DELL Technologies

Jak walczyć ze współczesnymi zagrożeniami cybernetycznymi

za pomocą zintegrowanych zabezpieczeń punktów końcowych i zarządzania nimi

CROWDSTRIKE intel ABSOLUTE®

DELL Technologies

Streszczenie dla kierownictwa

Nowe wektory ataków stwarzają nowe zagrożenia. Wyprzedź nowoczesne zagrożenia punktów końcowych dzięki wielu warstwom obrony, które współpracują ze sobą. Dowiedz się, w jaki sposób telemetria sprzętowa może zostać zintegrowana z oprogramowaniem w celu poprawy bezpieczeństwa i możliwości zarządzania w całej flocie. Szybciej eliminuj ataki, przestrzegaj zasad modelu „zero trust” i bezpiecznie wprowadzaj innowacje dzięki łatwym w zarządzaniu urządzeniom i rozwiązaniom.

Spis treści

Krajobraz zagrożeń

Analiza przypadku

W 2023 roku firma Eclypsium odkryła lukę w oprogramowaniu wewnętrznym płyt głównych sprzedawanych przez tajwańskiego producenta. Mając na celu jedynie aktualizację oprogramowania wewnętrznego, specjaliści odkryli, że kod został zaimplementowany w sposób niezabezpieczony, co mogło pozwolić na przejęcie mechanizmu i wykorzystanie go do zainstalowania złośliwego oprogramowania.

Kilka powodów, dla których to odkrycie było szczególnie przerażające

- Klienci zostali narażeni na niebezpieczeństwo za pośrednictwem luki w zabezpieczeniach oprogramowania wewnętrznego.
- Luka istniała w dziedzinie związanej z urządzeniem, w której dawniej trudno było wykryć zagrożenia.
- Może ona zostać wykorzystana do przeprowadzenia zdalnego ataku, który omija kontrole danych uwierzytelniających.

Informacje z nagłówków gazet...

WIRED BACKCHANNEL BUSINESS CULTURE GEAR IDEAS MORE SIGN IN SUBSCRIBE

Millions of PC Motherboards Were Sold With a Firmware Backdoor

Kod ukryty w setkach modeli płyt głównych w niewidoczny i niezabezpieczony sposób pobiera programy – funkcja, która, jak twierdzą specjaliści, może być nadużywana.

Krajobraz zagrożeń

Konsekwencje

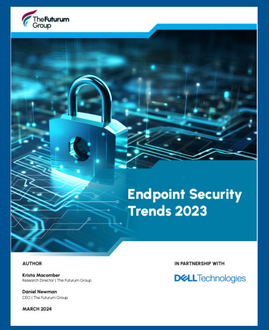
To kluczowy czynnik, który spędza sen z powiek zespołom IT i działom bezpieczeństwa:

Ataki oparte na urządzeniach.

Te wyrafinowane, złośliwe ataki mogą umożliwić przeciwnikom uzyskanie uprzywilejowanego dostępu. Co więcej, wiele z nich może całkowicie wyłączyć tradycyjne, czysto programowe zabezpieczenia, np. antywirusowe, całkowicie niewykryte.

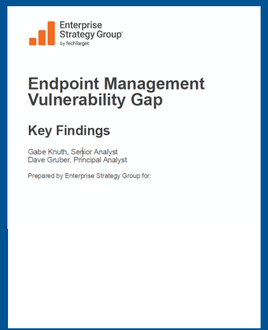
Według globalnej ankiety przeprowadzonej niedawno wśród specjalistów ds. IT i bezpieczeństwa[1], wśród najważniejszych kryteriów oceny wymienia się pozyskiwanie przez organizacje nowego sprzętu:

Automatyzacja wykrywania zdarzeń oprogramowania wewnętrznego systemu BIOS



Sześćdziesiąt dziewięć procent organizacji zgłosiło co najmniej JEDEN atak na poziomie urządzenia w ciągu ostatnich dwunastu miesięcy. To 1,5 raza więcej w stosunku do badania z 2020[2]!

Konfiguracje wysokiego ryzyka



Ponad 75% organizacji zgłasza, że doświadczyło co najmniej jednego cyberataku dokonanego za pośrednictwem nieznanego, niezarządzanego lub źle zarządzanego urządzenia końcowego[3].

Wyzwania

Co więc sprawia, że urządzenie jest łatwym celem?

Widoczność

Ataki te są trudne do zauważenia – są przeprowadzane w części urządzenia, która dawniej nie była widoczna i obserwowana.

