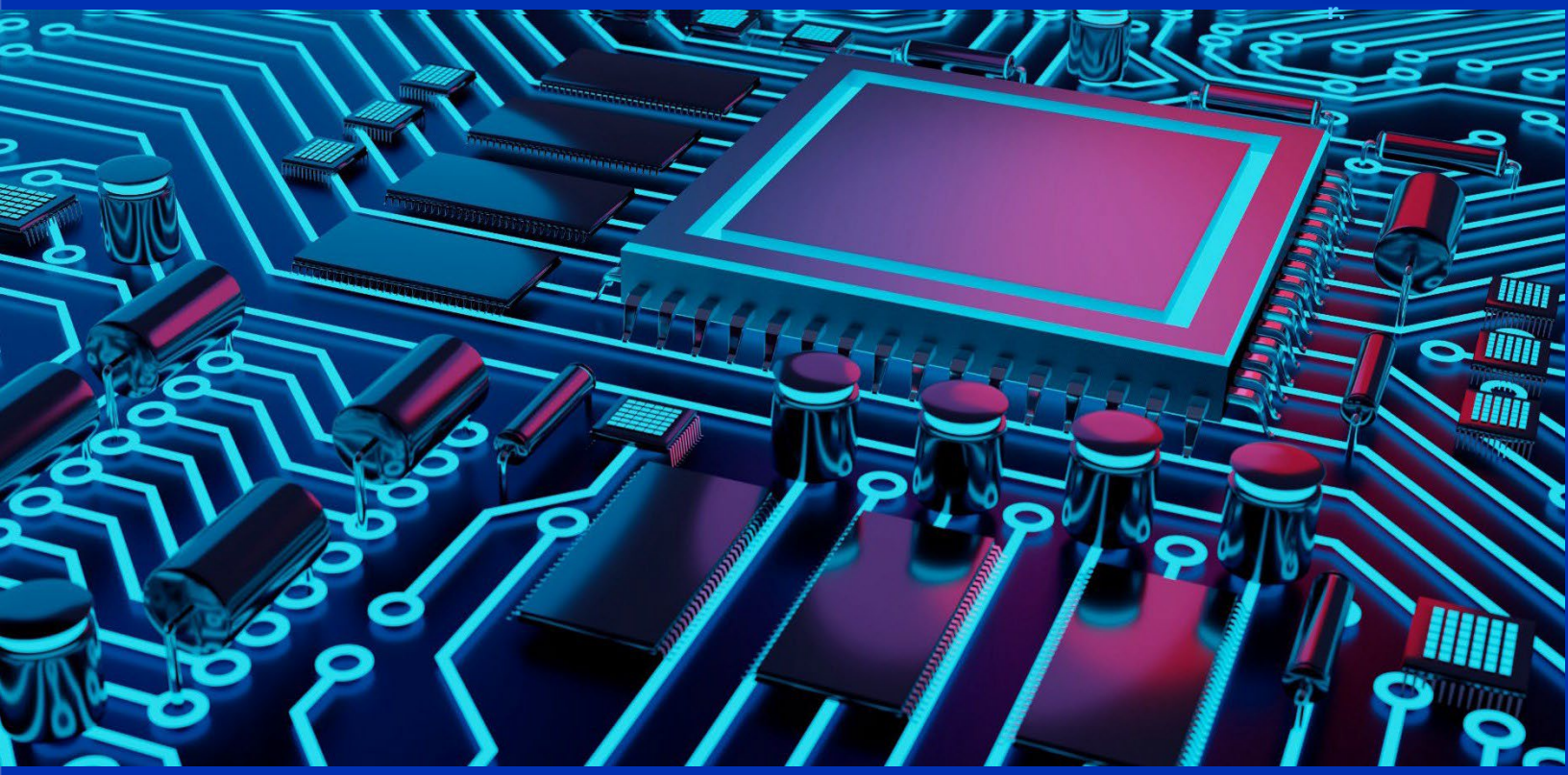
DELL Technologies intel

Jak wdrożyć kompleksowe zabezpieczenia sprzętowe i programowe

Najbezpieczniejsze na świecie komercyjne komputery AI PC* dostarczane przez firmy Dell i Intel®. Przygotuj swoją flotę na przyszłość i wyprzedzaj cyberprzeciwników dzięki wielu warstwom obrony.

lipiec 2025



Streszczenie dla zarządu

- Zapewnienie bezpieczeństwa danych biznesowych jest wyzwaniem, komplikowanym przez rozprzestrzenianie się punktów końcowych działających poza siecią organizacyjną i ciągłą ewolucję wektorów zagrożeń.
- Sztuczna inteligencja pojawiła się na urządzeniach, zwiększając innowacyjność, a także powierzchnię ataku. Wobec stosowania obecnie setek modeli i funkcji sztucznej inteligencji wrażliwe dane są teraz zagrożone ekspozycją na aplikacje, takie jak generatywna sztuczna inteligencja.
- Firmy Dell i Intel dokładają wszelkich starań, aby zapewnić bezpieczeństwo komercyjnych sieci klientów dzięki wielu warstwom ochrony.
- Firma Dell łączy wbudowane zabezpieczenia w sprzęcie i oprogramowaniu wewnętrznym z zabezpieczeniami firmy Intel na poziomie układów scalonych, aby chronić najgłębsze poziomy urządzenia przed podstawowymi atakami.
- Wzmacniamy te zabezpieczenia „poniżej poziomu systemu operacyjnego" dzięki inteligentnemu oprogramowaniu z naszego ekosystemu partnerskiego na potrzeby zaawansowanej ochrony przed zagrożeniami.
- Oprócz tego podejścia firmy Dell i Intel zainwestowały w praktyki i zasady, które mają na celu ciągłe zwiększanie bezpieczeństwa platform po ich wprowadzeniu na rynek i narażeniu na ataki ze strony złośliwych podmiotów.

Tematy omówione w tym dokumencie

Fundament bezpieczeństwa

Bezpieczny cykl rozwoju Firmy Dell i Intel projektują swoje produkty z zabezpieczeniami jako podstawowymi elementami i rygorystycznie testują je przed wydaniem.

Zabezpieczenia łańcucha dostaw Zabezpieczenia są stosowane w całym łańcuchu dostaw, aby zapewnić bezpieczeństwo urządzeń po opuszczeniu fabryki.

Kompleksowe ramy obronne

Wbudowane zabezpieczenia Rygorystyczne mechanizmy kontroli łańcucha dostaw i opcjonalna gwarancja zapewniają klientom bezpieczeństwo od pierwszego uruchomienia.

Wbudowane zabezpieczenia:

- Funkcje zabezpieczeń oparte na sprzęcie i oprogramowaniu wewnętrznym pomagają chronić urządzenia przed zagrożeniami, które atakują ich podstawowe warstwy, np. system BIOS.
- Zabezpieczenia oparte na krzemie zapewniają podstawową warstwę, która stanowi podstawę niezawodności i wiarygodności komputera ze sztuczną inteligencją.

Wbudowane zabezpieczenia: zabezpieczenia oparte na oprogramowaniu zapewniają zaawansowaną ochronę punktów końcowych, sieci i środowisk chmurowych, co ma kluczowe znaczenie dla nowoczesnego bezpieczeństwa urządzeń.

Stała pomoc techniczna: firmy Dell i Intel pracują nad tym, aby nasze produkty były bezpieczne, naprawiają luki w zabezpieczeniach i aktualizują zabezpieczenia na poziomie układów scalonych w systemie operacyjnym.

Najważniejsze trendy w zakresie bezpieczeństwa

1. W raporcie Endpoint Security Market Insights, firmy Forrester Research, Inc. z marca 2025 r. wyjaśniono, że „punkty końcowe (…) należą do czołowych celów zewnętrznych ataków na firmy, które doświadczyły naruszenia w ciągu ostatnich 12 miesięcy".

2. Według raportu Global Threat Report firmy CrowdStrike za rok 2025 bezplikowe ataki złośliwego oprogramowania stanowią obecnie 79% ataków — oznacza to ataki na pamięć, które są trudniejsze do wykrycia.

3. Według raportu z badania Enterprise Strategy Group z maja 2023 r. ponad 75% organizacji zgłasza, że doświadczyło co najmniej jednego cyberataku spowodowanego przez nieznane, niezarządzane lub źle zarządzane urządzenie końcowe.

