DELL Technologies

Bezpieczeństwo punktów końcowych to istotny element realizacji strategii modelu „zero trust”

Trzy zalecenia dotyczące przygotowania modelu „zero trust” do wdrożenia.

DELL Technologies

Streszczenie dla kierownictwa

Model „zero trust” to długoterminowa perspektywa. Nie jest to produkt czy rozwiązanie wdrażane przez organizacje: to strategiczne ramy zarządzania bezpieczeństwem, budowane w czasie. Ten e-book zawiera praktyczne wskazówki dla osób decyzyjnych w kwestiach IT dotyczące transformacji modelu „zero trust”, ze szczególnym uwzględnieniem roli zabezpieczeń urządzeń końcowych w tworzeniu nowoczesnej, prawdziwie bezpiecznej podstawy naszej pracy z dowolnego miejsca na świecie.

Spis treści

Stan unii w cyberprze-strzeni

Zagrożeń bezpieczeństwa jest coraz więcej, a wynikają one z coraz bardziej zdalnego/ hybrydowego świata pracy w chmurze.

W ciągu ostatnich kilku lat ogromnie wzrosła złożoność ochrony zasobów danych organizacji. Chmura zmienia zasady gry pod względem produktywności biznesowej w miarę wzrostu wykorzystania pracy zdalnej/ hybrydowej, ale nie jest pozbawiona kosztów. Przejście z zarządzania wyłącznie infrastrukturą lokalną na chmurę stworzyło większą przestrzeń ataku dla przeciwników, co pociąga za sobą coraz większe konsekwencje. Na przykład, jeśli atak się powiedzie, może wpłynąć nie tylko na jednego klienta, ale potencjalnie na każdego klienta tej usługi w chmurze i jego klientów w całym łańcuchu dostaw. Korzyści dla jednostek atakujących – zarówno państw narodowych, jak i pospolitych przestępców – mogą być ogromne, w wyniku czego będą one nadal znajdować nowe luki w zabezpieczeniach do wykorzystania.

Oczekuje się, że do 2025 r. koszty globalnych szkód spowodowanych cyberprzestępczością wzrosną do **10,5 bln USD**[i]

W badaniu z 2022 r. Verizon zgłosił **5200** potwierdzonych naruszeń danych – **o 1,3 raza więcej niż w poprzednim roku**[ii]

Konsekwencje dla naszej pracy z dowolnego miejsca na świecie

Organizacje muszą znaleźć sposób na pokonanie zmieniającego się krajobrazu zagrożeń.

Jakie są więc konsekwencje coraz bardziej zdalnego świata pracy? Są dwie rzeczy:

Wszystkie organizacje są podatne na ataki, ...

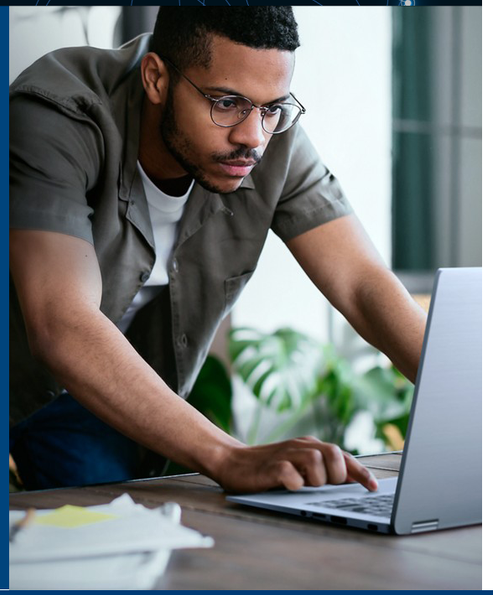
> "[Jeśli] skoncentrowany podmiot naprawdę chce dostać się do twojego systemu, istnieje duże prawdopodobieństwo powodzenia".
>
> — *Admirał Michael Rogers, były dyrektor Agencji Bezpieczeństwa Narodowego i były dowódca U.S. Cyber Command*[iii]

... a koszt popełnienia błędu może być paraliżujący.

> „Koszt naruszenia danych osiągnął rekordowy poziom i wyniósł średnio 4,88 mln USD w 2024 r."[iv]

Rośnie liczba wektorów ataków, poszerza się zakres ataków i żadna firma nie może być całkowicie bezpieczna. Organizacje muszą przyjąć najgorszy scenariusz i wzmocnić swoją obronę, by odeprzeć nieunikniony atak.

69% organizacji doświadczyło jakiegoś rodzaju cyberataku z powodu źle zarządzanych zasobów internetowych.[v]