Możliwość działania

Często organizacje dysponują dziesiątkami narzędzi, które działają w silosach, ponieważ w przypadku wykrycia ataku szybka reakcja i naprawa jest dużym wyzwaniem i wymaga dużej ilości pracy ręcznej.

Rozwiązanie

Widoczność | Możliwość działania

Jako jeden z największych dostawców technologii na świecie, firma Dell dużo myśli o bezpieczeństwie. Właśnie dlatego **konstruujemy komputery dla firm, aby od razu nadać priorytet widoczności i możliwości działania**. Takie działanie przekazuje władzę w ręce zespołów IT i zespołów ds. zabezpieczeń.

Nasze komputery komercyjne są wyposażone w **unikalne wbudowane funkcje zabezpieczeń**, takie jak BIOS Verification[4] i wskaźniki ataku[4], które pomagają wykrywać zagrożenia jeszcze przed wyrządzeniem szkód. Wykrywanie tych zagrożeń jest widoczne za pomocą **danych telemetrycznych urządzeń firmy Dell**[4]. Gdy komercyjny komputer firmy Dell z technologią Intel vPro® wykryje potencjalne zagrożenie na poziomie urządzenia, może wysłać je do systemu operacyjnego w celu szybszego i skuteczniejszego zbadania i udzielenia odpowiedzi

Przywództwo w branży

Firma Dell oferuje najbezpieczniejsze na świecie komercyjne komputery[4]

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

Przeczytaj informacje na temat badania dotyczącego bezpieczeństwa urządzeń przeprowadzonego przez firmę Principled Technologies →

Principled Technologies®

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 equipment manufacturers (OEMs): Dell, HP, and Lenovo®. Many of the Dell features relate to the Dell Trusted Device application.

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.

