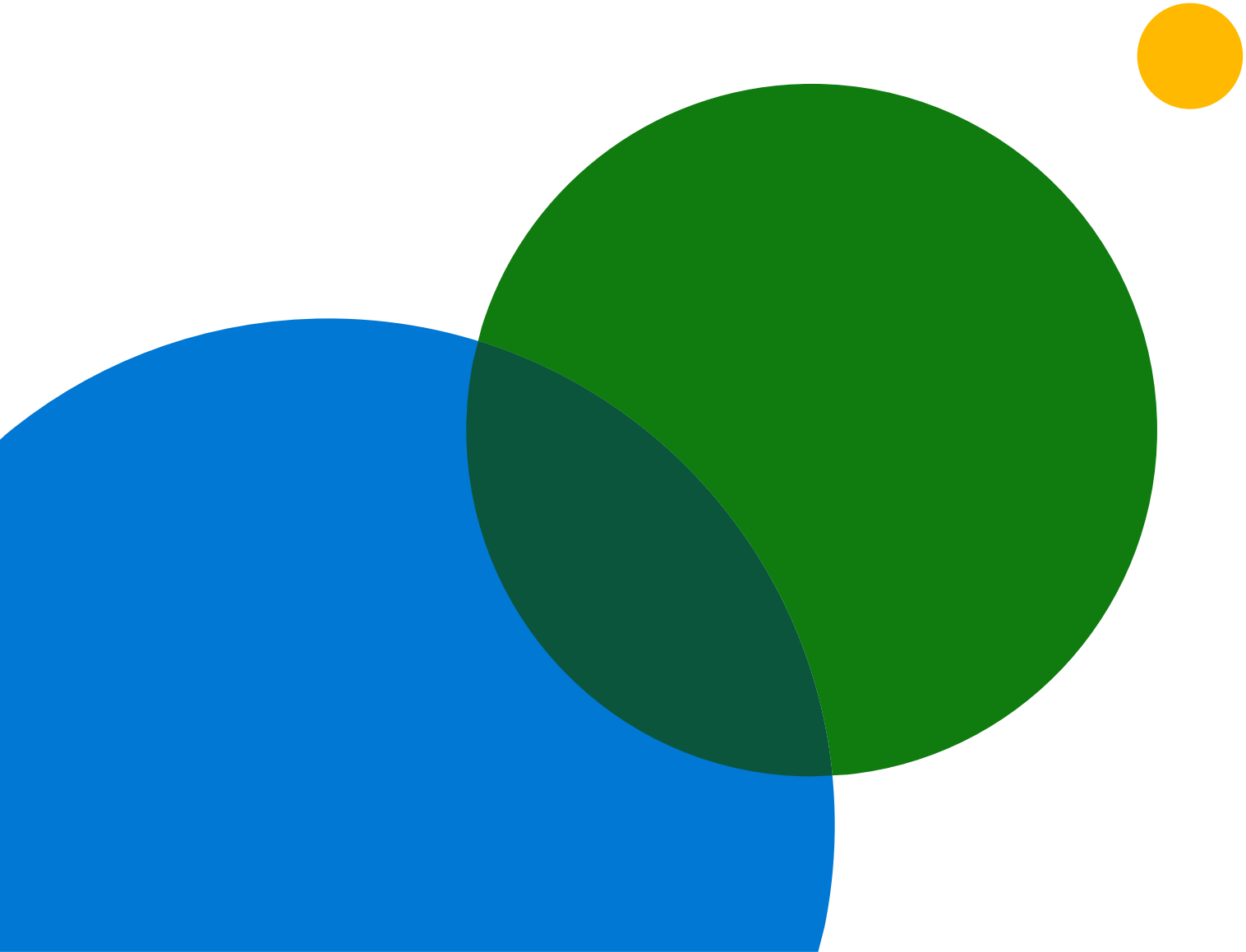
Microsoft

Ewolucja zerowego zaufania

W jaki sposób rzeczywiste wdrożenia i ataki kształtują przyszłość strategii Zero Trust



Spis treści

1. Streszczenie

Firma Microsoft pomogła tysiącom organizacji w ewolucji wdrożeń modelu Zero Trust w odpowiedzi na przejście do pracy zdalnej, a obecnie hybrydowej, przy jednoczesnym wzroście intensywności i wyrafinowania cyberataków. W niniejszym dokumencie przedstawiamy to, czego dowiedzieliśmy się od tych klientów na temat trendów rozwijających model Zero Trust, aktualizacje naszego punktu widzenia na ten model z perspektywy dojrzałości architektury i wdrożenia oraz kluczowe zalecenia, które pozwolą Ci jak najlepiej przygotować się do nowej rzeczywistości.