Strategie zabezpieczeń muszą ewoluować

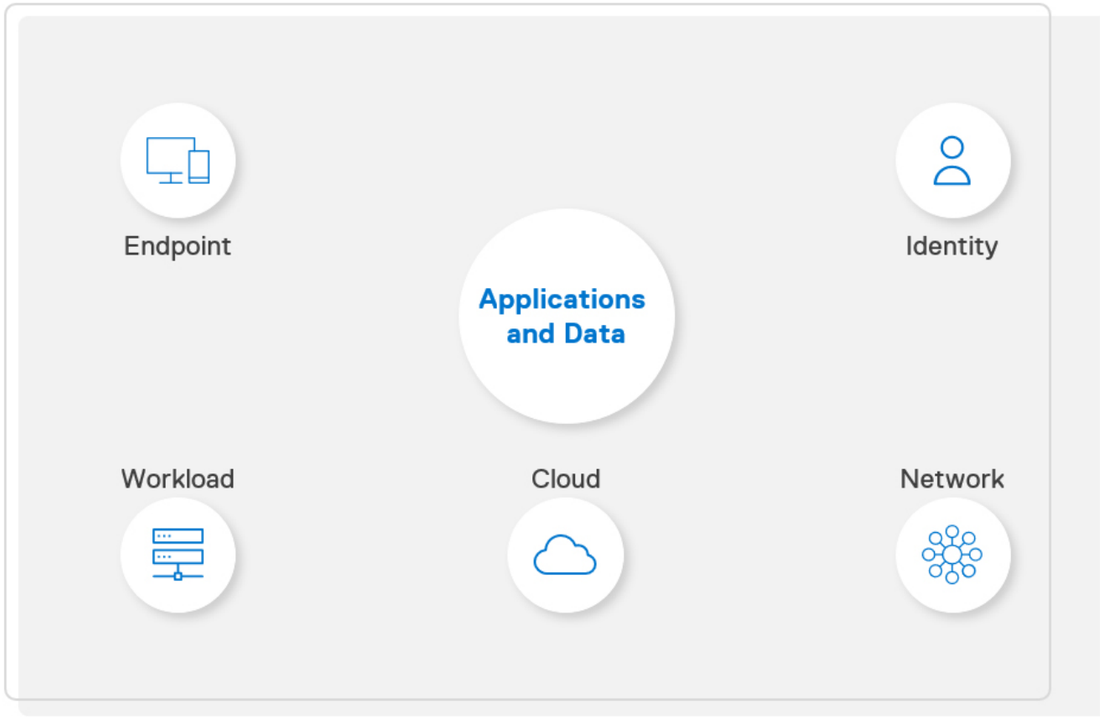
Musimy korzystać ze środowiska opartego na chmurze. W tym miejscu pojawia się model „zero trust”.

Tradycyjne modele zabezpieczeń już się nie sprawdzają. Oto przyczyny.

Aby organizacja osiągnęła odpowiedni stan zabezpieczeń, musi uwzględnić pięć punktów kontrolnych: punkt końcowy, obciążenie robocze, tożsamość, sieć i chmurę. Celem jest ochrona aplikacji i danych.

Tradycyjne podejścia są często odizolowane, co sprawia, że organizacje, które z nich korzystają, są bardziej podatne na ataki.

Dalej...

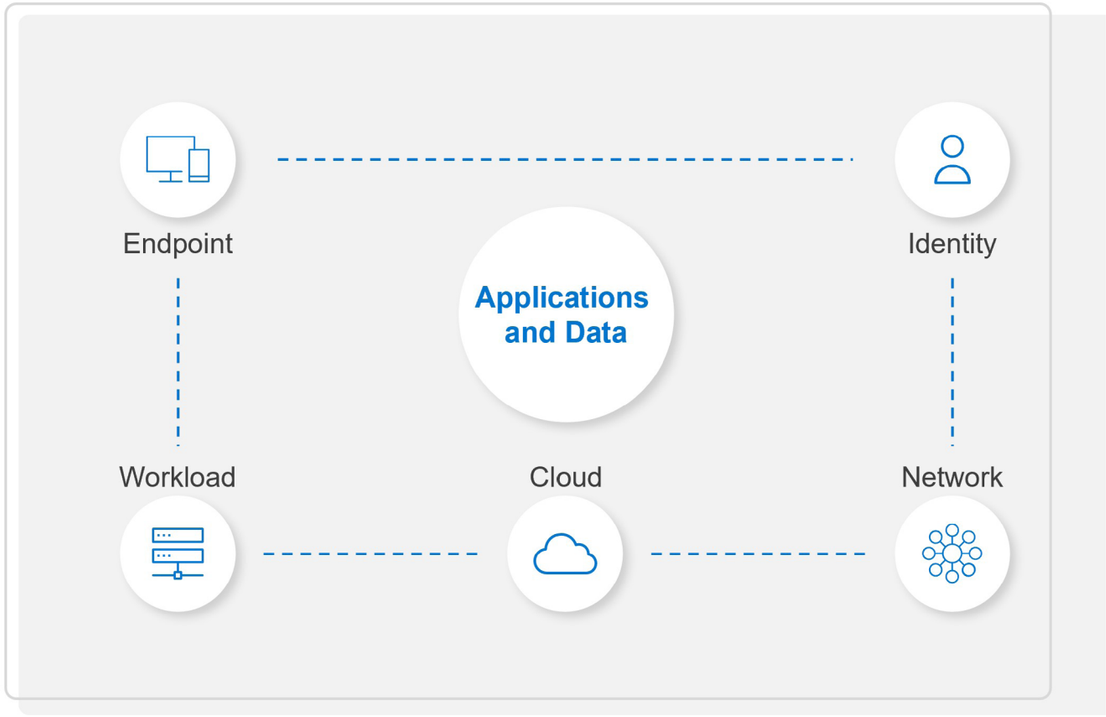


Strategie zabezpieczeń muszą ewoluować

Musimy korzystać ze środowiska opartego na chmurze. W tym miejscu pojawia się model „zero trust”.

Nowoczesne podejścia zmierzają w kierunku większej kontroli, z lepszą komunikacją między punktami kontrolnymi. Jednak w miarę jak przyjmujemy coraz bardziej zdalne/hybrydowe środowisko pracy, musimy jeszcze bardziej wzmocnić tę granicę.

Dalej...

