Anatomia zaufanego urządzenia

Poznaj, co czyni komercyjne komputery z obsługą sztucznej inteligencji firmy Dell najbezpieczniejszymi na świecie[1].

KRAJOBRAZ ZAGROŻEŃ I WYZWANIA

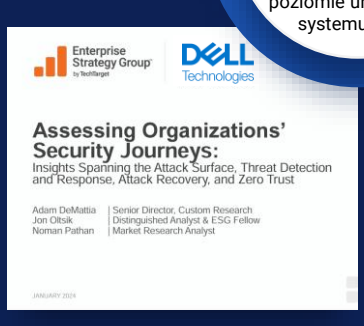
Pojawiające się wektory ataków poniżej systemu operacyjnego stwarzają nowe ryzyko

Urządzenia końcowe są główną bramą dla naruszeń. Ponieważ praca hybrydowa rozszerzyła powierzchnię ataku, w ostatnich latach wzrosły obawy dotyczące bezpieczeństwa na poziomie urządzenia. Atakujący coraz częściej zaczęli atakować łańcuch dostaw, a także rootkity i inne luki w oprogramowaniu układowym, które są w dużej mierze niewykrywalne przez samo starsze oprogramowanie EDR.

Zagrożenia związane z urządzeniami wzrosły 1,5-krotnie od 2020 r.[2]

69%

organizacji zgłasza co najmniej JEDEN atak na poziomie urządzenia/ systemu BIOS[2]



Najważniejsze kryteria oceny przy zakupie nowych komputerów:

- Zautomatyzowane wykrywanie zdarzeń w zakresie systemu BIOS[3]
- Rozwiązywanie problemów z konfiguracjami wysokiego ryzyka[3]

Aby zwalczać współczesne zagrożenia, urządzenia muszą być budowane w bezpieczny sposób i muszą mieć wbudowane zabezpieczenia, które pomogą wychwycić i odeprzeć ataki.

ROZWIĄZANIE

Zapobieganie, wykrywanie, reagowanie i przywracanie działania po podstawowych atakach z najbezpieczniejszymi komercyjnymi komputerami PC na świecie[1]

Flota jest tak bezpieczna, jak jej poszczególne komputery. Co sprawia jednak, że urządzenie jest zaufane i bezpieczne? Widoczność i możliwość działania. Dostęp do większej ilości danych prowadzi do świadomego podejmowania decyzji, pomagając wychwycić nawet najbardziej podstępne pojawiające się zagrożenia. Automatyzacja umożliwia szybsze rozwiązywanie potencjalnych problemów.

Zabezpieczenia sprzętowe i oprogramowanie wewnętrzne komercyjnych komputerów Dell (na platformie Intel lub AMD) zostały zaprojektowane tak, aby zapewnić widoczność i możliwość podejmowania działań we flocie.

Anatomia zaufanego urządzenia Dell

Korzyści

- Bezpieczeństwo od pierwszego uruchomienia dzięki rygorystycznym kontrolom łańcucha dostaw
- Zachowanie integralności systemu BIOS dzięki dogłębnej widoczności na poziomie oprogramowania układowego
- Ochrona tożsamości użytkowników końcowych przed złośliwym oprogramowaniem wykradającym dane uwierzytelniające
- Wzbogać dane na poziomie systemu operacyjnego o telemetrię „poniżej systemu operacyjnego", aby przyspieszyć wykrywanie, reagowanie i naprawianie

Większe bezpieczeństwo dzięki telemetrii PC

Zmniejsz lukę w zabezpieczeniach IT i wzbogać rozwiązania programowe dzięki informacjom 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 →

Utrzymaj integralność systemu BIOS

Wyłapuj i odpieraj zagrożenia dzięki unikalnej weryfikacji systemu BIOS firmy Dell. Oceń uszkodzony BIOS, napraw go i uzyskaj wgląd, który zmniejszy narażenie na przyszłe zagrożenia dzięki funkcji BIOS Image Capture[1].
Dowiedz się więcej →

