

Usługi AI związane z bezpieczeństwem i odpornością

Zaufaj sztucznej inteligencji

Sprostanie wyzwaniom związanym z wdrażaniem sztucznej inteligencji

Sztuczna inteligencja (AI) to przełom dla firm, umożliwiający wdrażanie rewolucyjnych innowacji i szybsze podejmowanie decyzji. Jednak z wielkim potencjałem wiążą się poważne wyzwania. Wdrożenie sztucznej inteligencji wprowadza wyjątkowe obawy w sferze bezpieczeństwa, zaufania i zgodności z przepisami, co wywiera nową presję na organizacje. W firmie Dell Technologies na nowo zdefiniowaliśmy sposób, w jaki powinny działać zabezpieczenia AI. Nasze podejście w wyjątkowy sposób integruje zarządzanie danymi, bezpieczeństwo infrastruktury i ochronę modelu sztucznej inteligencji, aby zaoferować kompleksowe, dostosowane do potrzeb rozwiązanie. Niezależnie od tego, czy dopiero zaczynasz korzystać ze sztucznej inteligencji, czy skalujesz istniejące rozwiązania, nasze kompleksowe usługi sprawiają, że wdrażanie sztucznej inteligencji jest szybsze, bezpieczniejsze i bardziej niezawodne.

Zapewnienie bezpieczeństwa leży nie tylko w gestii działu IT

Nowoczesne zabezpieczenia AI wymagają współpracy między zespołami. Bezpieczeństwo AI to zadanie zespołowe, wymagające zaangażowania i podejmowania decyzji na wszystkich szczeblach organizacji. Tradycyjne, odizolowane modele operacyjne IT nie są odpowiednie w tym zmieniającym się środowisku. Nasze wyjątkowe podejście obejmuje dane, infrastrukturę, aplikacje i modele w ramach jednej spójnej strategii, która dostosowuje się do konkretnych potrzeb biznesowych, oferując kompleksowe rozwiązanie, które pomoże Ci utrzymać przewagę nad konkurencją.

Rozwiązywanie unikalnych wyzwań związanych z bezpieczeństwem sztucznej inteligencji

Wdrożenie AI wiąże się ze złożonymi kwestiami dotyczącymi bezpieczeństwa i zgodności z przepisami, które mogą przyćmić potencjalne korzyści płynące z wykorzystania tej technologii, takie jak:

- Naruszenia danych i utrata własności intelektualnej (IP) z powodu nieodpowiedniej ochrony danych lub nieautoryzowanego dostępu.
- Zagrożenia oparte na sztucznej inteligencji, takie jak ataki antagonistyczne, manipulowanie modelami czy zatrucie danych szkoleniowych.
- Wyzwania związane z dostępnością najważniejszych obecnie narzędzi AI, takich jak agenci pomocy technicznej, które muszą być stale sprawne.
- Luki w zabezpieczeniach podmiotów zewnętrznych w łańcuchu dostaw wynikające z wzajemnie połączonych systemów.
- Rozszerzanie obszaru ataków w miarę skalowania aplikacji AI w środowiskach hybrydowych i wielochmurowych.
- Chociaż nie jest to wyłącznie kwestia bezpieczeństwa, halucynacje mogą wprowadzać użytkowników w błąd

Podstawowe korzyści

Większe zaufanie i przejrzystość:

Ochrona danych, własności intelektualnej i integralności AI w celu utrzymania zaufania wśród interesariuszy.

Odporność operacyjna: Zadbaj o to, aby systemy AI o znaczeniu krytycznym były zawsze sprawne i odporne na zagrożenia.

Zgodność z przepisami: Pomóż spełnić wymagania branżowe i państwowe, aby uniknąć kosztownych kar i szkód wizerunkowych.

Skalowalne rozwiązania: Wdrażaj elastyczne zabezpieczenia oparte na sztucznej inteligencji, które rosną wraz z Twoją organizacją i jej stosem technologicznym.

Wsparcie i wskazówki ekspertów: Współpracuj ze sprawdzonymi ekspertami ds. bezpieczeństwa, aby dostosować rozwiązanie i zapewnić wymierne wyniki.

Kompleksowe usługi zapewniające dostosowaną do potrzeb architekturę zabezpieczeń

Nasza architektura zabezpieczeń opracowana przez firmę Dell została zaprojektowana z myślą o Twoich unikalnych potrzebach i stanowi elastyczny oraz niezawodny fundament. Bezproblemowo integruje się z Dell AI Factory, aktywuje zasady modelu „zero trust” i wykorzystuje specjalistycznie zintegrowane technologie partnerskie, aby stymulować bezpieczne, przyszłościowe innowacje.



Modele i aplikacje AI



Dane



Infrastruktura

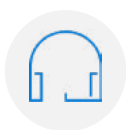
	Cechy i funkcje
Doradztwo Dopasuj zabezpieczenia AI do potrzeb organizacyjnych i wymagań dotyczących zgodności z przepisami	• Bezpieczeństwo i odporność dla usług doradczych AI obejmuje warsztaty biznesowe i techniczne pozwalające opracować kompleksową strategię zabezpieczeń i dostępności • Doradca CISO ds. AI zapewnia wirtualnego CISO, który jest ekspertem w dziedzinie AI, przy inauguracji strategii bezpieczeństwa AI. • Bezpieczeństwo danych dla AI pomaga zmniejszyć zagrożenia i ryzyko związane z bezpieczeństwem danych.
Implementacja Projektowanie i wdrażanie oprogramowania zabezpieczającego w celu zwiększenia widoczności stosu AI	• Projektowanie i konfigurowanie oprogramowania zabezpieczającego w celu zintegrowania narzędzi, które chronią zarządzanie dostępem, aplikacje i sieci
Obsługa Zapewnij szczegółowy wgląd w stos, aby szybko wykrywać zagrożenia i reagować na nie	• Zarządzanie wykrywaniem i reagowaniem (MDR) do wykrywania zagrożeń w trybie 24/7 w danych, infrastrukturze, aplikacjach i modelach • Zarządzana zaporą AI wprowadza odizolowany zestaw zabezpieczeń opartych na AI oraz sprawdza polecenia i dane wyjściowe pod kątem zgodności z zasadami • Testy penetracyjne dla AI w celu symulowania ataków antagonistycznych i wykrywania słabych punktów • Usługi reagowania na incydenty i odzyskiwanie danych pomagają szybko odzyskać sprawność i wrócić do działalności przy minimalnych zakłóceniach

Zbuduj bezpieczną przyszłość ze sztuczną inteligencją bez obaw

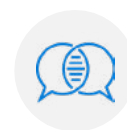
Usługi Dell AI związane z bezpieczeństwem i odpornością są zaprojektowane tak, aby eliminować nowe zagrożenia związane z integracją AI w Twojej organizacji. Nasze usługi zostały opracowane tak, aby współpracowały z zespołami w Twojej firmie już od momentu wdrożenia AI. Dają one dostęp do specjalistycznej wiedzy, która pomoże Ci przeprowadzić strategiczne planowanie, wdrożenie rozwiązania i korzystanie z zarządzanych usług zabezpieczeń, zmniejszając obciążenie operacyjne i pozwalając Ci bezpiecznie wprowadzać innowacje przy pomocy AI.



Poznaj usługi firmy Dell z zakresu [bezpieczeństwa i odporności](#)



[Skontaktuj się](#) z ekspertem Dell Technologies



Dołącz do rozmowy, stosując hasztag #DellTechnologies