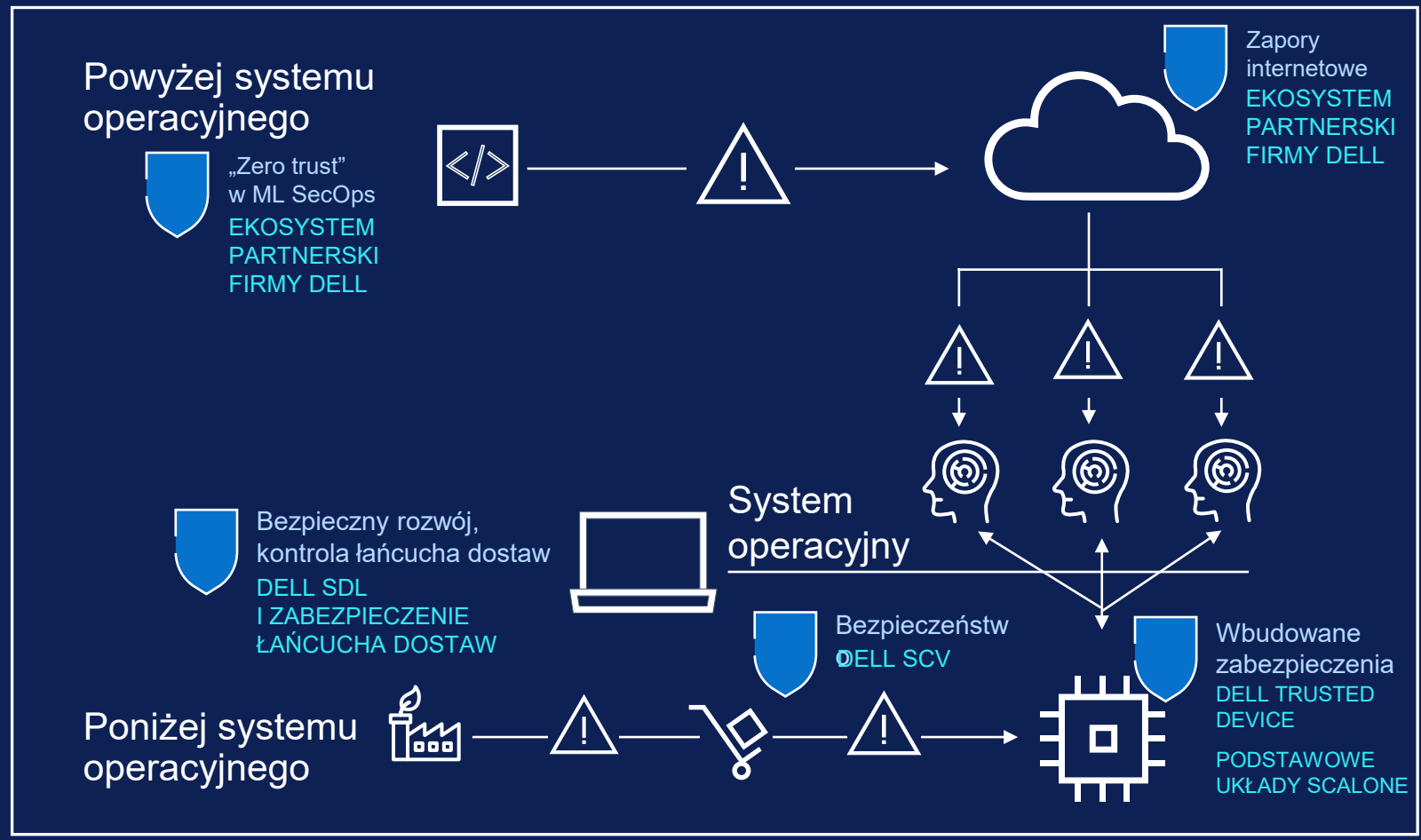
Stosowanie najlepszych praktyk we flocie — ciąg dalszy

W jaki sposób komputery Dell AI PC zapewniają podstawowe bezpieczeństwo Twojej floty — ciąg dalszy