Wprowadzenie

Sieć jest tak bezpieczna, jak najsłabszy punkt końcowy

Bezpieczeństwo zaczyna się dużo wcześniej, niż mogłoby się wydawać. Wydaje się, że co kilka miesięcy inna znana globalna marka doświadcza poważnego naruszenia bezpieczeństwa, a negatywna reakcja opinii publicznej powoduje poważne szkody dla jej wizerunku. To wystarczy, aby właściciele firm i specjaliści ds. bezpieczeństwa martwili się, że są również narażeni — czy to ze strony przeoczonej luki w zabezpieczeniach urządzeń, czy nieznanego, możliwego do wykorzystania słabego punktu w ich oprogramowaniu. Możesz być w stanie zaufać swojemu zespołowi IT w zakresie zabezpieczania sieci i wdrażania bezpiecznych praktyk w zakresie danych, ale jak możesz zaufać wszystkim punktom końcowym i aplikacjom, na których polegasz, aby prowadzić działalność, gdy nie masz nadzoru nad ich produkcją lub rozwojem?

Zabezpieczenia programowe to za mało. Częstym, ale wadliwym podejściem do rozwiązywania problemów z integralnością urządzeń jest próba stworzenia fałszywego poczucia bezpieczeństwa za pomocą rozwiązań opartych wyłącznie na oprogramowaniu bez eliminowania podstawowych luk sprzętowych. Ważne jest, aby liderzy biznesowi rozumieli ograniczenia tej strategii: polegając wyłącznie na oprogramowaniu do ochrony swojej firmy, pozostawiają sprzęt, na którym działa oprogramowanie, potencjalnie narażony na ataki. Zasadniczo, jeśli sprzęt nie jest bezpieczny, aplikacje i technologie zabezpieczeń działające na nim nie mogą być bezpieczne.

Inni dostawcy próbują stworzyć „ogrodzony ogród" w celu ochrony urządzeń, gdzie ograniczenia są wbudowane w aplikacje i usługi, które ograniczają elastyczność użytkownika. Chociaż może to mieć sens w kontekście konsumenckim, wiąże się to z kosztem swobody pełnego wykorzystania urządzeń, co jest wyzwaniem, które tylko nasila się w kontekście komercyjnym. Taki sposób działania może również skłonić atakujących do coraz większego skupienia się na tych systemach i ich łamania w celu ujawnienia słabych punktów w typowych konfiguracjach.

Mówiąc najprościej, to, co działa w przypadku urządzeń bezpośrednio dla konsumentów, często kończy się niepowodzeniem w przypadku zastosowania w środowisku komercyjnym, które stanowi bardziej atrakcyjny cel dla atakujących. Dlatego firmy Dell i Intel przyjmują inne, holistyczne podejście do zabezpieczeń. Firmy Dell i Intel wiedzą, że jedynym sposobem niezawodnego zabezpieczenia komercyjnych urządzeń i sieci jest harmonizacja działających wspólnie technologii zabezpieczeń sprzętu i oprogramowania. Podczas gdy nasze zespoły współpracowały ze sobą w celu stworzenia tarczy ochronnej ze ściśle zintegrowanych funkcji zabezpieczeń sprzętu i oprogramowania, inni dostawcy mogli nie dokonać tej inwestycji.

Zabezpieczenia sprzętowe dla komercyjnego komputera ze sztuczną inteligencją

Każdy komputer będzie komputerem AI PC. Analityk rynku technologicznego Canalys przewiduje, że w ciągu najbliższych sześciu lat komputery z sztuczną inteligencją zdominują cały rynek. Oznacza to, że komputery bez wbudowanej funkcji sztucznej inteligencji nie będą już sprzedawane do 2030 roku. Zasadniczo, aby zabezpieczyć swoją firmę na przyszłość, musisz zacząć już teraz. Dobra wiadomość: firmy Dell i Intel pomagają klientom poruszać się po zmieniającym się krajobrazie IT i zabezpieczeń dzięki komercyjnym komputerom AI PC posiadającymi podstawowe wbudowane zabezpieczenia, szybkość i wydajność potrzebną do zwalczania nowoczesnych zagrożeń.

Nie jest to jednak łatwe zadanie. Złożoność i obawy związane z zabezpieczaniem urządzeń i sieci są tak duże, że mogą przyprawić o zawrót głowy — a nowe technologie sztucznej inteligencji jeszcze bardziej skomplikowały ten obszar. Dlatego naszą misją jest dostarczanie klientom urządzeń zaprojektowanych z myślą o bezpieczeństwie, aby mogli skupić się na tym, co naprawdę ważne — na prowadzeniu działalności. Współpraca firm Dell i Intel w zakresie inżynierii trwa od kilku dekad i zawsze koncentrowała się na zapewnieniu bezpieczeństwa danych naszych klientów, zwłaszcza na rynku B2B. Dzięki współpracy z firmą Intel Dell zyskał reputację dostawcy urządzeń dla pracowników firm każdej wielkości i z każdej branży. Co wchodzi w skład komercyjnego urządzenia AI firmy Dell? To nie tylko zbiór przypadkowych funkcji — firmy Intel i Dell łączą technologie, narzędzia i polityki na każdym etapie cyklu życia komercyjnych komputerów PC, aby zapewnić klientom i ich firmom kompleksowe bezpieczeństwo.

Bezpieczeństwo z założenia

Firmy Intel i Dell wykraczają poza dzisiejsze zagrożenia, projektując systemy przyszłości w taki sposób, aby zminimalizować powierzchnię ataku i zapewnić bezpieczeństwo urządzeń komercyjnych.

Ochrona w transporcie

Wdrożyliśmy technologie i zasady, które pomagają chronić integralność urządzeń, zanim trafią one w Twoje ręce, pomagając utrzymać bezpieczeństwo podczas pozyskiwania, montażu i dostawy komponentów.

Obrona przed zmieniającymi się zagrożeniami

Wykorzystujemy zabezpieczenia sprzętowe oparte na rozwiązaniach Dell Trusted Devices i Intel vPro® Security, aby wzmocnić urządzenia, które zapewniają podstawowe funkcje cyberbezpieczeństwa, takie jak zapobieganie, wykrywanie, reagowanie, odzyskiwanie danych i działania naprawcze. Ponadto firmy Dell i Intel mają zespoły ds. bezpieczeństwa, które zajmują się testowaniem produktów i wykrywaniem nowych luk w zabezpieczeniach, zanim zrobią to osoby atakujące, aby szybko wdrażać poprawki pomagające zapewnić ochronę Tobie i Twojemu zespołowi.

W tym raporcie przedstawimy, w jaki sposób firmy Dell i Intel współpracowały, aby stworzyć komercyjne platformy AI PC, które mają wbudowane zabezpieczenia na najwyższym poziomie, zapewniając ochronę urządzeń w całym cyklu życia, podczas kolejnych aktualizacji i nie tylko.

Cyberbezpieczeństwo i generatywna sztuczna inteligencja — miecz obosieczny

Tak jak cyberobrońcy wykorzystują GenAI dla dobra, cybernapastnicy dążą do realizacji własnych złośliwych celów, przeprowadzając bardziej zaawansowane ataki szybciej i w większej skali.

Chociaż przypadki użycia generatywnej sztucznej inteligencji są wciąż w powijakach i codziennie się rozwijają, ważne jest, aby pamiętać o kilku kluczowych koncepcjach. Po pierwsze, istnieje wiele zagrożeń, które generatywna sztuczna inteligencja może stanowić dla organizacji w tym:

- Problemy z prywatnością i integralnością danych
- Problemy ze zgodnością
- Oraz naruszenia praw własności intelektualnej

Ponadto dostrzegamy wiele możliwości pomocy generatywnej sztucznej inteligencji w walce o bezpieczeństwo, takie jak m.in.:

- Wykrywanie zaawansowanych zagrożeń
- Wyspecjalizowane i skoncentrowane szkolenia dla pracowników oraz
- Automatyzacja

Firmy Dell i Intel aktywnie pracują nad umożliwieniem lepszego modelowania zagrożeń specyficznych dla generatywnej sztucznej inteligencji. Może to obejmować zapobieganie utracie danych, zarządzanie prawami do danych, zaawansowany phishing, manipulowanie modelami, kwestie prawne i zgodność z przepisami — wszystko to przy zastosowaniu odpowiednich środków kontroli.

Firma Dell może również pomóc w przetestowaniu środowiska generatywnej sztucznej inteligencji pod kątem bezpieczeństwa dzięki programom zarządzania lukami w zabezpieczeniach i testowania penetracyjnego, aby dotrzymać kroku zmieniającemu się pejzażowi zagrożeń.