2. Wstęp

Zero Trust to strategia bezpieczeństwa niezbędna w dzisiejszej rzeczywistości. W 2020 roku globalna pandemia zmusiła niemal każdą organizację do przyjęcia strategii Zero Trust, ponieważ pracownicy zaczęli pracować zdalnie, wirtualne sieci prywatne (VPN) zostały naruszone lub przeciążone, a transformacja cyfrowa stała się kluczowa dla zrównoważonego rozwoju organizacji. Pojawił się mandat dla podejścia Zero Trust, aby zweryfikować i zabezpieczyć każdą tożsamość, zweryfikować stan urządzeń, wymusić najmniejsze przywileje oraz przechwycić i przeanalizować dane telemetryczne, aby lepiej zrozumieć i zabezpieczyć środowisko cyfrowe. Rządy i przedsiębiorstwa na całym świecie dostrzegły tę konieczność i przyspieszyły przyjęcie strategii Zero Trust. Wspierając tysiące wdrożeń i obserwując rozszerzający się krajobraz zagrożeń, na podstawie zdobytych doświadczeń zweryfikowaliśmy i rozwinęliśmy architekturę Zero Trust oraz model dojrzałości, który opublikowaliśmy dwa lata temu. Chcemy podzielić się tymi doświadczeniami, aby organizacje mogły je wdrożyć dziś i jutro.

Zero Trust to proaktywne, zintegrowane podejście do bezpieczeństwa we wszystkich warstwach zasobów cyfrowych, które wyraźnie i w sposób ciągły weryfikuje każdą transakcję, zapewnia najmniejsze uprawnienia i opiera się na inteligencji, zaawansowanym wykrywaniu i reagowaniu na zagrożenia w czasie rzeczywistym.

3. Pięć wniosków wyciągniętych w ciągu ostatnich dwóch lat

3.1. Zwiększ doświadczenia użytkowników i produktywność dzięki Zero Trust.

Zero Trust umożliwił użytkownikom bezpieczną pracę w domu, rejestrowanie nowych urządzeń z dowolnego miejsca, prowadzenie bezpiecznych spotkań i osiągnięcie nowego poziomu produktywności. Skuteczne wdrożenia Zero Trust wykorzystują wszystkie dostępne dane telemetryczne, aby nadać priorytet doświadczeniom użytkowników i zwiększeniu możliwości biznesowych oraz skuteczniej delegować obowiązki na odpowiedni poziom organizacji. Organizacje te dodatkowo wzmacniają pozycję użytkowników i administratorów dzięki automatycznej ochronie i wglądowi w bezpieczeństwo, co pozwala im działać pewnie i sprawnie.

Uwierzytelnianie wieloczynnikowe (MFA) zmniejsza skuteczność ataków na tożsamość o ponad 99%.

Podejście Zero Trust umożliwia ludziom wydajną i bezpieczną pracę w dowolnym czasie, miejscu i w dowolny sposób.

3.2. Zastosuj zasadę Zero Trust do wszystkich swoich zasobów cyfrowych.

Ostatnie ataki państw narodowych pokazują, że napastnicy wykorzystają każdą podatność. Z naszych obserwacji wynika, że organizacje, które najlepiej poradziły sobie z takimi atakami, szeroko wdrożyły strategię Zero Trust. Organizacje te rozpoczęły od pełnej inwentaryzacji i oceny zasobów w środowiskach lokalnych i w chmurze, nadając priorytet zabezpieczeniom w oparciu o ich względne znaczenie dla firmy. Połączono to z weryfikacją i ochroną wszystkich aspektów ich cyfrowego majątku - w tym wszystkich ludzkich i nie-ludzkich tożsamości, platform punktów końcowych, sieci, mikroserwisów, maszyn wirtualnych i obciążeń.

Wdrożenie systemu Zero Trust wymaga kompleksowej wizji i planu, w ramach którego należy nadać priorytety najważniejszym zasobom.