Razem stanowi to ***bezpieczeństwo dla AI.*** Funkcje te chronią obciążenia robocze związane ze sztuczną inteligencją na urządzeniu przed cyberatakami, umożliwiając skupienie się na innowacjach i osiąganiu sukcesów biznesowych ▶

Zatrzymaj zaawansowane ataki na punkty końcowe dzięki skoordynowanym zabezpieczeniom sprzętu i oprogramowania

Firma Dell współpracuje z firmami Intel i CrowdStrike, aby zintegrować warstwy poniżej i powyżej systemu operacyjnego z zabezpieczeniami wspomaganym sprzętowo. *Więcej informacji >*



Najważniejsze wnioski i kolejne kroki

Zabezpieczanie sztucznej inteligencji w punkcie końcowym z pomocą firmy Dell

Firmy są podekscytowane sztuczną inteligencją, ale według niedawnego badania CISO przeprowadzonego przez Absolute gotowość na sztuczną inteligencję jest opóźniona. Analiza milionów urządzeń ujawniła, że populacja komputerów nie jest w stanie w pełni wykorzystać nowych możliwości sztucznej inteligencji. **Firma Dell może pomóc zebrać to wszystko razem.**

Opracowywanie i wdrażanie modeli sztucznej inteligencji na bezpiecznym, nowoczesnym fundamencie. Wsparcie techniczne dla systemu Windows 10 zakończy się w październiku 2025 r. Komputery z systemem Windows 10 nie będą już otrzymywać aktualizacji zabezpieczeń, nowych aktualizacji funkcji ani pomocy technicznej. Starsze urządzenia mogą nie spełniać wymagań systemu Windows 11 oraz nie będą miały najnowszych wbudowanych usprawnień w zakresie wydajności, zabezpieczeń i funkcji sztucznej inteligencji. Przejdź na komputery **Dell Pro** lub **Dell Pro Max z procesorami Intel® Core™ Ultra z technologią Intel vPro®**, aby zyskać zaawansowane zabezpieczenia i chronić obciążenia robocze związane ze sztuczną inteligencją dzięki **najbezpieczniejszym na świecie komputerom AI PC klasy komercyjnej***. ►

Wsparcie techniczne dla systemu Windows 10 zakończy się w październiku.

Przejdź na najnowsze komputery Dell AI PC z podzespołami firmy Intel, aby uzyskać korzyści z bezpieczeństwa i ulepszeń sztucznej inteligencji:

Kup Dell Pro ● Dell Pro Max

*Najbezpieczniejsze na świecie komputery AI PC klasy komercyjnej**

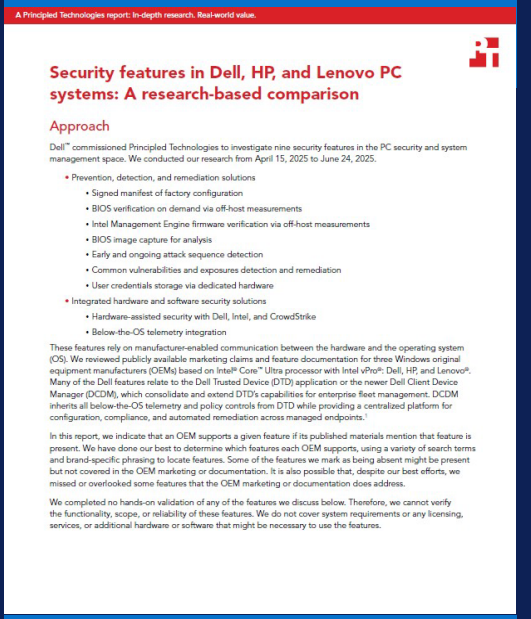
Zapoznaj się z oprogramowaniem i usługami o wartości dodanej, aby poprawić stan bezpieczeństwa:

Oprogramowanie i integracje

Dell AI Factory

WIODĄCA POZYCJA W BRANŻY

Firma Principled Technologies ustaliła, że zabezpieczenia komputerów AI PC klasy komercyjnej firm Dell i Intel wygrywają z konkurencją



A Principled Technologies report: In-depth research. Real-world value.