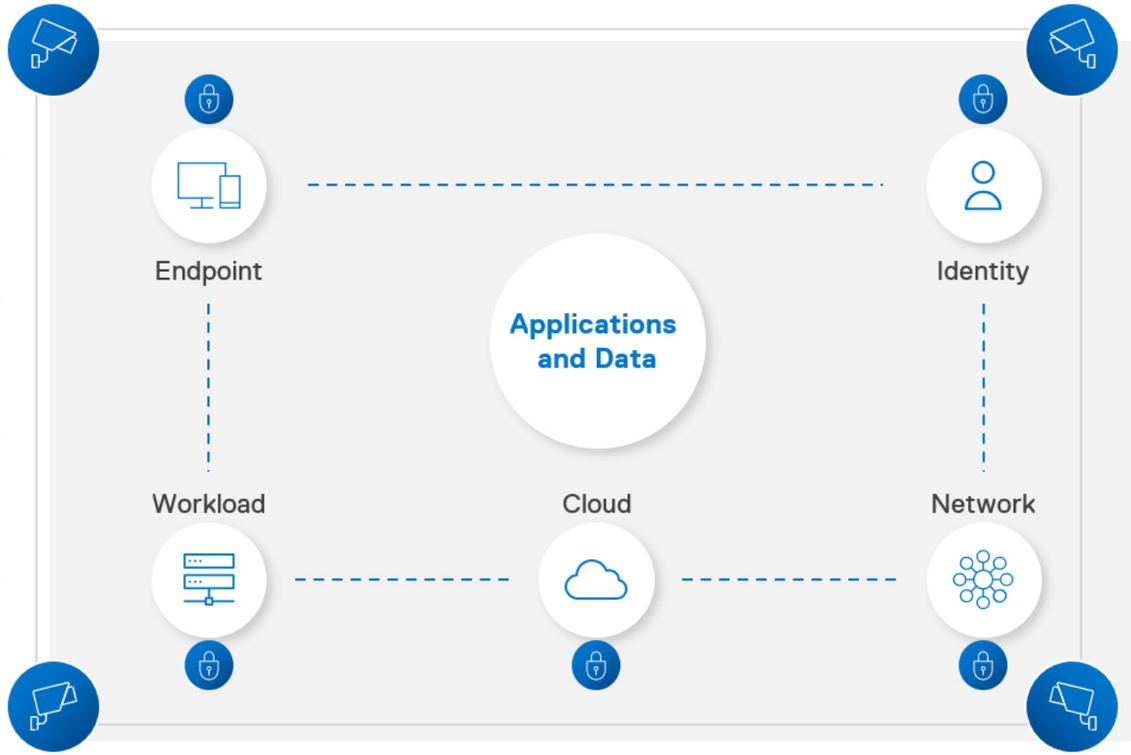


Strategie zabezpieczeń muszą ewoluować

Musimy korzystać ze środowiska opartego na chmurze. W tym miejscu pojawia się model „zero trust”.

Obecnie pracownicy pracują z dowolnego miejsca – z domu, kawiarni, hoteli – często korzystając z niezabezpieczonej sieci Wi-Fi z ograniczoną lub zerową łącznością z zabezpieczonymi zaporą sieciową biurami i centrami danych. Domyślnym połączeniem może być bezpośrednie połączenie z urządzeń do Internetu, w którym łączą się z serwerami plików w chmurze i aplikacjami SaaS (oprogramowanie jako usługa) oraz pracują z danymi przedsiębiorstwa.

Wraz z rosnącym zaawansowaniem ataków i liczbą ścieżek ataków tradycyjne strategie bezpieczeństwa oparte na ukrytym zaufaniu przestają działać. W tym miejscu pojawia się model „zero trust”.



Zrozumienie podstaw modelu „zero trust”

Model „zero trust” to nowy sposób myślenia o bezpieczeństwie. Zastępuje *domniemane* zaufanie – tj. po uwierzytelnieniu użytkownicy swobodnie poruszają się po sieci. Model „zero trust” odwraca paradygmat, dając organizacjom jawną kontrolę nad środowiskiem IT.

Zilustrujmy model „zero trust” dobrze znaną koncepcją: budowaniem protokołów bezpieczeństwa.

Pracujesz w biurze korporacji. Po zatrudnieniu otrzymujesz identyfikator i poznajesz protokoły bezpieczeństwa. Codziennie wchodzisz do budynku. Kamery są rozmieszczone wszędzie. Odbijasz identyfikator w wielu punktach. Gdy usiądziesz przy biurku, odblokowujesz komputer hasłem.

An employee arrives at their office building and gets their badge out to gain entry.

Dalej...

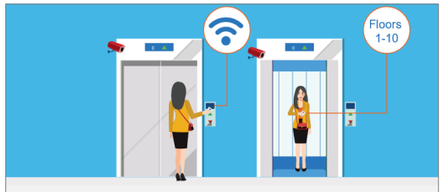
Zrozumienie podstaw modelu „zero trust”

Model „zero trust” to nowy sposób myślenia o bezpieczeństwie. Zastępuje *domniemane* zaufanie – tj. po uwierzytelnieniu użytkownicy swobodnie poruszają się po sieci. Model „zero trust” odwraca paradygmat, dając organizacjom jawną kontrolę nad środowiskiem IT.

Zilustrujmy model „zero trust” dobrze znaną koncepcją: budowaniem protokołów bezpieczeństwa.

Pracujesz w biurze korporacji. Po zatrudnieniu otrzymujesz identyfikator i poznajesz protokoły bezpieczeństwa. Codziennie wchodzisz do budynku. Kamery są rozmieszczone wszędzie. Odbijasz identyfikator w wielu punktach. Gdy usiądziesz przy biurku, odblokowujesz komputer hasłem.

An employee arrives at their office building and gets their badge out to gain entry.



They use their badge to gain access to the elevator assigned to their floor.

Dalej...