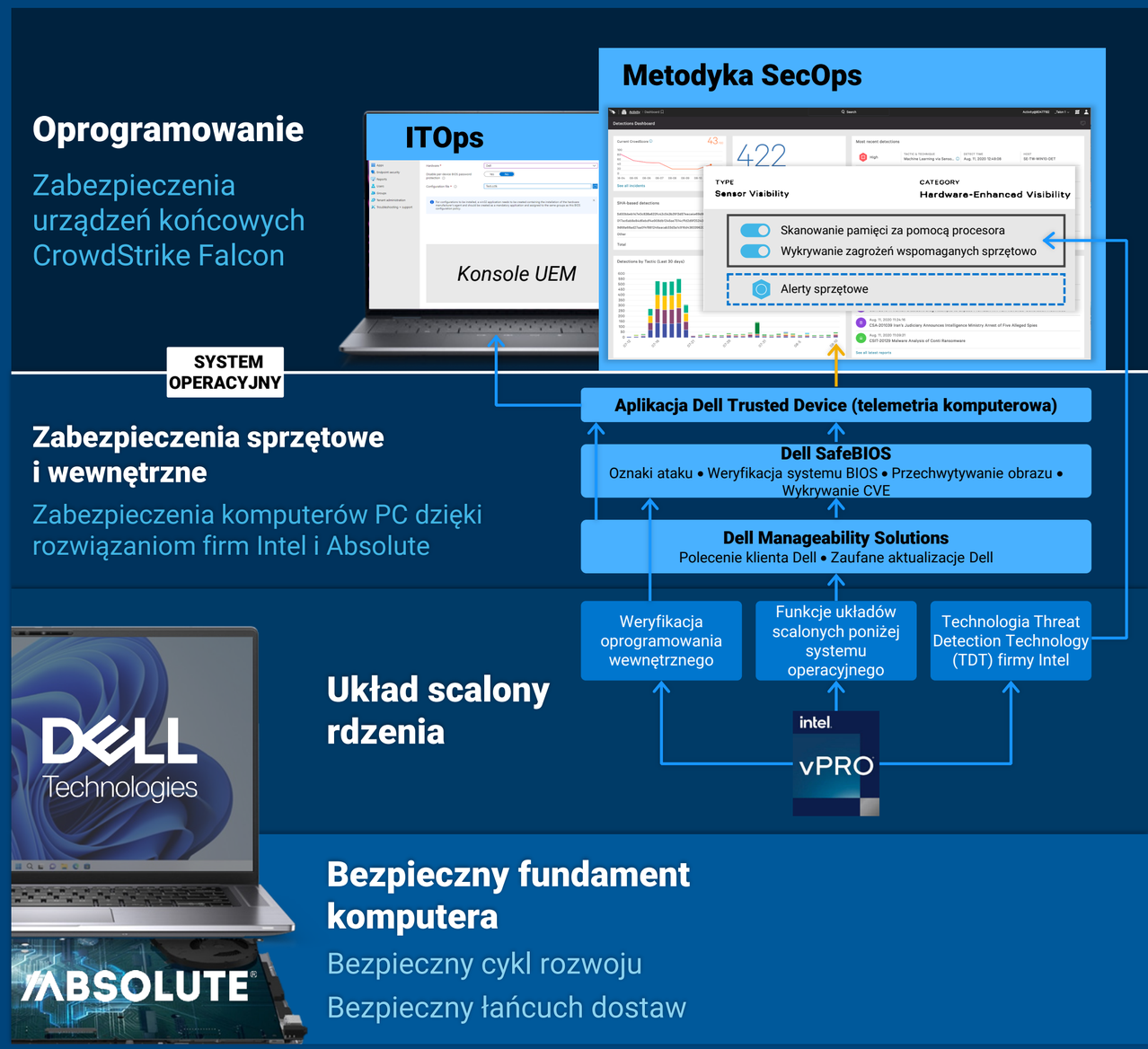
Rozwiązanie

Zwalczaj zagrożenia dzięki powiązanym zabezpieczeniom i funkcjom zarządzania

Firma Dell i nasz połączony ekosystem partnerski pracują nad zapewnieniem widoczności i możliwości działania w przestrzeni roboczej. Obejmuje to:

- Zabezpieczenia łańcucha dostaw oraz wbudowane zabezpieczenia sprzętu i oprogramowania wewnętrznego firmy Dell
- Zabezpieczenia układu scalonego rdzenia i zabezpieczenia „poniżej systemu operacyjnego” firmy Intel
- Możliwość zarządzania za pośrednictwem firmy Dell i ujednoliconych konsol zarządzania punktami końcowymi
- Zaawansowana ochrona przed zagrożeniami obejmująca punkty końcowe, sieci i chmurę zapewniana przez partnerów, takich jak CrowdStrike i Absolute

Ekosystem wykorzystuje telemetrię komputerów, jako integratora, pomagając wypełnić lukę między rozwiązaniami IT i bezpieczeństwa, przez którą zagrożenia mogą się prześlizgnąć. Takie podejście może nie tylko pomóc w zapobieganiu atakom, ale także w ich wykrywaniu, reagowaniu na nie, odzyskiwaniu po ich działaniu i naprawianiu ich.



Przypadki użycia i środki zaradcze

Aby pokazać, w jaki sposób zintegrowane zabezpieczenia i funkcje zarządzania wpływają na poprawę cyberodporności, przyjrzymy się dwóm przypadkom użycia, w tym scenariuszom ataków i środkom zaradczym.

Najpierw atak na oprogramowanie wewnętrzne BIOS. Tutaj widzimy, jak mogą przebiegać fazy cyber kill chain[5],ataku polegającego na obniżeniu wersji systemu BIOS.

Atak po obniżeniu wersji systemu BIOS

Wstępny dostęp: replikacja za pomocą nośników wymiennych + phishing

Krok 1a

Złośliwe zagrożenie wewnętrzne wykorzystuje istniejącą lukę w zabezpieczeniach systemu BIOS, aby zdalnie wykraść poświadczenia systemu operacyjnego. Włamuje się do urządzenia i obniża wersję systemu BIOS.

Krok 1b

Agresor inicjuje atak typu spear-phishing i kradnie token sesji, gdy administrator omyłkowo uwierzytelnia się w złośliwej witrynie.

Krok 2

Dostęp do poświadczeń

Osoba atakująca osiąga możliwość kontynuacji, tworząc dodatkowe konta administratorów i przechodząc do poruszania się po sieci.

Krok 3

Ruch boczny

Osoba atakująca mapuje sieć i lokalizuje serwery zarządzania systemem.

Krok 4

Eksfiltracja

Osoba atakująca eksfiltruje dane za pośrednictwem usługi internetowej.

Przypadki użycia i środki zaradcze

Środki zapobiegania obniżeniu wersji systemu BIOS

Przeciwnicy włamują się do sieci szybciej niż kiedykolwiek wcześniej. Jak podaje CrowdStrike's Global Threat Report, w roku 2023 rzeczywisty średni czas włamania eCrime (czas potrzebny na włamanie się do systemu i ruchy boczne) zmniejszył się z 84 minut w roku 2022 do 62 minut. Najszybszy zaobserwowany czas włamania wynosił zaledwie 2 minuty i 7 sekund[6]!