Security features in Dell, HP, and Lenovo PC systems: A research-based comparison

Approach

Dell™ commissioned Principled Technologies to investigate nine security features in the PC security and system management space. We conducted our research from April 15, 2025 to June 24, 2025.

- Prevention, detection, and remediation solutions
  - Signed manifest of factory configuration
  - BIOS verification on demand via off-host measurements
  - Intel Management Engine firmware verification via off-host measurements
  - BIOS image capture for analysis
  - Early and ongoing attack sequence detection
  - Common vulnerabilities and exposures detection and remediation
  - User credentials storage via dedicated hardware
- Integrated hardware and software security solutions
  - Hardware-assisted security with Dell, Intel, and CrowdStrike
  - Below-the-OS telemetry integration

These features rely on manufacturer-enabled communication between the hardware and the operating system (OS). We reviewed publicly available marketing claims and feature documentation for three Windows original equipment manufacturers (OEMs) based on Intel® Core™ Ultra processor with Intel vPro®: Dell, HP, and Lenovo®. Many of the Dell features relate to the Dell Trusted Device (DTD) application or the newer Dell Client Device Manager (DCDM), which consolidate and extend DTD's capabilities for enterprise fleet management. DCDM inherits all below-the-OS telemetry and policy controls from DTD while providing a centralized platform for configuration, compliance, and automated remediation across managed endpoints.[1]

In this report, we indicate that an OEM supports a given feature if its published materials mention that feature is present. We have done our best to determine which features each OEM supports, using a variety of search terms and brand-specific phrasing to locate features. Some of the features we mark as being absent might be present but not covered in the OEM marketing or documentation. It is also possible that, despite our best efforts, we missed or overlooked some features that the OEM marketing or documentation does address.

We completed no hands-on validation of any of the features we discuss below. Therefore, we cannot verify the functionality, scope, or reliability of these features. We do not cover system requirements or any licensing, services, or additional hardware or software that might be necessary to use the features.

Przeczytaj opracowanie

Zastrzeżenia

* Na podstawie analizy zewnętrznej przeprowadzonej przez firmę Principled Technologies polegającej na porównywaniu komputerów AI PC klasy komercyjnej firmy Dell z procesorami Intel z komputerami firm HP i Lenovo, lipiec 2025 r. Na podstawie wewnętrznej analizy firmy Dell dotyczącej światowego rynku komputerów osobistych, październik 2024 r. Stwierdzenie dotyczy komputerów z procesorami Intel. Nie wszystkie funkcje są dostępne na wszystkich komputerach osobistych. W przypadku niektórych funkcji wymagany jest dodatkowy zakup.

Więcej informacji:

Skontaktuj się z nami: Global.Security.Sales@Dell.com

Odwiedź nas: Dell.com/Endpoint-Security

Obserwuj nas: LinkedIn @DellTechnologies | X @DellTech

Dell Endpoint Security — informacje

Bezpieczeństwo to trudny temat dla organizacji każdej wielkości. **Zaangażuj doświadczonego partnera w zakresie zabezpieczeń i technologii, aby zmodernizować zabezpieczenia punktów końcowych**.

Dell Trusted Workspace pomaga zabezpieczyć punkty końcowe w nowoczesnym środowisku IT gotowym do modelu „zero trust”. Zmniejsz podatność na ataki i zwiększ cyberodporność dzięki kompleksowej ofercie firmy Dell dotyczącej zabezpieczeń sprzętowych i programowych. Nasze wysoce skoordynowane, oparte na obronie podejście równoważy zagrożenia, łącząc wbudowane zabezpieczenia z ciągłą czujnością. Użytkownicy końcowi mogą działać produktywnie, a dział IT czuć się pewnie dzięki rozwiązaniom zabezpieczającym stworzonym z myślą o współczesnym środowisku chmurowym.