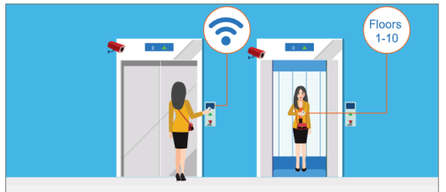
Zrozumienie podstaw modelu „zero trust”

Model „zero trust” to nowy sposób myślenia o bezpieczeństwie. Zastępuje *domniemane* zaufanie – tj. po uwierzytelnieniu użytkownicy swobodnie poruszają się po sieci. Model „zero trust” odwraca paradygmat, dając organizacjom jawną kontrolę nad środowiskiem IT.

Zilustrujmy model „zero trust” dobrze znaną koncepcją: budowaniem protokołów bezpieczeństwa.

Pracujesz w biurze korporacji. Po zatrudnieniu otrzymujesz identyfikator i poznajesz protokoły bezpieczeństwa. Codziennie wchodzisz do budynku. Kamery są rozmieszczone wszędzie. Odbijasz identyfikator w wielu punktach. Gdy usiądziesz przy biurku, odblokowujesz komputer hasłem.

An employee arrives at their office building and gets their badge out to gain entry.



They use their badge to gain access to the elevator assigned to their floor.

The employee uses their badge again to activate their floor selection in the elevator.

Dalej...

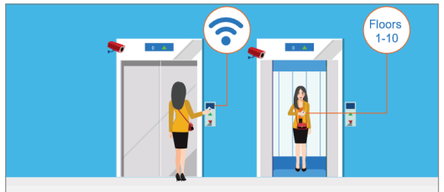
Zrozumienie podstaw modelu „zero trust”

Model „zero trust” to nowy sposób myślenia o bezpieczeństwie. Zastępuje *domniemane* zaufanie – tj. po uwierzytelnieniu użytkownicy swobodnie poruszają się po sieci. Model „zero trust” odwraca paradygmat, dając organizacjom jawną kontrolę nad środowiskiem IT.

Zilustrujmy model „zero trust” dobrze znaną koncepcją: budowaniem protokołów bezpieczeństwa.

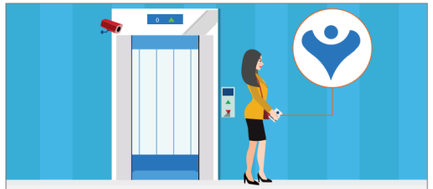
Pracujesz w biurze korporacji. Po zatrudnieniu otrzymujesz identyfikator i poznajesz protokoły bezpieczeństwa. Codziennie wchodzisz do budynku. Kamery są rozmieszczone wszędzie. Odbijasz identyfikator w wielu punktach. Gdy usiądziesz przy biurku, odblokowujesz komputer hasłem.

An employee arrives at their office building and gets their badge out to gain entry.



They use their badge to gain access to the elevator assigned to their floor.

The employee uses their badge again to activate their floor selection in the elevator.



Once they arrive on their floor, the employee walks to their office suite.

Dalej...

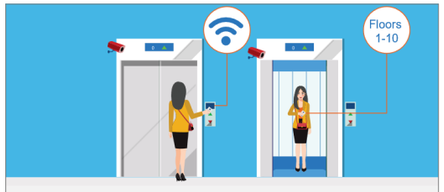
Zrozumienie podstaw modelu „zero trust”

Model „zero trust” to nowy sposób myślenia o bezpieczeństwie. Zastępuje *domniemane* zaufanie – tj. po uwierzytelnieniu użytkownicy swobodnie poruszają się po sieci. Model „zero trust” odwraca paradygmat, dając organizacjom jawną kontrolę nad środowiskiem IT.

Zilustrujmy model „zero trust” dobrze znaną koncepcją: budowaniem protokołów bezpieczeństwa.

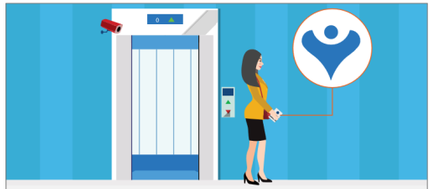
Pracujesz w biurze korporacji. Po zatrudnieniu otrzymujesz identyfikator i poznajesz protokoły bezpieczeństwa. Codziennie wchodzisz do budynku. Kamery są rozmieszczone wszędzie. Odbijasz identyfikator w wielu punktach. Gdy usiądziesz przy biurku, odblokowujesz komputer hasłem.

An employee arrives at their office building and gets their badge out to gain entry.



They use their badge to gain access to the elevator assigned to their floor.

The employee uses their badge again to activate their floor selection in the elevator.



Once they arrive on their floor, the employee walks to their office suite.

They swipe their ID card to gain entry to their suite.

Dalej...

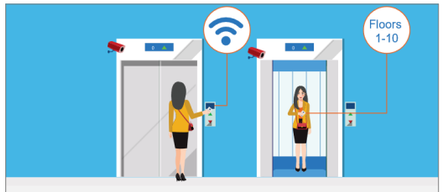
Zrozumienie podstaw modelu „zero trust”

Model „zero trust” to nowy sposób myślenia o bezpieczeństwie. Zastępuje *domniemane* zaufanie – tj. po uwierzytelnieniu użytkownicy swobodnie poruszają się po sieci. Model „zero trust” odwraca paradygmat, dając organizacjom jawną kontrolę nad środowiskiem IT.

Zilustrujmy model „zero trust” dobrze znaną koncepcją: budowaniem protokołów bezpieczeństwa.

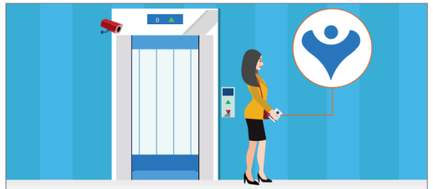
Pracujesz w biurze korporacji. Po zatrudnieniu otrzymujesz identyfikator i poznajesz protokoły bezpieczeństwa. Codziennie wchodzisz do budynku. Kamery są rozmieszczone wszędzie. Odbijasz identyfikator w wielu punktach. Gdy usiądziesz przy biurku, odblokowujesz komputer hasłem.