3.3. Zintegrowanie weryfikacji i kontroli w ramach filarów bezpieczeństwa.

Atakujący wykorzystują luki ujawnione przez nieskoordynowane programy i procesy. Aby zapobiec ingerencjom, konieczna jest kompleksowa widoczność i kontrola całego systemu bezpieczeństwa. Organizacje, które posiadają oddzielne narzędzia do monitorowania poszczególnych aspektów, takich jak sieć, dostęp do Internetu i triage internetowy, nie będą

miały pełnego obrazu swojej infrastruktury. Integracja kontroli i telemetrii w ramach filarów bezpieczeństwa umożliwia organizacjom stosowanie ujednoliconych polityk i ich konsekwentne egzekwowanie, co skutkuje bardziej solidną postawą w zakresie bezpieczeństwa.

Ujednolicenie strategii i polityki bezpieczeństwa za pomocą Zero Trust przełamuje podziały w zespołach informatycznych (IT), umożliwiając lepszą widoczność i ochronę w całym stosie IT.

3.4. Monitoruj swój status w zakresie bezpieczeństwa dzięki silnemu zarządzaniu.

Silne zarządzanie jest bezpośrednio związane z efektywnością inicjatyw Zero Trust. Organizacje o zaawansowanych strategiach weryfikują biznesowe oświadczenia o bezpieczeństwie poprzez regularne sprawdzanie tych oświadczeń, takich jak "czy to urządzenie jest zarejestrowane" lub "czy te dane są poufne?". Najlepsze strategie zarządzania opierają się na modelach zarządzania, które zapewniają integralność danych w celu prowadzenia ciągłej oceny i doskonalenia. Analiza sygnałów dotyczących wydajności i bezpieczeństwa pomaga również ocenić kulturę bezpieczeństwa, identyfikując obszary wymagające poprawy lub najlepszych praktyk.

Egzekwowanie silnego zarządzania w podejściu Zero Trust obejmuje weryfikację twierdzeń biznesowych, ocenę stanu bezpieczeństwa i zrozumienie wpływu kultury bezpieczeństwa.

Program Verify explicitly został rozszerzony o weryfikację oprogramowania w Twoim łańcuchu dostaw.

Wdrożenia Zero Trust stosują dostęp o najniższych uprawnieniach do infrastruktury, zapewniając oddzielony dostęp do systemów, które mogą dodawać lub modyfikować uprawnienia lub polityki.

3.5. Automatyzuj, aby uprościć i wzmocnić swój status w zakresie bezpieczeństwa.

Automatyzacja ma kluczowe znaczenie dla solidnego i zrównoważonego programu bezpieczeństwa. Najlepsze wdrożenia Zero Trust automatyzują rutynowe zadania, takie jak udostępnianie zasobów, weryfikacja dostępu i atestacja. Organizacje te wykorzystują uczenie maszynowe i sztuczną inteligencję w taktykach ochrony przed zagrożeniami, takich jak automatyzacja i orkiestracja bezpieczeństwa, aby bronić się same, umożliwiając im szybkie odbudowanie infrastruktury po ataku. Biorąc pod uwagę zalew powiadomień o zagrożeniach i alarmów trafiających do centrum operacji bezpieczeństwa (SOC), automatyzacja ma kluczowe znaczenie dla zarządzania środowiskiem cyfrowym z prędkością i skalą potrzebną do nadążania za dzisiejszymi atakami.

W podejściu Zero Trust priorytetem jest automatyzacja rutynowych zadań, redukująca ręczne czynności, dzięki czemu zespoły bezpieczeństwa mogą skupić się na krytycznych zagrożeniach.

4. Zasady przewodnie programu "Zero zaufania

Rzeczywiste wdrożenia przetestowały i potwierdziły podstawowe zasady skutecznej strategii Zero Trust.