Oto, w jaki sposób firma Dell i nasi partnerzy, Intel® i CrowdStrike, pomagają wykryć i odeprzeć ataki mające na celu obniżenie wersji BIOS w ramach łańcucha kill chain za pomocą zabezpieczeń wspomaganych sprzętowo.

Zapobieganie | **Wykrywanie i reagowanie** | **Odzyskiwanie i naprawa**

Bezpieczny łańcuch dostaw: rygorystyczne kontrole chronią komputery począwszy od faz projektowania i rozwoju, poprzez zaopatrzenie i montaż, aż po dostawę. Firmy Dell i Intel niestrudzenie dokładają wszelkich starań, aby produkty były opracowywane w sposób ograniczający ryzyko związane z lukami w zabezpieczeniach i manipulowaniem produktami w całym cyklu życia.




Security	Integrity	Quality	Resilience
• Secure development lifecycle • Software partners securely onboarded • Information exchange with partners securely • Quality Process Audit • Separation of Duties • Least Privilege Access	• Supplier accountability • Supplier due diligence • Piece-Part Identification • SAFECode • US Exec Order 14028 SBOM -SPDX	• Counterfeit prevention & detection • Enhanced manufacturing security program • Enterprise code signing • Secured Component Verification • Freight Tracking	• Silicon Root of Trust • Platform Firmware Resiliency Guidelines • BIOS Protection Guidelines • Built-in Supplier Redundancy

Przypadki użycia i środki zaradcze

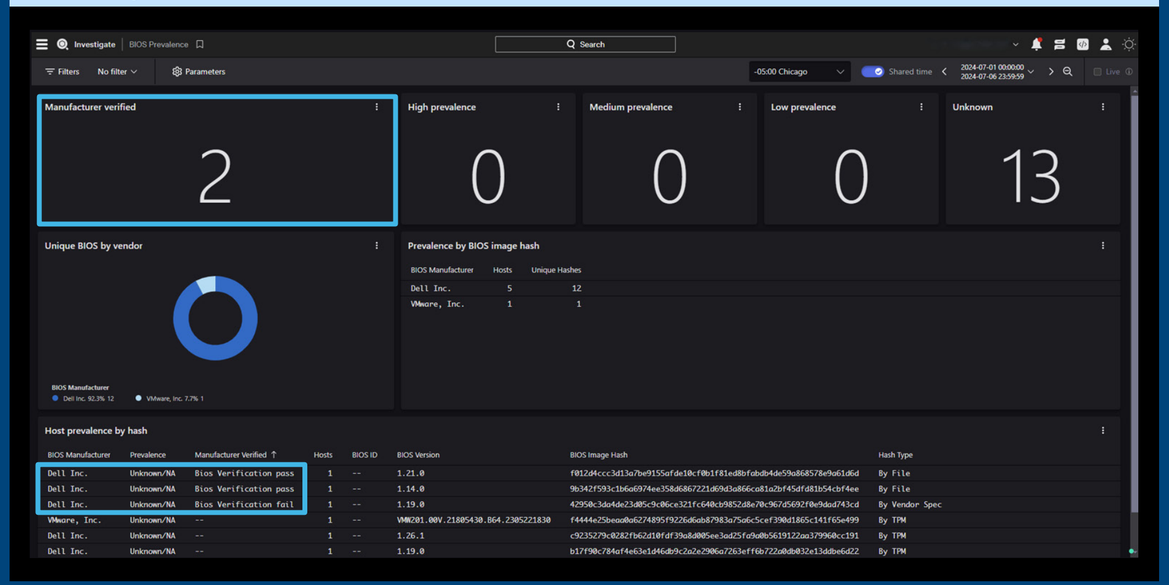
Środki zapobiegania obniżeniu wersji systemu BIOS

Przeciwnicy włamują się do sieci szybciej niż kiedykolwiek wcześniej. Jak podaje CrowdStrike's Global Threat Report, w roku 2023 rzeczywisty średni czas włamania eCrime (czas potrzebny na włamanie się do systemu i ruchy boczne) zmniejszył się z 84 minut w roku 2022 do 62 minut. Najszybszy zaobserwowany czas włamania wynosił zaledwie 2 minuty i 7 sekund[6]!