Wykrywanie zagrożeń

Indicators of Attack — funkcja wczesnego ostrzegania oferowana wyłącznie przez firmę Dell — skanuje w poszukiwaniu zagrożeń opartych na zachowaniu, zanim zdążą one wyrządzić szkody[1].
Dowiedz się więcej →

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. [1]

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.[1]
Dowiedz się więcej →

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.[1]
Dowiedz się więcej →

Bezpieczeństwo w całym cyklu życia komputera

Rygorystyczne, najnowocześniejsze kontrole łańcucha dostaw i opcjonalne dodatki, takie jak unikalna dla firmy Dell bezpieczna weryfikacja komponentów, zapewniają integralność komputera w momencie dostawy i przez cały okres jego użytkowania.[1]
Dowiedz się więcej →

WIODĄCA POZYCJA W BRANŻY

Żaden producent komputerów nie zapewnia takiej widoczności na poziomie systemu BIOS jak Dell[1].

Dowiedz się, co jest potrzebne, aby utrzymać zaufanie do urządzeń w obliczu współczesnych zagrożeń[4].

Więcej informacji →

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

A comparison of security features in Dell, HP, and Lenovo PC systems

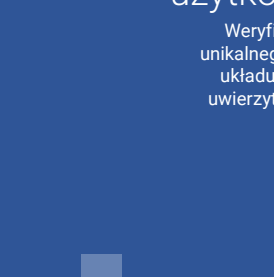
Approach

Dell™ commissioned Principled Technologies to investigate 10 security features in the PC security and system management space:

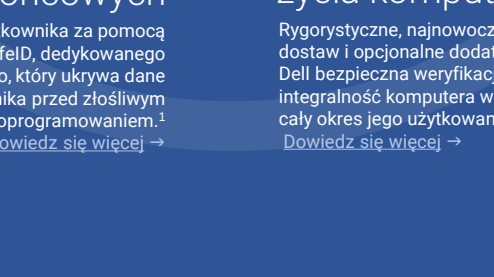
- Support for monitoring solutions
- BIOS security and protection features
  - Platform integrity validation
  - Device integrity validation via off-site measurements
  - Component integrity validation for Intel® Management Engine (ME) via off-site measurements
  - BIOS image capture for analysis
  - Built-in hardware cache for monitoring BIOS changes with security information and event management (SIEM) integration
- Microsoft Intune management
  - BIOS setting management integrations for Intune
  - BIOS access management security enhancements for Intune
- Remote management
  - Intel vPro® remote management
  - PC management using cellular data

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

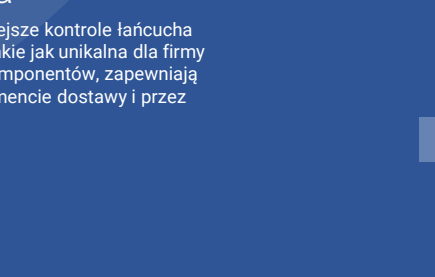
Więcej informacji o Dell Trusted Devices



Notebooki →



Komputery stacjonarne →



Stacje robocze →

Zabezpieczanie pracy zdalnej za pomocą rozwiązania Dell Trusted Workspace

Zabezpieczenia wbudowane i sprzętowe

Zewnętrzne zabezpieczenia oprogramowania

Odwiedź nas
dell.com/endpoint-security

Kontakt
global.security.sales@dell.com

Więcej informacji
Zabezpieczenia punktów końcowych — blogi →

Dołącz do dyskusji
delltechnologies @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. Zatwierdzenie przez Principled Technologies. Porównanie zabezpieczeń, kwiecień 2024 r.

[2] Źródło: Futurum Group, Endpoint Security Trends, 2023 r.

[3] Źródło: Enterprise Strategy Group, oddział TechTarget, niestandardowe badanie zlecone przez Dell Technologies,*Assessing Organizations' Security Journeys*, listopad 2023 r.

[4] Wyniki opublikowanych badań Principled Technology obejmują tylko urządzenia z procesorami Intel.