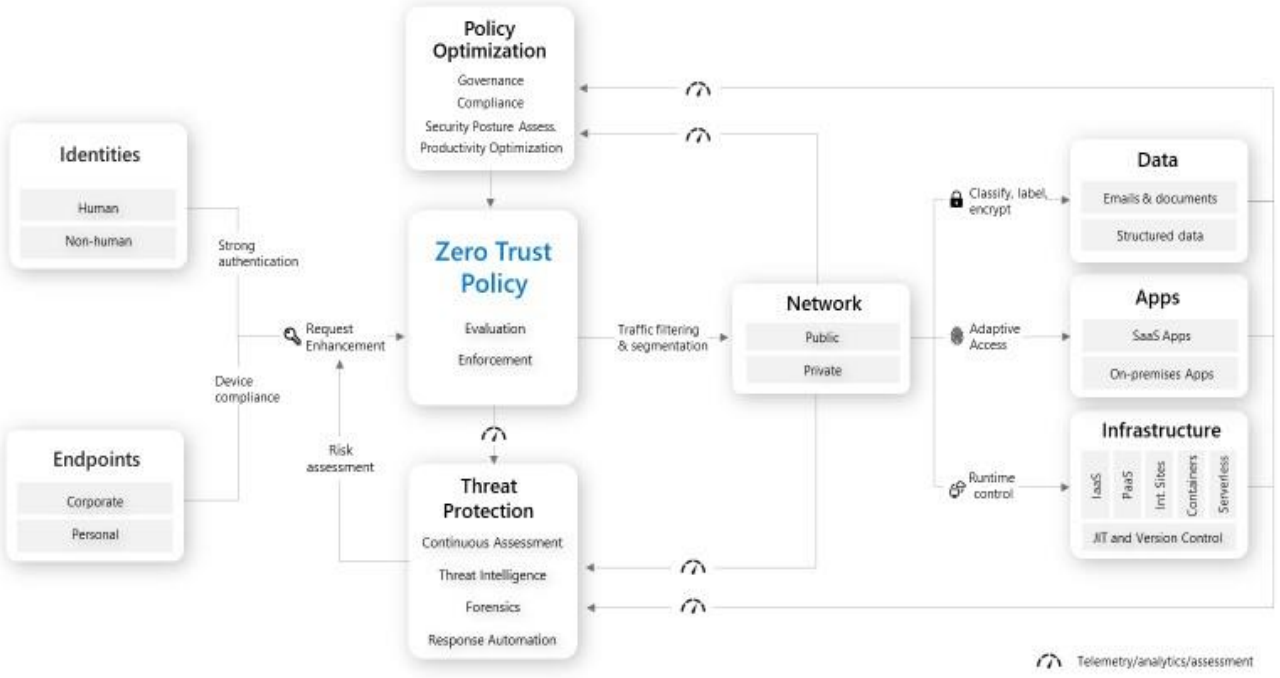
Zweryfikuj jednoznacznie
Zawsze podejmuj decyzje dotyczące bezpieczeństwa, wykorzystując wszystkie dostępne punkty danych, w tym tożsamość, lokalizację, stan urządzenia, zasoby, klasyfikację danych i anomalie.

Stosuj dostęp o najniższych uprawnieniach
Ograniczanie dostępu za pomocą zasad just-in-time i just-enough-access (JIT/JEA) oraz adaptacyjnych polityk opartych na ryzyku.

Zakładaj, że nastąpiło naruszenie
Zminimalizuj promień rażenia dzięki mikrosegmentacji, szyfrowaniu end-to-end, ciągłemu monitorowaniu oraz zautomatyzowanemu wykrywaniu i reagowaniu na zagrożenia.

5. Architektura zero zaufania

Wnioski z ostatnich dwóch lat udoskonaliły naszą architekturę Zero Trust, podkreślając kluczowe znaczenie integracji egzekwowania polityk i automatyzacji, inteligencji zagrożeń oraz ochrony przed zagrożeniami we wszystkich filarach bezpieczeństwa.



Zintegrowane elementy działają na podstawie danych telemetrycznych w każdym filarze, aby informować o decyzjach za pomocą sygnałów w czasie rzeczywistym.

6. Model dojrzałości

Oceń, w jakim punkcie znajduje się Twoja organizacja na drodze do Zero Trust, zadając poniższe pytania:

Pierwszy etap

- *Czy ograniczasz ryzyko związane z hasłami, stosując silne metody autoryzacji, takie jak MFA i zapewniając dostęp SSO do aplikacji w chmurze?*
- *Czy masz wgląd w zgodność urządzeń, środowiska chmurowe i logowania w celu wykrycia anomalii?*
- *Czy Twoje sieci są podzielone na segmenty, aby zapobiec nieograniczonemu ruchowi bocznemu wewnątrz obwodu firewalla?*

Znaczący postęp

- *Czy używasz analizy ryzyka w czasie rzeczywistym do oceny zachowań użytkowników i stanu urządzeń aby podejmować mądrzejsze decyzje?*
- *Czy potrafisz skorelować sygnały bezpieczeństwa z wielu filarów, aby wykryć zaawansowane zagrożenia i szybko podjąć działania?*
- *- Czy proaktywnie znajdujesz i naprawiasz luki w zabezpieczeniach wynikające z błędnej konfiguracji i brakujących poprawek, aby ograniczyć wektory zagrożeń?*