Oto, w jaki sposób firma Dell i nasi partnerzy, Intel® i CrowdStrike, pomagają wykryć i odeprzeć ataki mające na celu obniżenie wersji BIOS w ramach łańcucha kill chain za pomocą zabezpieczeń wspomaganych sprzętowo.

Zapobieganie | **Wykrywanie i reagowanie** | **Odzyskiwanie i naprawa**

Wykrywanie poświadczenia wersji systemu BIOS na platformie CrowdStrike: po włączeniu telemetrii urządzeń firmy Dell administrator może przeglądać powiadomienia z wbudowanych funkcji zabezpieczeń, takich jak weryfikacja systemu BIOS zdalnie w CrowdStrike Falcon, co przyspiesza wykrywanie podejrzanej aktywności, zanim dojdzie do trwałych uszkodzeń.



Przypadki użycia i środki zaradcze

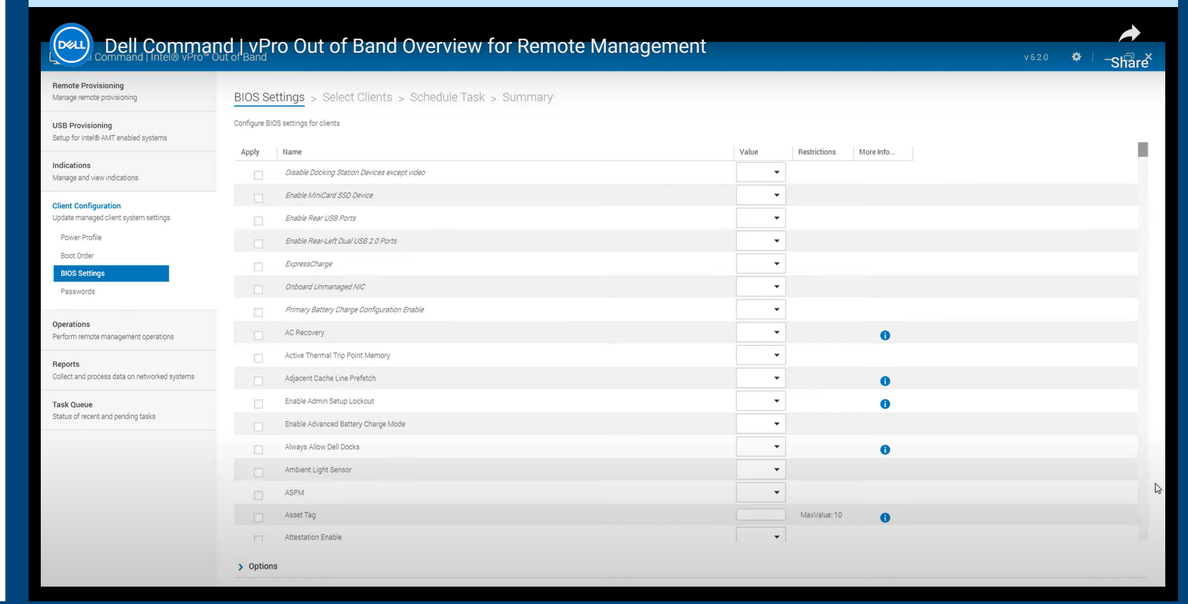
Środki zapobiegania obniżeniu wersji systemu BIOS

Przeciwnicy włamują się do sieci szybciej niż kiedykolwiek wcześniej. Jak podaje CrowdStrike's Global Threat Report, w roku 2023 rzeczywisty średni czas włamania eCrime (czas potrzebny na włamanie się do systemu i ruchy boczne) zmniejszył się z 84 minut w roku 2022 do 62 minut. Najszybszy zaobserwowany czas włamania wynosił zaledwie 2 minuty i 7 sekund[6]!

Oto, w jaki sposób firma Dell i nasi partnerzy, Intel® i CrowdStrike, pomagają wykryć i odeprzeć ataki mające na celu obniżenie wersji BIOS w ramach łańcucha kill chain za pomocą zabezpieczeń wspomaganych sprzętowo.

Zapobieganie | **Wykrywanie i reagowanie** | **Odzyskiwanie i naprawa**

Naprawa obniżenia wersji systemu BIOS: pomoc w zapobieganie przyszłym zagrożeniom związanym z systemami zewnątrz-pasmowymi. Pakiet Dell Client Command Suite z technologią Intel vPro umożliwia zdalne rozwiązywanie problemów.



Przypadki użycia i środki zaradcze

W tym drugim przypadku użycia, etap w łańcuchu kill chain ataku na łańcuch dostaw oprogramowania może wyglądać następująco.