An employee arrives at their office building and gets their badge out to gain entry.



They use their badge to gain access to the elevator assigned to their floor.

The employee uses their badge again to activate their floor selection in the elevator.



Once they arrive on their floor, the employee walks to their office suite.

They swipe their ID card to gain entry to their suite.

The employee arrives at their desk and unlocks their computer using a password.

Dalej...

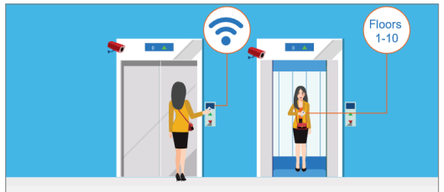
Zrozumienie podstaw modelu „zero trust”

Tak działa model „zero trust”.

Pracodawca zidentyfikował Cię pierwszego dnia. Każdy dostęp, o który prosisz od tego czasu, został zweryfikowany w celu ochrony zasobów organizacji (użytkowników, danych itp.). Aby zapewnić dodatkową warstwę bezpieczeństwa, ochroniarze obserwują cały ruch w budynku na monitorach. Każde dziwne zachowanie – np. próba uzyskania dostępu do pokoju przez osobę, której nie powinno tam być – jest sprawdzane.

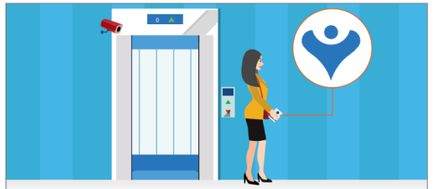
Obecnie użytkownicy, urządzenia, aplikacje i dane częściej niż kiedykolwiek znajdują się poza sieciami korporacyjnymi. W rezultacie tożsamość użytkownika stała się martwym punktem, a naruszenie tożsamości jest kluczowym elementem w większości naruszeń. Kurs „zero trust” rozwiązuje ten problem.

An employee arrives at their office building and gets their badge out to gain entry.



They use their badge to gain access to the elevator assigned to their floor.

The employee uses their badge again to activate their floor selection in the elevator.



Once they arrive on their floor, the employee walks to their office suite.

They swipe their ID card to gain entry to their suite.

The employee arrives at their desk and unlocks their computer using a password.

Stosowanie zasad „zero trust

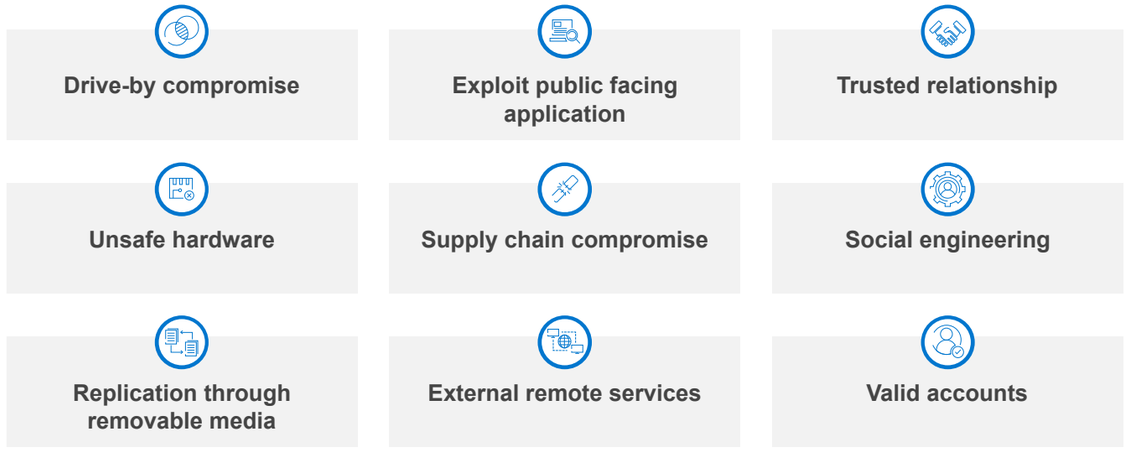
Zabezpieczenie punktów końcowych są kluczowym elementem transformacji opartej na modelu „zero trust”.

Aby skutecznie wdrożyć strategię modelu „zero trust”, należy zabezpieczyć punkty końcowe.

Zgodnie z ramami MITRE ATT&CK®, obecnie jest dziewięć „technik wstępnego dostępu”, których przeciwnicy używają, aby uzyskać dostęp do sieci *(patrz ilustracja)*.[vi] Jak pokazują badania, w naszym świecie opartym na chmurze tradycyjne zabezpieczenia nie są w stanie zapewnić bezpieczeństwa punktów końcowych. Atakujący potrzebuje tylko jednego punktu wejścia. Z punktami końcowymi atakujący mogą wykorzystywać dziesiątki luk w zabezpieczeniach pojawiających się na kolejnych etapach cyklu życia urządzeń.

Wraz ze wzrostem liczby urządzeń w sieci punkty końcowe stają się coraz większym wektorem ataku.

Zasady bezpieczeństwa w modelu „zero trust” definiują „sprawność” w sposób wyraźny – wszystko inne jest blokowane. Następnie dział zarządzania zagrożeniami monitoruje wszelkie odchylenia od sprawności, oznaczając nietypowe zachowanie i uruchamiając odpowiednie działania w celu usunięcia potencjalnego zagrożenia.