Fundament bezpieczeństwa

Bezpieczny cykl rozwoju

Zabezpieczenie naszych platform zaczyna się od tablicy

Planowanie, ocena i analiza

Przed zaprojektowaniem naszych najnowszych platform i chipsetów eksperci z firm Dell i Intel ustalają ścisłe parametry tego, co bezpieczna platforma musi uwzględnić, aby sprostać przyszłym potrzebom w zakresie bezpieczeństwa i spełnić wymagane przepisy dotyczące bezpieczeństwa. Proces ten rozpoczyna się od określenia możliwych przyszłych zagrożeń bezpieczeństwa i prywatności oraz działań niezbędnych do ich rozwiązania. Ta ocena służy do określenia celów bezpieczeństwa, które będą podstawą do oceny naszych architektur. Dzięki tym informacjom zespoły ds. bezpieczeństwa firm Dell i Intel opracowują modele zagrożeń, przyjmując podejście przeciwstawne względem tej architektury koncepcyjnej, testując pod kątem potencjalnych luk w zabezpieczeniach i zagrożeń, które należy unieszkodliwić. To ćwiczenie wykazało, że zapewnia znaczną poprawę w wykrywaniu i ograniczaniu potencjalnych luk w zabezpieczeniach systemu BIOS, oprogramowania wewnętrznego i konstrukcji sprzętu.

Konstrukcja zorientowana na bezpieczeństwo

Po zakończeniu oceny zagrożeń i utworzeniu modeli w celu zdefiniowania powierzchni zagrożenia i miejsca, w którym powinny być skoncentrowane testy, inżynierowie zaczynają opracowywać kod produktu. Cele w zakresie bezpieczeństwa zdefiniowane na poprzednim etapie stanowią wskazówki na tym etapie rozwoju i służą jako kryteria określania, czy produkt jest na dobrej drodze do zaspokojenia potrzeb naszych klientów.

Weryfikacja i testowanie

Po dopracowaniu kodu do poziomu spełniającego cele bezpieczeństwa określone na początku cyklu rozwoju produkt przechodzi do rygorystycznego procesu testowania. Testy te zwykle zaczynają się od bezpiecznych recenzji kodu i statycznej analizy kodu, zautomatyzowanego procesu, który wykorzystuje specjalne narzędzia do znajdowania i naprawiania usterek. Niektóre produkty z bardziej skomplikowanym kodem wymagają ręcznego procesu przeglądu, w którym eksperci ds. bezpieczeństwa przeprowadzają bezpośrednie przeglądy kodu produktu, aby znaleźć nieznane wcześniej błędy i zapewnić, że został on zaprojektowany w bezpieczny sposób. I wreszcie, zespoły najlepszych hakerów są angażowane w testy penetracyjne i inne działania symulujące szkodliwe zachowania w celu znalezienia potencjalnych luk, które zostały przeoczone we wcześniejszych fazach. Ustalenia te są ponownie łagodzone w oparciu o ryzyko, dzięki czemu wszelkie dodatkowe zidentyfikowane narażenie zostało udokumentowane i skorygowane.

Wydanie i po wydaniu

Po rygorystycznym przetestowaniu produktu i stwierdzeniu, że spełnia lub przekracza cele bezpieczeństwa określone na początku, jest on gotowy do wprowadzenia na rynek. Jednak te fazy stanowią tylko fragment cyklu bezpiecznego rozwoju. Dla firm Dell i Intel utrzymanie bezpieczeństwa ich platform jest ciągłym wysiłkiem. Nasze zespoły pracują nad wykrywaniem luk w zabezpieczeniach, zanim zostaną one wykorzystane przez atakujących, a następnie opracowują i udostępniają aktualizacje zabezpieczeń w celu ich naprawienia. Przykładem zaangażowania firm Dell i Intel w kompleksowe zabezpieczenia jest nasza inwestycja w bezpieczny łańcuch dostaw od montażu do dostawy urządzenia, co jest jednym z najszybciej zyskujących na popularności wektorów ataków wśród osób i podmiotów mających złe intencje. W następnej sekcji omówimy, w jaki sposób firmy Dell i Intel ograniczają ryzyko w ich łańcuchach dostaw, aby zapewnić bezpieczeństwo urządzenia dostarczonego do drzwi od pierwszego uruchomienia.

Zabezpieczenie łańcucha dostaw

Zapewnienie łańcucha dostaw ma fundamentalne znaczenie dla bezpieczeństwa urządzeń

Wiele może się zdarzyć między opuszczeniem fabryki przez element lub urządzenie a dotarciem do miejsca przeznaczenia. Każdy etap łańcucha dostaw stanowi nowy wektor, który otwiera pracowników, firmę i klientów na potencjalny atak. Firmy Dell i Intel opracowały narzędzia, technologie i procesy, które pomagają zapewnić bezpieczeństwo naszych produktów przed dotarciem do firm klientów i umożliwiają samodzielną weryfikację autentyczności urządzeń przed wdrożeniem ich u pracowników.

Źródło
Firma Dell stosuje rygorystyczny proces weryfikacji partnerów, aby zapewnić jakość i bezpieczeństwo urządzeń i ich komponentów. Partnerzy ci regularnie przechodzą audyty w celu zapewnienia zgodności z kompleksowym zestawem standardów bezpieczeństwa łańcucha dostaw firmy Dell.

Tworzenie
Oprócz przestrzegania standardów bezpieczeństwa łańcucha dostaw firmy Dell producenci urządzeń Dell często testują części podczas produkcji, aby upewnić się, że podrobione produkty nie wchodzą w skład łańcucha dostaw. Aby jeszcze bardziej ograniczyć to ryzyko, na określonych elementach wysokiego ryzyka znajdują się etykiety z unikatowym numerem identyfikacyjnym części (PPID), zawierające informacje o dostawcy, numerze części, kraju pochodzenia i dacie produkcji, dzięki czemu Dell może identyfikować, uwierzytelniać, śledzić i ostatecznie weryfikować te elementy, aby upewnić się, że klient otrzyma dokładnie to, co zostało wysłane.

Dostarczenie
Transport firmy Dell jest chroniony warstwami zabezpieczeń fizycznych — od plomb zabezpieczających przed manipulacją i mechanizmów blokowania drzwi po różne urządzenia śledzące zaprojektowane w celu wykrywania, czy urządzenia firmy Dell znajdujące się wewnątrz nie zostały poddane manipulacjom podczas transportu.

Same urządzenia Dell są również wyposażone w technologie wykrywania manipulacji. Rozwiązania Dell SafeSupply Chain obejmują mechanizmy kontroli bezpieczeństwa i integralności łańcucha dostaw, takie jak plomby zabezpieczające przed manipulacją i czyszczenie dysków twardych na poziomie NIST, aby pomoc Ci utrzymać nieskazitelny wizerunek korporacyjny.

Weryfikacja
Urządzenia Dell z wbudowaną sztuczną inteligencją są dostarczane z podpisanymi kryptograficznie certyfikatami platformy, które przechwytują atrybuty platformy podczas produkcji, montażu, testowania i integracji. Te atrybuty platformy są następnie kryptograficznie powiązane z określonym urządzeniem przy użyciu modułu TPM (Trusted Platform Module) jako sprzętowego źródła zaufania.

Dowiedz się więcej o wspólnych wysiłkach firm Dell i Intel w zakresie zabezpieczenia łańcucha dostaw. Obejrzyj wywiad ***z SiliconANGLE***