Atak na łańcuch dostaw oprogramowania

Krok 1

Pierwszy dostęp: naruszenie bezpieczeństwa łańcucha dostaw

Atakujący wprowadza złośliwy kod do narzędzia programowego (BIOS / oprogramowanie wewnętrzne).

Krok 2

Możliwość kontynuacji

Klienci pobierają złośliwy kod, gdy przechodzą do aktualizacji swoich urządzeń.

Osoba atakująca instaluje złośliwe oprogramowanie.

Krok 3

Ruch boczny

Atakujący podszywa się pod użytkownika, którego właśnie zaatakował i wysyła złośliwe łącze do innego użytkownika. Ten użytkownik klika łącze, a atakujący kradnie jego dane uwierzytelniające.

Krok 4

Eksfiltracja

Osoba atakująca eksfiltruje dane.

Przypadki użycia i środki zaradcze

Łańcuch dostaw stał się kluczowym celem atakujących. Chociaż ataki te są mniej powszechne, skutki udanego ataku mogą być druzgocące, ponieważ organizacje wciąż uczą się, jak wzmacniać swoją obronę przed nimi.

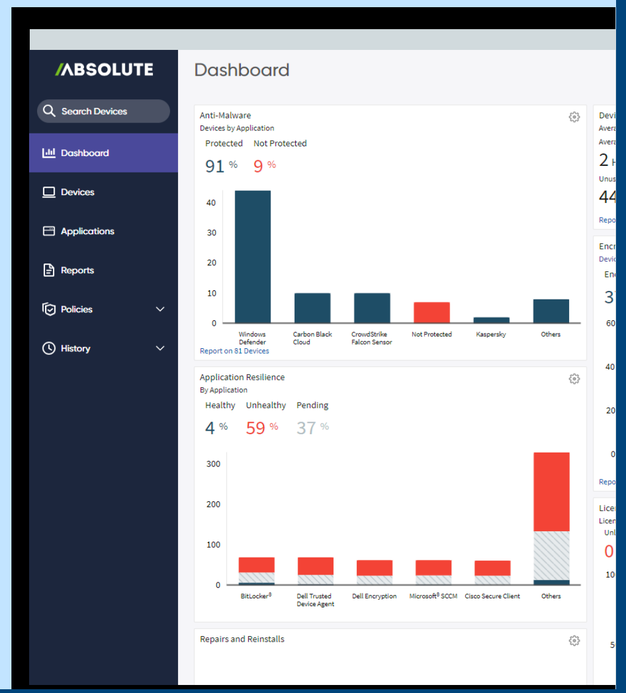
Podstawowym obowiązkiem wszystkich dostawców technologii jest zapewnienie, że to, co sprzedają, nie stanowi niezamierzonego zagrożenia dla użytkowników poprzez luki w zabezpieczeniach.

Aby pomóc w zapobieganiu atakom i zapewnić odporność zabezpieczeń, firmy Dell i Intel® przestrzegają rygorystycznych procesów i protokołów naszego cyklu bezpiecznego rozwoju[7]. Dodatkowe zabezpieczenia łańcucha dostaw, np. rozwiązanie Dell Secured Component Verification[8] i zabezpieczenia na poziomie oprogramowania wewnętrznego za pomocą rozwiązania Absolute (przedstawione po prawej stronie), dają klientom pewność przez cały okres eksploatacji komputera.

Zapobieganie | **Wykrywanie i reagowanie** | **Odzyskiwanie i naprawa**

Widoczność punktów końcowych na poziomie fabryki: widoczność wszystkich urządzeń w sieci i poza nią dzięki rozwiązaniu Absolute wbudowanemu w fabrykach zarządzanych przez firmę Dell. Niestandardowa instalacja fabryczna rozwiązania Absolute usuwa etap wdrażania i chroni urządzenia, które mogą być wysyłane do magazynów lub wielu lokalizacji użytkowników końcowych. Ogranicz ryzyko dzięki pełnemu wglądowi w flotę z poziomu pulpitu nawigacyjnego w chmurze.

- Łatwe wyszukiwanie i utrzymywanie pełnej inwentaryzacji zasobów IT i aplikacji
- Zlokalizuj i zmapuj całą flotę
- Optymalizacja wykorzystania zasobów i monitorowanie stanu bezpieczeństwa
- Obsługa wszystkich platform (Windows, Mac i Chrome)
- Osadzony w systemie BIOS 27 czołowych producentów OEM komputerów



Przypadki użycia i środki zaradcze

Łańcuch dostaw stał się kluczowym celem atakujących. Chociaż ataki te są mniej powszechne, skutki udanego ataku mogą być druzgocące, ponieważ organizacje wciąż uczą się, jak wzmacniać swoją obronę przed nimi.