Ilustracja 1/3

Stosowanie zasad „zero trust”

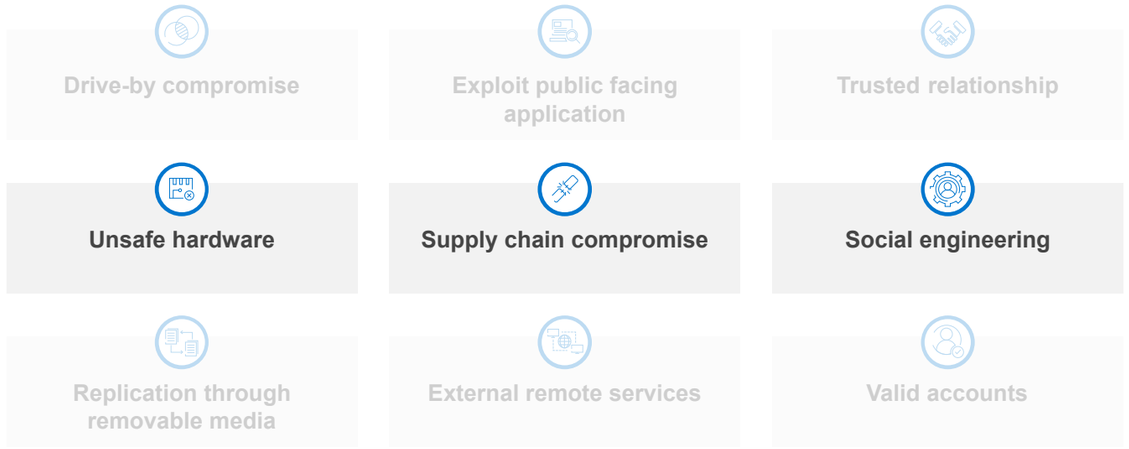
Zabezpieczenie punktów końcowych są kluczowym elementem transformacji opartej na modelu „zero trust”.

Aby skutecznie wdrożyć strategię modelu „zero trust”, należy zabezpieczyć punkty końcowe.

Zgodnie z ramami MITRE ATT&CK®, obecnie jest dziewięć „technik wstępnego dostępu”, których przeciwnicy używają, aby uzyskać dostęp do sieci *(patrz ilustracja)*.[vi] Jak pokazują badania, w naszym świecie opartym na chmurze tradycyjne zabezpieczenia nie są w stanie zapewnić bezpieczeństwa punktów końcowych. Atakujący potrzebuje tylko jednego punktu wejścia. Z punktami końcowymi atakujący mogą wykorzystywać dziesiątki luk w zabezpieczeniach pojawiających się na kolejnych etapach cyklu życia urządzeń.

Wraz ze wzrostem liczby urządzeń w sieci punkty końcowe stają się coraz większym wektorem ataku.

Zasady bezpieczeństwa w modelu „zero trust” definiują „sprawność” w sposób wyraźny – wszystko inne jest blokowane. Następnie dział zarządzania zagrożeniami monitoruje wszelkie odchylenia od sprawności, oznaczając nietypowe zachowanie i uruchamiając odpowiednie działania w celu usunięcia potencjalnego zagrożenia.



Ilustracja 2/3

Stosowanie zasad „zero trust

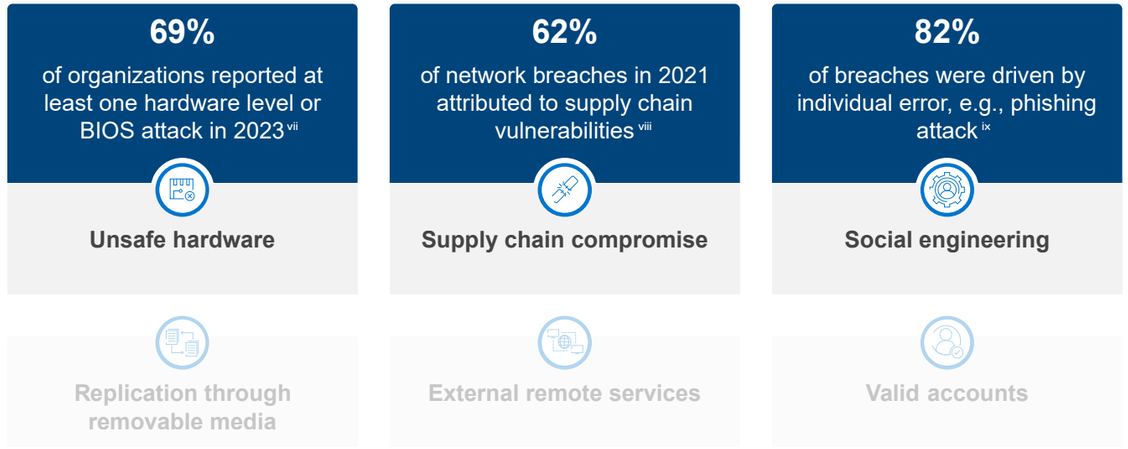
Zabezpieczenie punktów końcowych są kluczowym elementem transformacji opartej na modelu „zero trust”.

Aby skutecznie wdrożyć strategię modelu „zero trust”, należy zabezpieczyć punkty końcowe.

Zgodnie z ramami MITRE ATT&CK®, obecnie jest dziewięć „technik wstępnego dostępu”, których przeciwnicy używają, aby uzyskać dostęp do sieci *(patrz ilustracja)*.[vi] Jak pokazują badania, w naszym świecie opartym na chmurze tradycyjne zabezpieczenia nie są w stanie zapewnić bezpieczeństwa punktów końcowych. Atakujący potrzebuje tylko jednego punktu wejścia. Z punktami końcowymi atakujący mogą wykorzystywać dziesiątki luk w zabezpieczeniach pojawiających się na kolejnych etapach cyklu życia urządzeń.

Wraz ze wzrostem liczby urządzeń w sieci punkty końcowe stają się coraz większym wektorem ataku.