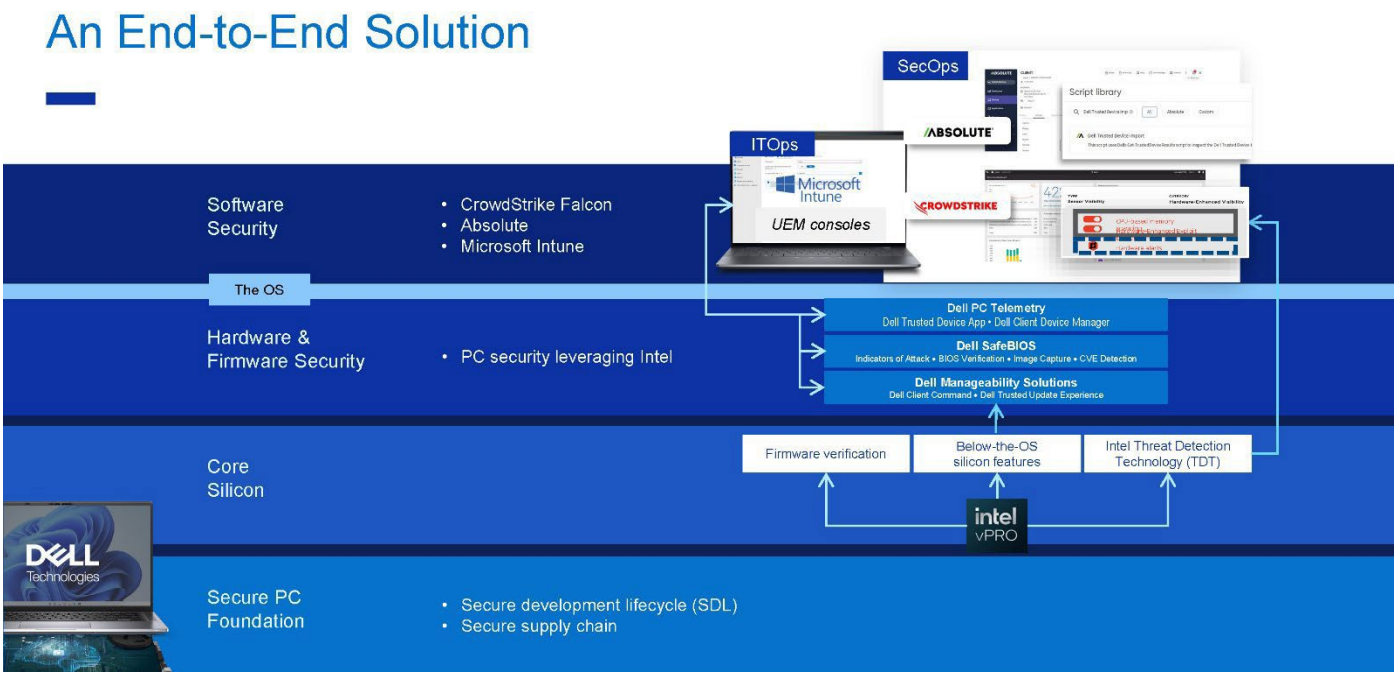
Dell wdrożył certyfikaty platformy Trusted Computing Group (TCG) w ramach rozwiązania Dell Secured Component Verification (SCV) dla komercyjnych komputerów AI PC z procesorami Intel (certyfikat dostępny zarówno na urządzeniu dla organizacji federalnych, jak i w chmurze dla klientów komercyjnych). SCV dostarcza podpisane kryptograficznie certyfikaty inwentaryzacji dla obsługiwanych urządzeń firmy Dell. Dzięki bezpiecznym narzędziom autoweryfikacji unikalne dla firmy Dell rozwiązanie SCV* pomaga zapewnić pełną integralność sprzętu podczas transportu do środowisk IT i umożliwia klientom sprawdzenie, czy komercyjne komputery AI PC i kluczowe komponenty firmy Dell są dostarczane zgodnie z zamówieniem, tak jak zostały wyprodukowane.

Kompleksowe ramy obronne

Ochrona poniżej poziomu systemu operacyjnego

Wbudowane technologie zabezpieczeń pomagają zapobiegać zagrożeniom, wykrywać je, reagować na nie i odzyskiwać dane

Kompleksowe zabezpieczenia oznaczają wyjście poza tradycyjny model oprogramowania chroniącego oprogramowanie, aby dotrzymać kroku nowym kategoriom zagrożeń dla bezpieczeństwa cyfrowego, bezpieczeństwa fizycznego i prywatności. Połączenie ich z technologią zabezpieczeń sprzętowych „poniżej poziomu systemu operacyjnego" pomaga chronić każdą warstwę stosu obliczeniowego, zapobiegając atakom podstawowym i wykrywając je, z uwzględnieniem wariantów zagrożeń, które najczęściej występują w łańcuchu dostaw. Współpraca techniczna firm Dell i Intel koncentrowała się na objęciu tej powierzchni ataku złożoną kombinacją technologii zarówno na poziomie komponentów, jak i platformy.



Rysunek 1: Obecnie skuteczne zabezpieczenia wymagają wielu warstw środków zaradczych. Firmy Dell i Intel współpracują z partnerami w zakresie oprogramowania, aby zapewnić kompleksową ochronę.

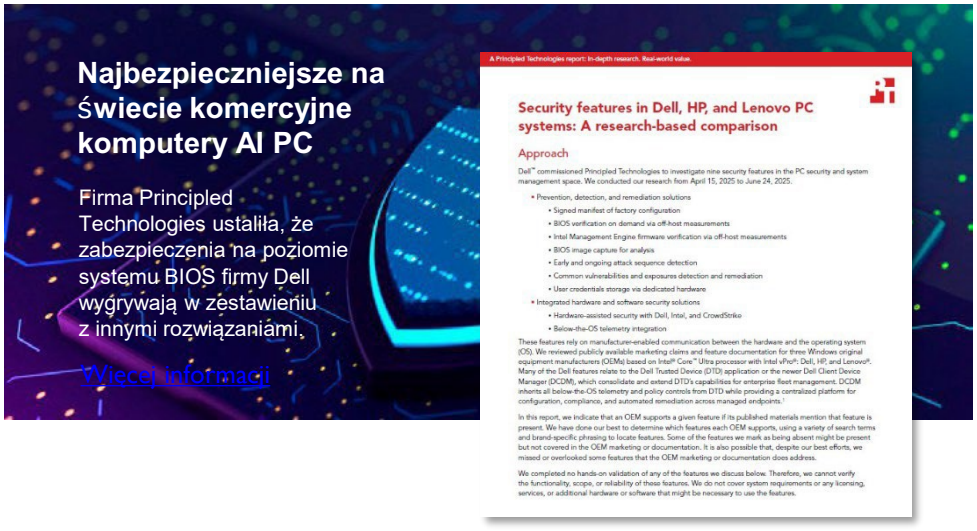
Omówiliśmy łańcuch dostaw i bezpieczną platformę komputerów AI PC, którą oferują firmy Dell i Intel. Przyjrzyjmy się teraz warstwom pośrednim.

Zabezpieczenia Intel vPro®

Rozwiązanie Intel vPro Security jest dołączone do każdego komercyjnego urządzenia firmy Dell działającego na platformie Intel vPro® i zapewnia sprzętowe funkcje zabezpieczeń, które pomagają chronić wszystkie warstwy stosu obliczeniowego. Ten zbiór technologii zabezpieczeń pomaga chronić się przed nowoczesnymi zagrożeniami na każdej warstwie: Sprzętu, systemu BIOS/oprogramowania wewnętrznego, monitora maszyny wirtualnej, maszyn wirtualnych, systemu operacyjnego i aplikacji.

Wbudowane zabezpieczenia Dell w sprzęcie i oprogramowaniu wewnętrznym

Ochrona systemu BIOS (Basic Input Output System) ma kluczowe znaczenie dla bezpieczeństwa urządzenia. Jeśli atakującemu uda się uszkodzić system BIOS urządzenia, będzie mógł uzyskać kontrolę nad całym urządzeniem ze względu na wyjątkową i uprzywilejowaną pozycję systemu BIOS w architekturze urządzenia. Aby chronić tę krytyczną warstwę, komercyjne urządzenia z wbudowaną sztuczną inteligencją firmy Dell są dostarczane z SafeBIOS, pakietem zabezpieczeń warstwowych na poziomie oprogramowania wewnętrznego. Podstawowe funkcje systemu SafeBIOS usprawniają ochronę, wykrywanie i odzyskiwanie danych na poziomie systemu BIOS.



Rysunek 2: Według Principled Technologies, firmy Dell i Intel dostarczają najbezpieczniejsze komercyjne komputery AI PC*.

Ważne jest również, aby pamiętać, że skuteczne zabezpieczenia obejmują wgląd w obecny stan bezpieczeństwa. Firma Dell sprawia, że takie zdarzenia poniżej poziomu systemu operacyjnego z systemu SafeBIOS są widoczne na poziomie systemu operacyjnego, aby administratorzy i użytkownicy końcowi widzieli je i mogli podejmować decyzje za pomocą aplikacji Dell Trusted Device (DTD).
Aplikacja DTD wykrywa, czy system BIOS nie został zmanipulowany, porównując pomiary działającego obrazu systemu BIOS z kopią wzorcową zabezpieczoną w środowisku firmy Dell, co stanowi naszą wyróżniającą się na rynku weryfikację systemu BIOS poza hostem. Ponadto weryfikacja oprogramowania wewnętrznego Intel Management Engine (ME), dostępna wyłącznie na komputerach komercyjnych firmy Dell, chroni przed nieautoryzowanym dostępem do wysoce uprzywilejowanego oprogramowania wewnętrznego i manipulacją nim.