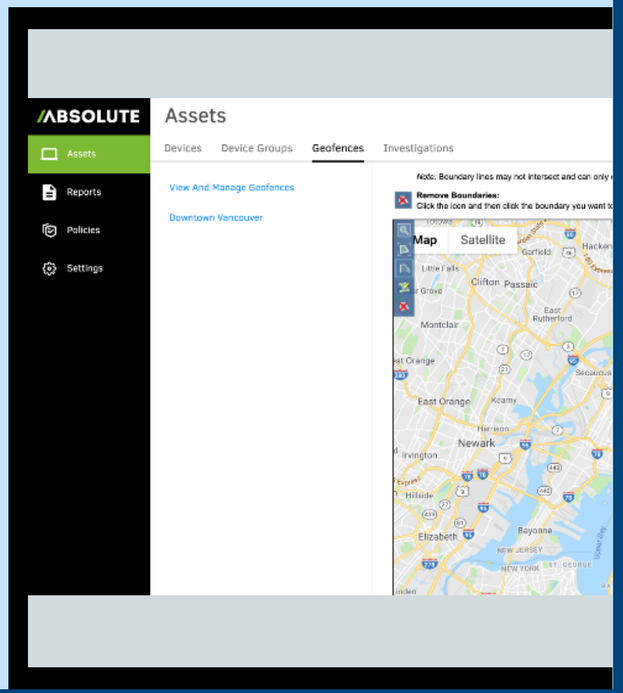
Podstawowym obowiązkiem wszystkich dostawców technologii jest zapewnienie, że to, co sprzedają, nie stanowi niezamierzonego zagrożenia dla użytkowników poprzez luki w zabezpieczeniach.

Aby pomóc w zapobieganiu atakom i zapewnić odporność zabezpieczeń, firmy Dell i Intel® przestrzegają rygorystycznych procesów i protokołów naszego cyklu bezpiecznego rozwoju[7]. Dodatkowe zabezpieczenia łańcucha dostaw, np. rozwiązanie Dell Secured Component Verification[8] i zabezpieczenia na poziomie oprogramowania wewnętrznego za pomocą rozwiązania Absolute (przedstawione po prawej stronie), dają klientom pewność przez cały okres eksploatacji komputera.

Zapobieganie | **Wykrywanie i reagowanie** | **Odzyskiwanie i naprawa**

Punkty końcowe kontroli: rozwiązanie Absolute umożliwia wykrywanie naruszenia zabezpieczeń punktów końcowych (np. uszkodzenie aplikacji o znaczeniu krytycznym przez złośliwe oprogramowanie lub zaginięcie komputera podczas transportu). Podejmij zdalne działania w celu natychmiastowego usunięcia zagrożeń, czyniąc urządzenia bezużytecznymi i/lub usuwając zawarte na nich dane.

- Chroń urządzenia, gdy przekroczą zdefiniowane granice
- Zdalna ochrona i usuwanie danych o znaczeniu krytycznym
- Czyszczenie danych po zakończeniu eksploatacji z certyfikatami zgodności
- Blokada urządzeń w celu ochrony krytycznych zasobów na żądanie
- Włączanie zdalnej ochrony oprogramowania wewnętrznego



Przypadki użycia i środki zaradcze

Łańcuch dostaw stał się kluczowym celem atakujących. Chociaż ataki te są mniej powszechne, skutki udanego ataku mogą być druzgocące, ponieważ organizacje wciąż uczą się, jak wzmacniać swoją obronę przed nimi.