Zasady bezpieczeństwa w modelu „zero trust” definiują „sprawność” w sposób wyraźny – wszystko inne jest blokowane. Następnie dział zarządzania zagrożeniami monitoruje wszelkie odchylenia od sprawności, oznaczając nietypowe zachowanie i uruchamiając odpowiednie działania w celu usunięcia potencjalnego zagrożenia.



Ilustracja 3/3

Trzy zalecenia dotyczące przygotowania modelu „zero trust” do wdrożenia

Przygotuj swoją organizację na udaną transformację w kierunku modelu „zero trust’.

1 Wprowadzenie odpowiednich zasad i mechanizmów kontroli, które wspomagają priorytety Twojej firmy.

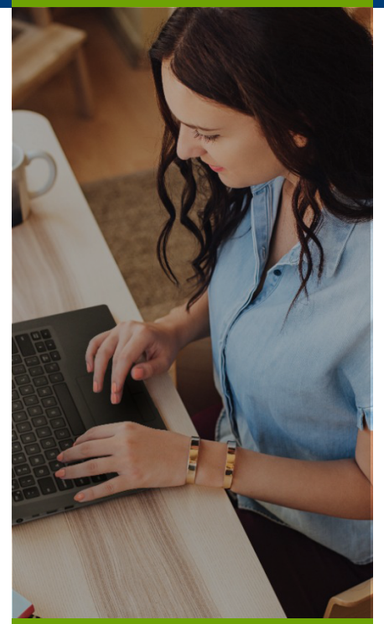
Mechanizmy zasad i zarządzanie nimi mają kluczowe znaczenie dla skutecznego wdrożenia modelu „zero trust”. Jednak żadna organizacja nie ma nieograniczonego budżetu na bezpieczeństwo, więc najpierw należy określić swoje priorytety biznesowe. Jakie są najważniejsze zasoby i własność intelektualna, które próbujesz chronić? Porównaj ten zakres ataku z dopuszczalnym ryzykiem organizacji.

Następnie zapoznaj się z obecnie obowiązującymi zasadami i mechanizmami kontroli. Dzisiejsze zagrożenia wynikają ze świata opartego na chmurze, w którym żyjemy. Czy Twój mechanizm zasad to uwzględnia?

Dzięki wdrożonym zasadom regulującym dostęp do najważniejszych zasobów można rozszerzyć zakres.

DOWIEDZ SIĘ WIĘCEJ

Aby uzyskać więcej informacji, *obejrzyj ten film*, w którym eksperci ds. cyberbezpieczeństwa firmy Dell omawiają najważniejsze zagrożenia bezpieczeństwa, z którymi borykają się obecnie organizacje.



Ponieważ coraz więcej użytkowników, aplikacji, danych i urządzeń znajduje się poza siecią firmową, **82%** osób decyzyjnych w kwestiach bezpieczeństwa IT twierdzi, że musiało ponownie ocenić swoje zasady bezpieczeństwa.[x]

Trzy zalecenia dotyczące przygotowania modelu „zero trust” do wdrożenia

Przygotuj swoją organizację na udaną transformację w kierunku modelu „zero trust’.

2 Zacznij od bezpiecznych urządzeń.

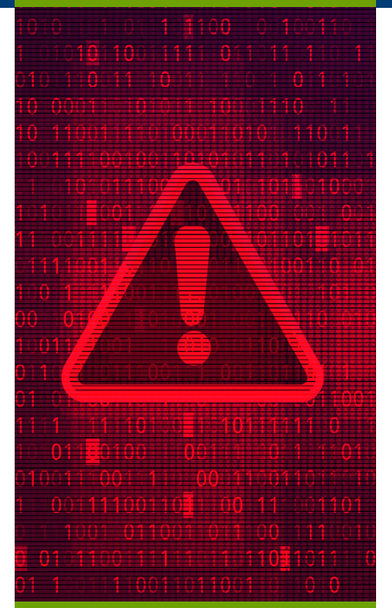
Planowanie modelu „zero trust” należy oprzeć na solidnych podstawach. Wzmocnij ochronę dzięki urządzeniom zaprojektowanym i opracowanym z myślą o bezpieczeństwie. Są to:

A. **Zabezpieczenia sprzętowe i w oprogramowaniu wewnętrznym**, które zabezpieczają stos punktów końcowych i zapewniają ich widoczność (np. wykrywają, czy system BIOS został naruszony oraz powiadamiają dział IT). Wyposaż swoją organizację w technologie, które weryfikują tożsamość przy każdym nowym żądaniu dostępu – przy jak najmniejszym wpływie na produktywność pracowników.

B. **Zabezpieczenia łańcucha dostaw i mechanizmy kontroli integralności**, które zabezpieczają każdy etap cyklu życia komputera. Jak widzieliśmy w ostatnich latach, ataki na łańcuch dostaw mogą być niszczycielskie. W przypadku prawdziwej architektury „zero trust” uwierzytelnianie, weryfikacja i monitorowanie rozpoczyna się w łańcuchu dostaw. Współpracuj z dostawcami, którzy 1) stosują bezpieczne praktyki i 2) umożliwiają weryfikację integralności urządzeń na każdym etapie – od nabywania, przez produkcję, po dostawę.

DOWIEDZ SIĘ WIĘCEJ

Więcej informacji na temat najlepszych praktyk w zakresie zabezpieczeń urządzeń można znaleźć w opracowaniu firm Dell i Intel „Jak wdrożyć kompleksowe zabezpieczenia sprzętowe i systemowe”.



W **2021** roku firma zarządzająca IT przeprowadziła atak ransomware na co najmniej **1500** klientów.[xi]

Trzy zalecenia dotyczące przygotowania modelu „zero trust” do wdrożenia

Przygotuj swoją organizację na udaną transformację w kierunku modelu „zero trust’.