Ta unikatowa dla firmy Dell telemetria komputerowa (dostępna za pośrednictwem programu Dell Client Device Manager (DCDM) w przypadku zarządzanych środowisk IT lub konsoli aplikacji DTD w przypadku środowisk niezarządzanych) jest tajnym składnikiem w równaniu bezpieczeństwa. Taka telemetria umożliwia integrację z konsolami innych firm, takimi jak CrowdStrike i Absolute w zakresie zabezpieczeń oraz Microsoft Intune w zakresie zarządzania (patrz Rysunek 1). W rzeczywistości Dell jest jedynym producentem komputerów PC, który zapewnia integrację i widoczność wykrywania zagrożeń na poziomie oprogramowania układowego za pośrednictwem konsol bezpieczeństwa firm trzecich*.

Dell ogranicza również rosnące ryzyko naruszenia tożsamości i nieautoryzowanego dostępu do wrażliwych obciążeń roboczych. Wybrane urządzenia komercyjne Dell obejmują Dell SafeID z ControlVault 3+, unikatowy chip zabezpieczający z certyfikatem FIPS 140-3 poziomu 3*, który przechowuje poświadczenia użytkowników końcowych, izolując je od systemu operacyjnego, co znacznie zmniejsza podatność na ataki.

Zabezpieczenia poniżej poziomu systemu operacyjnego to tylko jeden z elementów holistycznego podejścia firmy Dell do zabezpieczania urządzeń

Aby w pełni zabezpieczyć komercyjne urządzenia sztucznej inteligencji firmy Dell, firmy Dell i Intel zainwestowały również w weryfikację i nadzorowanie ekosystemu najlepszych w branży rozwiązań w zakresie zabezpieczeń oprogramowania. Funkcje te zapewniają ochronę przed zaawansowanymi zagrożeniami stwarzanymi przez zaawansowanych atakujących, oferując dodatkową warstwę zabezpieczeń w warstwie danych i aplikacji.

Firmy Dell i Intel mogą również wzbogacić technologie oprogramowania o telemetrię komputerową poniżej poziomu systemu operacyjnego, aby usprawnić wykrywanie zagrożeń i reagowanie na nie.

Powyżej poziomu zabezpieczeń systemu operacyjnego

Wbudowane zabezpieczenia programowe zapewniają zaawansowaną ochronę przed zagrożeniami

Biorąc pod uwagę potencjalną opłacalność choćby jednego udanego naruszenia, cyberprzestępcy są bardzo zmotywowani, często podejmując dziesiątki prób na jednym urządzeniu w ciągu całego jego okresu eksploatacji. W porównaniu z flotą organizacji budzi to poważne obawy. Czy możesz ryzykować prześlizgnięcie się ataku? W tym momencie jedno jest pewne: żadne rozwiązanie nie może zablokować 100% ataków. Oznacza to punkty końcowe we flocie, jak również wszystkie sieci i środowiska chmurowe, w których działają.
Inteligentne rozwiązania programowe mogą pomóc w zapobieganiu zagrożeniom, wykrywaniu, reagowaniu na nie i odzyskiwaniu danych z dowolnego miejsca. W tym celu oferta zabezpieczeń punktów końcowych Dell Trusted Workspace obejmuje najlepsze w branży oprogramowanie upraszczające zaopatrzenie i zapewniające liderom biznesowym wszystko, czego potrzebują do ochrony punktów końcowych. Dostępne są następujące możliwości:

- Zapobieganie, wykrywanie, reagowanie i działania naprawcze w środowiskach punktów końcowych, sieci i chmury, wykorzystując sztuczną inteligencję i uczenie maszynowe
- Geolokalizacja punktów końcowych, geofencing, zdalne wymazywanie danych, a także autonaprawa aplikacji o znaczeniu krytycznym w sieci lub poza nią
- Rozwiązania Security Service Edge dla zorientowanego na dane podejścia do bezpieczeństwa i dostępu w chmurze, chroniącego dane i użytkowników w każdym miejscu

Funkcje zabezpieczeń firmy Intel, zintegrowane głęboko w układzie scalonym, takie jak Intel Control-flow Enforcement Technology., chronią przed atakami wymierzonymi w system operacyjny, podczas gdy inne funkcje w technologii Intel vPro® Security pomagają chronić system poniżej poziomu systemu operacyjnego, zabezpieczają aplikacje i dane oraz zapewniają zaawansowaną ochronę przed zagrożeniami.

Zabezpieczenia wspomagane sprzętowo

Zintegrowane zabezpieczenia

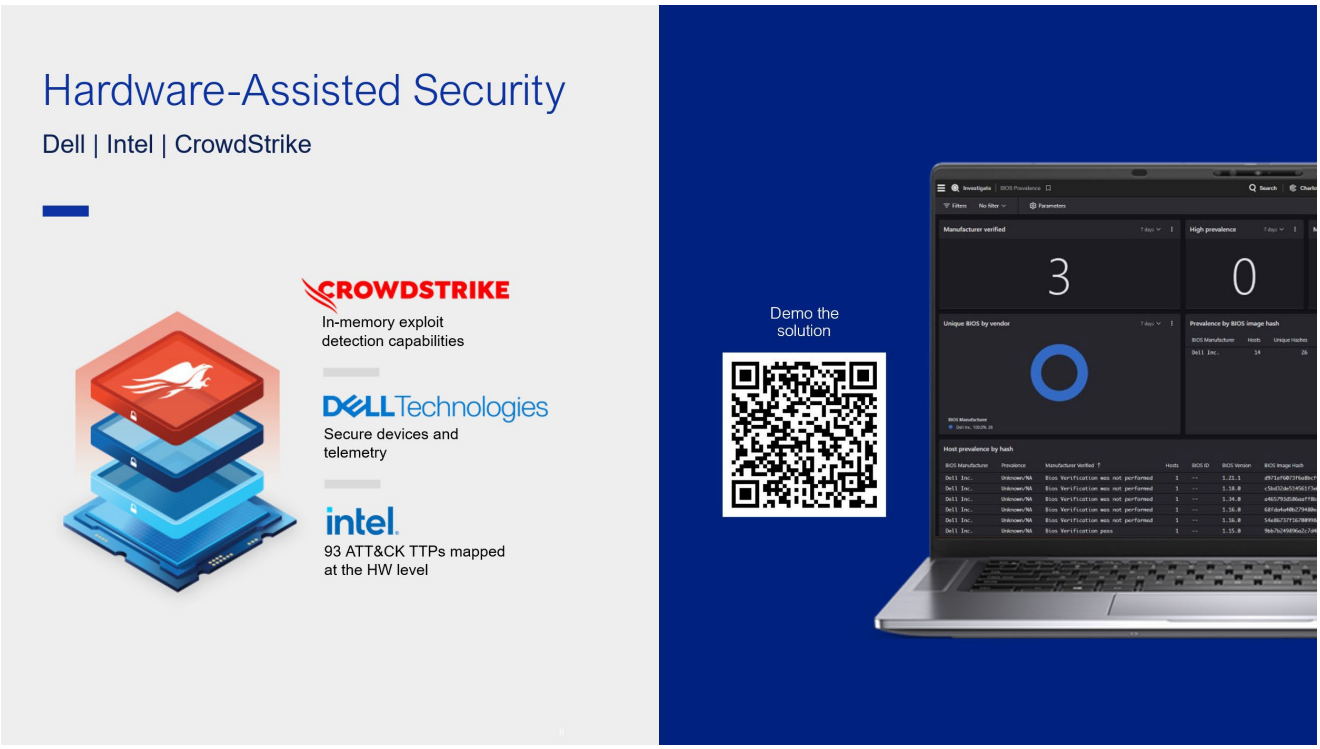
Atakujący coraz częściej skupiają się na całym łańcuchu obliczeniowym organizacji, który tradycyjnie nie był odpowiednio monitorowany i kontrolowany. Te ewoluujące zagrożenia omijają tradycyjne narzędzia bezpieczeństwa oprogramowania do wykrywania i reagowania na punkty końcowe (EDR), dlatego bezpieczeństwo komputerów jest tak ważne. Aby wyprzedzać o krok nowoczesne, szybko rozwijające się zagrożenia, potrzebna jest dogłębna współpraca w obrębie całego ekosystemu w celu odpowiedniego połączenia zabezpieczeń powierzchni ataku od różnych dostawców w spójne rozwiązanie.