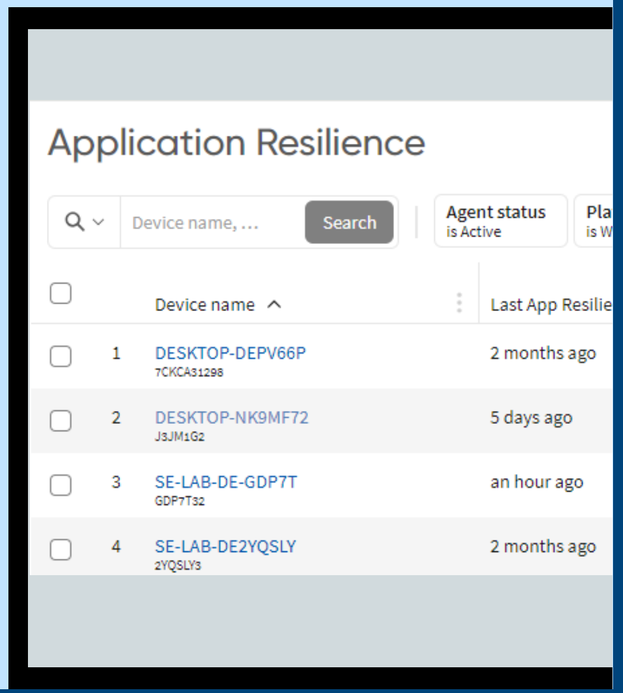
Podstawowym obowiązkiem wszystkich dostawców technologii jest zapewnienie, że to, co sprzedają, nie stanowi niezamierzonego zagrożenia dla użytkowników poprzez luki w zabezpieczeniach.

Aby pomóc w zapobieganiu atakom i zapewnić odporność zabezpieczeń, firmy Dell i Intel® przestrzegają rygorystycznych procesów i protokołów naszego cyklu bezpiecznego rozwoju[7]. Dodatkowe zabezpieczenia łańcucha dostaw, np. rozwiązanie Dell Secured Component Verification[8] i zabezpieczenia na poziomie oprogramowania wewnętrznego za pomocą rozwiązania Absolute (przedstawione po prawej stronie), dają klientom pewność przez cały okres eksploatacji komputera.

Zapobieganie | **Wykrywanie i reagowanie** | **Odzyskiwanie i naprawa**

Mechanizm autonaprawy: dzięki funkcji Absolute Persistence wbudowanej w oprogramowanie wewnętrzne systemu BIOS firmy Dell można przywrócić pierwotny stan po wykryciu ingerencji. Rozwiązanie Absolute może samodzielnie naprawić albo utrwalić dowolny zaatakowany punkt końcowy lub obsługiwaną aplikację z katalogu Application Resilience (ponad 80 aplikacji), w tym bibliotekę innych stosowanych środków zaradczych, np. Dell Trusted Device Application, Zscaler.

- Znajdowanie i łatwe usuwanie poufnych danych w punktach końcowych
- Podejmowanie działań naprawczych na różnych urządzeniach za pomocą biblioteki dostosowanych skryptów
- Aplikacje do monitorowania i samonaprawiania
- Duży i rozwijający się katalog Application Resilience kontroli punktów końcowych innych firm
- Prowadzenie dochodzeń dotyczących zagubionych lub skradzionych urządzeń oraz lokalizowanie ich wraz z zespołem dochodzeniowym Absolute



Najważniejsze wnioski

Flota jest tak bezpieczna, jak jej poszczególne komputery.

Aby skutecznie chronić się przed nowymi zagrożeniami, urządzenia muszą być zbudowane w bezpieczny sposób i mieć wbudowane zabezpieczenia.

Wykrywanie i odpieranie ataków oraz odzyskiwanie danych przez zapewnienie bezpieczeństwa punktów końcowych i łatwość zarządzania.

Bezpieczeństwo to sport zespołowy. Wykorzystaj zarówno sprzęt, jak i oprogramowanie, aby uzyskać najlepszą ochronę.

Więcej informacji:

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

Odwiedź nas: Dell.com/Endpoint-Security

Obserwuj nas: LinkedIn @DellTechnologies | X @DellTech

Dalsze działania

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 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.

1. Źródło: Enterprise Strategy Group, oddział TechTarget, niestandardowe badanie zlecone przez Dell Technologies,*Assessing Organizations' Security Journeys*, listopad 2023 r.
2. Źródło: Futurum Group, Endpoint Security Trends, 2023 r.
3. Źródło: Enterprise Strategy Group, oddział TechTarget, raport z badania *Managing the Endpoint Vulnerability Gap: The Convergence of IT and Security to Reduce Exposure*, maj 2023 r.
4. Na podstawie wyników wewnętrznej analizy przeprowadzonej przez Dell, 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. Zatwierdzenie przez Principled Technologies. A comparison of security features, kwiecień 2024 r.
5. Źródło: What is the Cyber Kill Chain? Introduction Guide – CrowdStrike.
6. Źródło: CrowdStrike 2024, Global Threat Report.
7. Źródło: Three Considerations for Establishing Device Trust | Dell USA.
8. Źródło: How to Keep Device Trust Close to the Vest | Dell USA.