3

Dąż do bezproblemowej integracji i interoperacyjności w całym ekosystemie.

Aby osiągnąć efektywną postawę bezpieczeństwa na wysokim poziomie, kluczowe znaczenie mają trzy rzeczy:

A. integracja wszystkich zabezpieczeń w całym ekosystemie IT,

B. widoczność w czasie rzeczywistym i

C. zdolność do podejmowania działań w razie potrzeby.

W naszym świecie opartym na chmurze, w którym nawet najmniejsza niesprawdzona luka w zabezpieczeniach jest potencjalnym zagrożeniem, ważne jest, aby wszystkie systemy rozpoznawały potencjalne zagrożenia *i* były skonfigurowane do podjęcia niezbędnych działań.

Czy Twoje systemy są zintegrowane, czy działają w izolacji? Czy mechanizm zasad może wyzwolić określony przepływ pracy, gdy administrator IT zostanie powiadomiony o uszkodzonym systemie BIOS w sieci?

W zintegrowanym środowisku automatyzacje powinny natychmiast poddać kwarantannie każdy system BIOS, ograniczyć dodatkowy dostęp i zainstalować poprawki.

Czy masz wgląd we wszystkie swoje punkty końcowe? Idealnie byłoby, gdyby dane telemetryczne pochodziły z każdej warstwy, od łańcucha dostaw (np. doku załadunkowego) po oprogramowanie wewnętrzne (np. alerty sabotażowe na poziomie BIOS).

Jednak ta telemetria jest tylko tak dobra, jak integracje. Czy możesz wykorzystywać swoje dane? Ważne jest, aby dysponować odpowiednimi zasobami – np. wykwalifikowanymi specjalistami ds. cyberbezpieczeństwa – co pozwoli zrozumieć przepływy pracy związane z danymi i programami, które rozwiązują problemy.

41% organizacji wdraża model „zero trust[xii]

DELL Technologies

Kluczowe wnioski

Przyszłość zabezpieczeń to model „zero trust”.

- W miarę jak poznawaliśmy przyszłość pracy, mnożyły się wektory ataków.
- Naruszenia zabezpieczeń danych są nieuniknione. Zminimalizuj zakres ataku dzięki zabezpieczeniom, które przygotowują na najgorszy scenariusz.
- Model „zero trust” to nowy sposób myślenia o bezpieczeństwie, który daje organizacjom jawną kontrolę nad środowiskiem IT.
- Zabezpieczenia punktów końcowych, które aktywują zasady zerowego zaufania, są kluczem do utrzymania bezpiecznych, nowoczesnych fundamentów.
- Wskaż najważniejsze zasoby, aby nadać priorytet budowie architektury „zero trust”.
- Pozyskuj urządzenia od dostawców, którzy oferują wbudowane zabezpieczenia i inwestuj znaczne środki w kontrolę łańcucha dostaw.
- Oceniaj zabezpieczenia i interoperacyjności IT. Kontynuuj osadzanie przepływów pracy, aby wzmocnić stan zabezpieczeń.

Dalsze działania

Bezpieczeństwo to trudny temat dla organizacji każdej wielkości. Zaangażuj doświadczonego partnera w zakresie zabezpieczeń i technologii, aby usprawnić transformację w ramach modelu „zero trust”.

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.

Skontaktuj się z nami: global.security.sales@dell.com
Odwiedź nas na: Dell.com/Endpoint-Security
Obserwuj nas: LinkedIn @DellTechnologies | Twitter @DellTech

DELL Technologies

[i] Almanach cyberbezpieczeństwa, wydanie 2. Cybersecurity Ventures, 2022 r. https://cybersecurityventures.com/cybersecurity-almanac-2022/

[ii] Ponemon Institute i IBM, raport na temat kosztów naruszenia danych, 2024 r. https://www.ibm.com/security/data-breach

[iii] American College of Cardiology, Zostaniesz zhakowany. Zaplanuj teraz: Cyberbezpieczeństwo w opiece zdrowotnej, 2021 r. https://www.acc.org/Latest-in-Cardiology/Articles/2021/11/01/01/42/Feature-You-Will-Be-Hacked-Plan-Now-Cybersecurity-in-Health-Care

[iv] Ponemon Institute i IBM, raport na temat kosztów naruszenia danych, 2024 r. https://www.ibm.com/security/data-breach

[v] Wyniki pełnej ankiety ESG, higiena bezpieczeństwa i zarządzanie postawą, 2022 r. https://www.esg-global.com/research/esg-complete-survey-results-security-hygiene-and-posture-management

[vi] MITRE ATT&CK https://attack.mitre.org/tactics/TA0001/

[vii] Grupa Futurum, Trendy w zabezpieczeniach punktów końcowych, 2023 r. https://www.delltechnologies.com/asset/en-us/solutions/business-solutions/industry-market/futurum-group-endpoint-security-trends-research-report.pdf

[viii] Raport badań naruszania danych Verizon, 2022 r. https://www.verizon.com/business/resources/reports/dbir/2022/summary-of-findings/

[ix] Raport badań naruszania danych Verizon, 2022 r. https://www.verizon.com/business/resources/reports/dbir/2022/summary-of-findings/

[x] Raport bezwzględnego ryzyka punktów końcowych, 2021 r. https://www.absolute.com/go/reports/endpoint-risk-report/

[xi] Cel technologiczny, 2021 r. https://www.techtarget.com/searchsecurity/news/252503605/Kaseya-1500-organizations-affected-by-REvil-attacks

[xii] Ponemon Institute i IBM, raport na temat kosztów naruszenia danych, 2022 r. https://www.ibm.com/security/data-breach