Jednak integracja zaplecza jest złożona i czasochłonna, a także wymaga znacznych zasobów. Aby pomóc w rozwiązaniu tego problemu, firmy Dell i Intel wykorzystały nasze dogłębne zrozumienie problemów przeciwników i klientów, aby wspólnie z partnerami opracować zintegrowane rozwiązanie sprzętowe i programowe o nazwie „Hardware-Assisted Security". Dell nie tylko dostarcza bezpieczne komputery AI PC i pozyskuje czołowych partnerów w zakresie oprogramowania — nasza unikalna telemetria urządzeń* wzbogaca cały ekosystem zabezpieczeń, zapewniając flocie większą widoczność na poziomie systemu BIOS. Ta funkcja integracji ma kluczowe znaczenie dla wyeliminowania luki w zabezpieczeniach IT, z którą obecnie boryka się wiele organizacji. Dzięki współpracy firm Dell, Intel i naszego ekosystemu partnerskiego sprzęt i oprogramowanie komunikują się ze sobą, co poprawia bezpieczeństwo całej floty i ułatwia zarządzanie.

Rysunek 3. Ewoluujące cyberzagrożenia omijają zabezpieczenia oparte wyłącznie na oprogramowaniu. Pomóż zmniejszyć powierzchnię ataku punktów końcowych za pomocą zabezpieczeń wspomaganych sprzętowo.

Poznaj zabezpieczenia wspomagane sprzętowo dzięki firmom Dell, Intel i CrowdStrike

Firmy Dell, Intel i CrowdStrike wspólnie opracowały funkcje wykrywania zagrożeń i reagowania na nie, które łączą zalety urządzeń Dell Trusted Device, najbezpieczniejszych na świecie komercyjnych komputerów AI PC*, z możliwościami układów scalonych firmy Intel i rozwiązaniami firmy CrowdStrike umieszczonymi w Gartner Magic Quadrant 2024. Współpracując ze sobą, firmy CrowdStrike, Dell i Intel stworzyły wielowarstwowe rozwiązanie, które na nowo definiuje bezpieczeństwo punktów końcowych w Twojej firmie, wykraczając poza ochronę oprogramowania i obejmując zabezpieczenia sprzętowe.



Rysunek 4. Wielowarstwowe zabezpieczenia komercyjnych komputerów AI PC firmy Dell, zintegrowane z rozwiązaniami CrowdStrike i Intel.

Dodatkowa wartość integracji rozwiązań Intel i CrowdStrike na komputerach AI PC firmy Dell

Zwiększanie bezpieczeństwa punktów końcowych dzięki sztucznej inteligencji i akceleracji GPU/NPU: cyberzagrożenia stają się coraz bardziej zaawansowane, a komputery AI PC pozostają o krok przed nimi dzięki wykorzystaniu sztucznej inteligencji na urządzeniu w celu szybszego wykrywania zagrożeń w czasie rzeczywistym przy jednoczesnym zmniejszeniu zależności od usług w chmurze. Narzędzia takie jak CrowdStrike mogą przesyłać wykrywanie złośliwego oprogramowania do wbudowanych procesorów neuronowych (NPU), szybciej wykrywając zagrożenia przy minimalnym wpływie na wydajność procesora. Dzięki lokalnemu przetwarzaniu danych i zaawansowanym funkcjom ochrony przed phishingiem na komputerach AI PC opartych na technologii firmy Intel poufne informacje pozostają bezpieczne, zmniejszając ekspozycję na ryzyko zewnętrzne.

Oto kilka przykładów prac firm Intel i CrowdStrike (obecnie w fazie weryfikacji koncepcji, ale dostępnych publicznie w nadchodzących miesiącach) w celu zwiększenia bezpieczeństwa punktów końcowych dzięki akceleracji sztucznej inteligencji i NPU:

- Hardware Enhanced Exploit Detection (HEED): wykorzystuje telemetrię procesorów Intel do śledzenia przepływu sterowania w aplikacjach w celu identyfikacji ataków na pamięć.
- Accelerated Memory Scanning (AMS): wykorzystuje technologię Intel Threat Detection w celu przeniesienia intensywnie wykorzystującego moc obliczeniową skanowania pamięci do zintegrowanej karty graficznej Intel, aby umożliwić nawet 7-krotne przyspieszenie skanowania pamięci.

Dzięki tym dwóm funkcjom firma Intel odgrywa kluczową rolę w zasilaniu danymi opartych na sztucznej inteligencji wskaźników możliwości ataku CrowdStrike obecnych w punkcie końcowym i w chmurze zabezpieczeń CrowdStrike. Te możliwości zapewniają również nowy wgląd w warstwę pamięci, dzięki czemu CrowdStrike może w przyszłości wprowadzać nowe modele wykrywania skanów, poprawiając bezpieczeństwo w czasie.

Sprawdzona w branży ochrona bezpieczeństwa komputerów AI PC: nowe badanie przeprowadzone przez firmę MITRE pokazuje, że wybór sprzętu komputerowego odgrywa kluczową rolę w zapewnieniu oprogramowania zabezpieczającego i funkcji systemu operacyjnego do skutecznej ochrony zasobów.

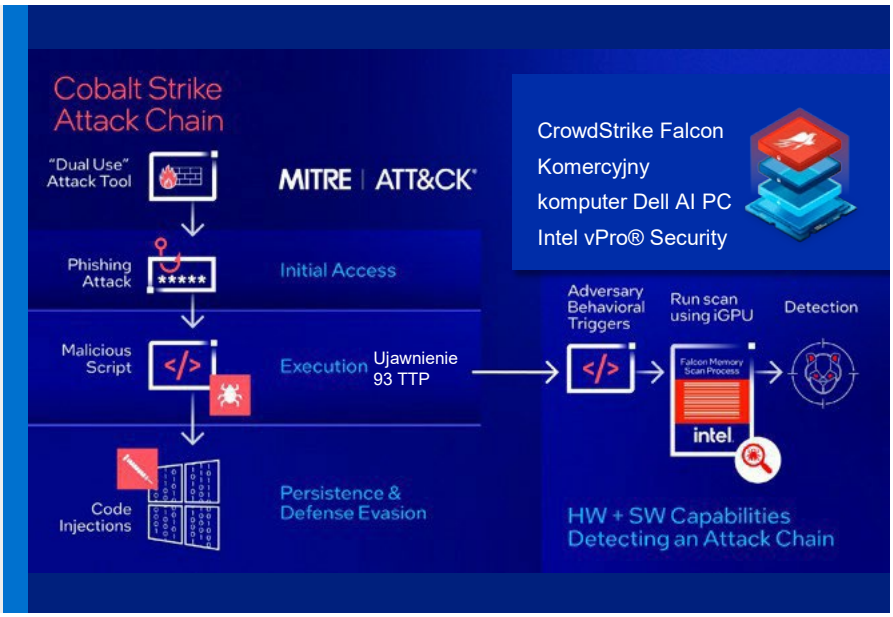
Zespoły ds. operacji bezpieczeństwa (SecOps) wdrażają zaawansowane agenty we wszystkich flotach komputerów końcowych, aby sprawdzić każdy proces pod kątem oznak złośliwego oprogramowania. Dostawcy oprogramowania zabezpieczającego zmapowali swoje możliwości do struktury MITER ATT&CK, aby pokazać, gdzie zapewniają rozwiązania. Dostawcy zarządzanych zabezpieczeń pomagają przedsiębiorstwom w selekcjonowaniu codziennych alertów w narzędziach bezpieczeństwa XDR, SIEM i Copilot. Całkiem wyrafinowane, ale zastosowanie zabezpieczeń sprzętowych w komputerach, które już masz, do prawdziwych ataków pozostawało tajemnicą... aż do teraz.

Pod koniec 2024 roku firma MITRE Center for Informed Defense* (CTID), we współpracy z ponad trzydziestoma ekspertami z firm Intel, Microsoft, CrowdStrike i ATTACK IQ opracowało mapę i ranking znaczenia funkcji oprogramowania zabezpieczającego zoptymalizowanego pod kątem sprzętu w odniesieniu do taktyk i (pod)technik zawartych w ramach MITRE ATTACK. Wspólniegrupa przyporządkowała funkcje zabezpieczeń Intel vPro® do 150 skumulowanych i unikatowych taktyk, (pod)technik i procedur zagrożeń (TTP), przed którymi sprzęt komputerowy zapewnia gotową ochronę dzięki zoptymalizowanemu oprogramowaniu zabezpieczającemu.

Do weryfikacji mapowania i testów emulacji firma MITRE wykorzystała system Dell Pro z procesorem Intel Core Ultra (wraz z pełnym zestawem zabezpieczeń Intel vPro włączonych w typowym pakiecie oprogramowania zabezpieczającego klasy korporacyjnej), który wzbogaca unikatowe, wbudowane zabezpieczenia Dell poniżej poziomu systemu operacyjnego.

Zweryfikowana przez branżę ochrona

komercyjnych komputerów PC AI Dell i Intel z obsługą sztucznej inteligencji



Rysunek 5. Zabezpieczenia wspomagane sprzętowo działają.

W przykładowym scenariuszu (scenariusz łańcucha ataków Cobalt Strike) przedstawiamy bezplikowy atak Cobalt Strike na pamięć i sposób, w jaki CrowdStrike Falcon pomaga w jego unieszkodliwieniu z wykorzystaniem sprzętu. Jak wspomniano wcześniej, bezplikowe ataki złośliwego oprogramowania stały się popularne wśród przestępców. Prawie 75% wszystkich typów ataków nadużywa prawidłowych procesów systemowych, takich jak wykonywanie w pamięci, gdzie mogą uniknąć tradycyjnych zabezpieczeń EDR. Jest to doskonała ilustracja sytuacji, w której sprzęt komputera zapewnia przyrostową moc obliczeniową do skanowania pamięci bez zakłócania pracy użytkownika. **W przypadku firmy CrowdStrike, która wykorzystuje algorytmy przyspieszonego skanowania pamięci w technologii Intel Threat Detection Technology (Intel TDT) i jej zdolność do przenoszenia przetwarzania do zintegrowanego procesora graficznego Intel Graphics Technology, zapewnia to nawet 7-krotne przyspieszenie działania, co pomaga zapewnić dobre doświadczenia użytkownika, a jednocześnie możliwość głębszego skanowania i wykrywania ponad 93 TTP.** (Uwaga: funkcja skanowania pamięci CrowdStrike, wbudowana w oprogramowanie tej firmy, działa tylko na komputerach z procesorem Intel vPro).

Zrozumienie zarówno zabezpieczeń opartych na oprogramowaniu, jak i sprzęcie może pomóc przedsiębiorstwom w pełni wykorzystać potencjał nowoczesnych komputerów AI PC. Wyniki pokazują, że wybór sprzętu komputerowego ma znaczny wpływ na zdolność oprogramowania zabezpieczającego i funkcji systemu operacyjnego do przeciwdziałania określonym zagrożeniom i ochrony zasobów firmowych przed zaawansowanymi cyberatakami.

Struktury zabezpieczeń firm Dell i Intel, zarówno poniżej, jak powyżej poziomu systemu operacyjnego, oferują kompleksowe podejście do ochrony urządzeń komercyjnych, ale jako eksperci w dziedzinie bezpieczeństwa wiemy, że żadne urządzenie nie jest całkowicie bezpieczne. Dlatego jesteśmy liderami branży w zakresie inwestycji w bezpieczeństwo po wprowadzeniu produktu na rynek, aby zapewnić bezpieczeństwo naszych urządzeń przez wiele lat po ich wprowadzeniu.

Bieżące wsparcie

Firmy Dell i Intel inwestują w ciągłe bezpieczeństwo swoich platform po wprowadzeniu produktu na rynek

Firmy Dell i Intel poczyniły znaczne i trwałe inwestycje, aby zapewnić bezpieczeństwo w całym cyklu życia produktu. Po wprowadzeniu urządzenia lub platformy na rynek zespoły Dell i Intel nadal aktywnie badają swoje produkty pod kątem luk w zabezpieczeniach. W przypadku firmy Intel proces ten obejmuje współpracę z naukowcami i uniwersytetami w celu znalezienia możliwych ataków, zanim zrobią to złośliwe podmioty, szybkiego naprawienia wszelkich wykrytych luk w zabezpieczeniach, a następnie zgłaszania ich po zamknięciu luki w zabezpieczeniach.

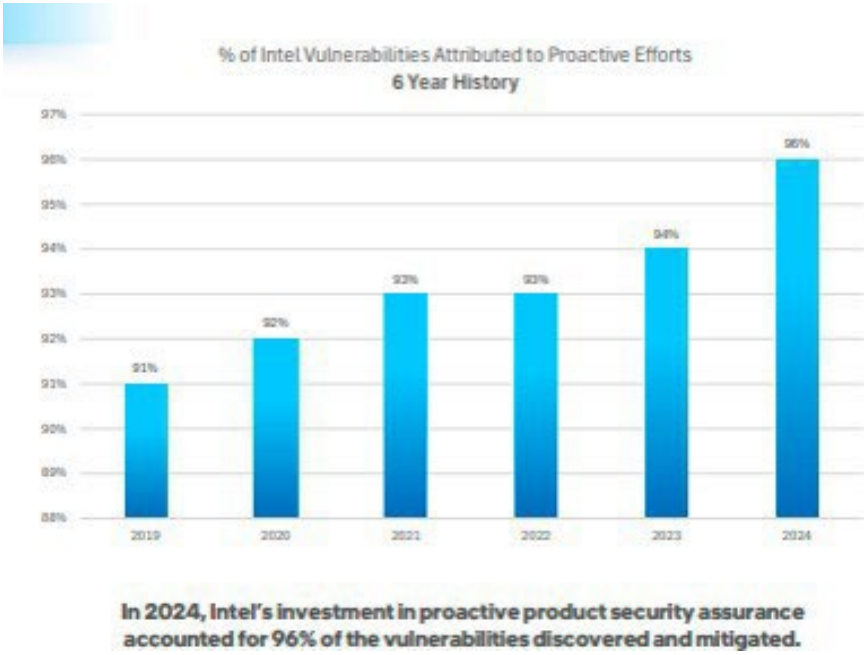
Proaktywne zapewnienie bezpieczeństwa produktów obejmuje wysiłki mające na celu wyszukiwanie luk w zabezpieczeniach podejmowane zarówno wewnętrznie, jak i poprzez zachęcanie zewnętrznej społeczności badania bezpieczeństwa za pośrednictwem programów Bug Bounty. W 2024 r. inwestycje firmy Intel w proaktywne zapewnienie bezpieczeństwa produktów stanowiły 96% wszystkich wykrytych i wyeliminowanych luk w zabezpieczeniach. Pozostałe 4% luk usuniętych przez firmę Intel nie zostało zgłoszonych w ramach programu Intel Bug Bounty lub zostało zgłoszonych przez partnerów lub inne organizacje, które nie zabiegają o nagrody finansowe. W każdym przypadku Intel współpracował z badaczami, aby skoordynować publiczne ujawnienie tych problemów, co oznacza, że środki zaradcze były dostępne dla klientów w dniu publicznego ujawnienia.

Aby wyeliminować typowe luki w zabezpieczeniach i zagrożenia (CVE) wykryte w ramach szeroko zakrojonych programów, Intel regularnie udostępnia aktualizacje platformy Intel Platform Updates dla wszystkich systemów działających na jej produktach. Ten proces kwartalny obejmuje aktualizacje mikrokodu, oprogramowania wewnętrznego i systemu BIOS w zakresie bezpieczeństwa, funkcjonalności i funkcji. Regularne aktualizacje umożliwiają partnerom firmy Intel weryfikację i integrację aktualizacji sprzętu i oprogramowania wewnętrznego z ich platformami w przewidywalnym harmonogramie kwartalnym, co prowadzi do skoordynowanego publicznego ujawniania informacji w całym ekosystemie.

Koordynacją ujawniania informacji o wykrytych lukach w zabezpieczeniach produktów i reagowaniem na nie zajmują się dedykowane zespoły ds. reagowania na incydenty związane z bezpieczeństwem produktów firm Dell i Intel. Wspólnie pracują nad tym, aby CVE były szybko i bezpiecznie obsługiwane, skutecznie ograniczając wszelkie związane z nimi ryzyko.

Firmy Dell i Intel dokonały tych inwestycji, aby zapewnić naszym klientom stałe wsparcie i odciążyć ich zespoły IT. Zatrudniliśmy naukowców, architektów bezpieczeństwa i analityków cyberprzestępczości, aby pomóc w zapewnieniu bezpieczeństwa Twojej firmy i umożliwić zespołom skupienie się na wyposażeniu pracowników do wykonywania jak najlepszej pracy.

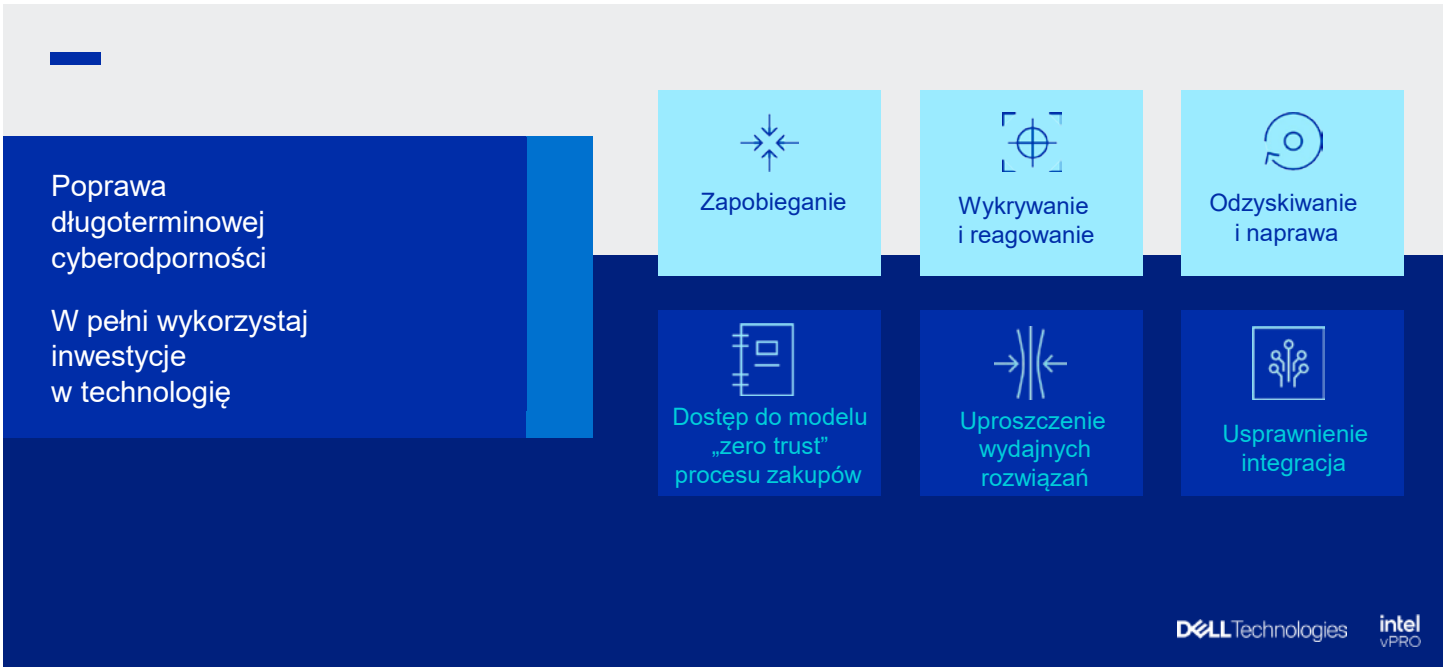
Inwestycje firmy Intel odpowiadają 96% wszystkich luk w zabezpieczeniach usuniętych w 2024 r.



Rysunek 6: Procent luk w zabezpieczeniach firmy Intel przypisanych do działań proaktywnych (źródło: Raport dotyczący bezpieczeństwa produktów firmy Intel z 2024 r.)

Wnioski

Wyniki współpracy z firmami Dell i Intel



Firmy Dell i Intel koncentrują się na wynikach w zakresie bezpieczeństwa i opracowują rozwiązania w oparciu o podejście przeciwników. Głównym celem cyberprzestępców są pieniądze, które zdobywają poprzez kradzież danych, a następnie ich sprzedaż lub przetrzymywanie w celu uzyskania okupu. Chociaż ich metody dostępu różnią się (struktura MITRE ATT&CK® śledzi dziewięć ogólnych metod wstępnego dostępu), łańcuchy działania cyberataków przebiegają w bardzo podobny sposób: rozpoznanie, wstępny dostęp (przez wykorzystanie wykrytej luki w zabezpieczeniach, słabego punktu lub ekspozycji czy znalezionego błędu), infiltracja sieci, rozprzestrzenianie się / uzyskanie bardziej uprzywilejowanego dostępu, węszenie i uczenie się, eksfiltracja danych.

Możemy pomóc Ci zabezpieczyć każde obciążenie robocze dzięki inteligentnym produktom, rozwiązaniom i usługom zaprojektowanym z myślą o przeciwniku. Zamiast próbować blokować 100% ataków (co jest niemożliwe), zakładamy, że atak jest nieunikniony i tworzymy warstwy zabezpieczeń na najgorszy scenariusz. Kładziemy nacisk na widoczność i możliwości działania w całej flocie komputerów stacjonarnych. Pomaga to naszym klientom wyprzedzić nowe wektory ataków.

Dzięki rozwiązaniom firmy Dell i Intel w zakresie bezpieczeństwa punktów końcowych organizacje **osiągają kluczowe wyniki w zakresie bezpieczeństwa**:

- **Poprawa długoterminowej cyberodporności**
- **W pełni wykorzystaj inwestycje w technologię**

Poznaj oba przypadki użycia w cyberbezpieczeństwie:

- **Zmniejszenie powierzchni ataku** — ograniczenie ryzyka prześlizgnięcia się ataku; minimalizacja luk w zabezpieczeniach i punktów dostępu, które mogą zostać wykorzystane w celu naruszenia środowiska.
- **Usprawnij wykrywanie zagrożeń i reagowanie na nie** — aktywnie identyfikuj potencjalne incydenty związane z bezpieczeństwem i złośliwe działania oraz radź sobie z nimi dzięki zintegrowanym warstwom ochrony, które przyspieszają wykrywanie i reagowanie.
- **Zyskaj możliwości odzyskiwania i naprawy** – przechwytuj dane dotyczące naruszeń w celu analizy, aby chronić przed przyszłymi zagrożeniami i przywrócić punkty końcowe do poprzedniego, znanego, bezpiecznego i operacyjnego stanu po incydencie bezpieczeństwa.

…a także zmniejszenie obciążenia operacyjnego związanego z bezpieczeństwem:

- Utrzymuj zaufanie do urządzeń i tożsamości dzięki **ofertom obsługującym model „zero trust”**
- **Uprość zaopatrzenie**, konsolidując dostawców i uzyskując dostęp do sprzętu, oprogramowania i usług pod jednym dachem
- Oszczędzaj czas i zasoby dzięki **usprawnionej integracji**

W walce o cyberbezpieczeństwo zwycięstwo lub porażka zależą od umiejętności gromadzenia, analizowania i reagowania na informacje o zagrożeniach. Współcześni atakujący są innowacyjni. Wiedząc, że większość rozwiązań zabezpieczających działa wyłącznie powyżej poziomu systemu operacyjnego, przestępcy biorą na cel bardziej subtelne powierzchnie ataku: warstwy poniżej poziomu systemu operacyjnego i łańcuch dostaw. Aby być o krok przed takimi przestępcami i chronić swoje firmy, obecni liderzy muszą wykorzystywać wbudowane, sprzętowe technologie zabezpieczeń osadzone głęboko w układach scalonych jako kluczowe przy wdrażaniu urządzeń komercyjnych wśród swoich pracowników.

Zobacz, jakie rozwiązania są dla Ciebie odpowiednie

Komputery komercyjne z obsługą sztucznej inteligencji

ZAPYTAJ O:

Bezpieczeństwo sprzętu i oprogramowania wewnętrznego • Bezpieczeństwo łańcucha dostaw • Łatwość zarządzania • Optymalizacje rdzeni procesorów i sztucznej inteligencji

Oprogramowanie i integracje

ZAPYTAJ O:

Licencje dostępne do zakupu z komputerami firmy Dell • Licencje autonomiczne • Integracje telemetryczne

Dell AI Factory

ZAPYTAJ O:

Zarządzane wykrywanie i reagowanie (MDR) • Odzyskiwanie danych po incydentach

Dzięki światowej klasy zabezpieczeniom łańcucha dostaw, zabezpieczeniom sprzętowym, oprogramowaniu do ochrony przed zaawansowanymi zagrożeniami, usługom zarządzanym i ciągłej pomocy technicznej firmy Dell i Intel są gotowe zaoferować Tobie i Twojej firmie komercyjne urządzenia, które spełniają swoje zadanie i zostały zaprojektowane z myślą o ochronie danych biznesowych przed siecią dark web.

* Najbezpieczniejsze komercyjne komputery AI PC: na podstawie analizy zewnętrznej przeprowadzonej przez firmę Principled Technologies polegającej na porównywaniu komercyjnych komputerów AI PC 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 na temat rozwiązań firmy Dell

Skontaktuj się z ekspertem firmy Dell Technologies

Zobacz więcej zasobów

Dołącz do dyskusji

DELL Technologies

intel