Najbardziej dojrzały

- *Czy jesteś w stanie dynamicznie egzekwować polityki po przyznaniu dostępu, aby chronić przed naruszeniami?*
- *Czy Twoje środowisko jest chronione za pomocą zautomatyzowanego wykrywania i reagowania na zagrożenia we wszystkich filarach bezpieczeństwa, aby szybciej reagować na zaawansowane zagrożenia?*
- *Czy analizujesz sygnały dotyczące wydajności i bezpieczeństwa, aby pomóc w optymalizacji doświadczeń użytkowników poprzez samoleczenie i użyteczne spostrzeżenia?*

Definicje komponentów architektury oraz pełny podział modelu dojrzałości na filary bezpieczeństwa znajdują się w Dodatku do niniejszego dokumentu.

7. Co dalej z Zero Trust

Zero Trust jest dynamicznym modelem, który będzie nadal ewoluował. Oto trendy, których przyspieszenia spodziewa się Microsoft:

Głębsza integracja w ramach poszczególnych filarów uprości egzekwowanie ujednoliconych zasad.
Punkt ciężkości Zero Trust przesuwa się z zabezpieczania poszczególnych filarów za pomocą odpowiednich polityk i kontroli na unifikację polityk we wszystkich filarach, zapewniając spójne egzekwowanie i holistyczną ochronę. Na przykład, unifikacja polityk pomiędzy tożsamością a punktami końcowymi była już możliwa. Obecnie obserwujemy konwergencję kontroli dostępu pomiędzy tożsamością a siecią, co pozwala zespołom bezpieczeństwa na stosowanie granularnych, spójnych polityk dla wszystkich użytkowników do wszystkich zasobów.
W przyszłości takie ujednolicenie polityk obejmie kolejne filary Zero Trust, dzięki czemu zespoły bezpieczeństwa będą mogły zautomatyzować egzekwowanie zasad w całej infrastrukturze i osiągnąć jeszcze silniejszą pozycję w zakresie bezpieczeństwa.

Inteligencja zagrożeń i zautomatyzowane reagowanie jeszcze bardziej wzmocnią pozycję zespołów ds. bezpieczeństwa.
W miarę jak ataki stają się coraz bardziej wyrafinowane i rozległe, inteligencja zagrożeń ma kluczowe znaczenie dla korelacji sygnałów w poszczególnych filarach i nadawania priorytetu incydentom. Zintegrowane rozszerzone wykrywanie i reagowanie (XDR) we wszystkich filarach odegrają kluczową rolę, zapewniając pełną widoczność i zautomatyzowane reagowanie w celu ochrony zasobów, usuwania zagrożeń i wspierania dochodzeń. Takie podejście zapewni również zespołom ds. bezpieczeństwa czas i telemetrię, których potrzebują do wykrywania, powstrzymywania i pokonywania najbardziej krytycznych ataków i zagrożeń, z jakimi mają do czynienia, zarówno wewnętrznych, jak i zewnętrznych.

Oprogramowanie i procesy DevOps będą opierać się na zasadach Zero Trust.
Dostęp użytkownika do kodu i narzędzi programistycznych będzie wykorzystywał dostęp "just-in-time" i "just-enough-access", aby zminimalizować narażenie bezpiecznych informacji i zasobów. Organizacje będą jednoznacznie weryfikować integralność bezpieczeństwa aplikacji i oprogramowania za pomocą testów wewnętrznych i zewnętrznych. Nowoczesne aplikacje i narzędzia do zarządzania siecią będą stale weryfikować sygnały i egzekwować polityki w czasie rzeczywistym, aby skuteczniej chronić dane. Organizacje będą w stanie wdrożyć podejście Zero Trust bez konieczności modernizacji aplikacji. Natywne integracje, wbudowane łączniki i konfigurowalne interfejsy programu aplikacyjnego (API) uproszczą wysiłek wymagany do integracji wektorowej.

Zero Trust zwiększy efektywność zarządzania postawami bezpieczeństwa.

W miarę jak narzędzia bezpieczeństwa będą stawały się coraz bardziej inteligentne, dadzą one IT większe możliwości i pomogą uprościć złożoność konfiguracji i zarządzania politykami. Zarządzanie postawą Zero Trust będzie oceniać ryzyka, takie jak dryf konfiguracji, pominięte poprawki oprogramowania i luki w politykach bezpieczeństwa. W miarę dojrzewania narzędzi do zarządzania postawą oczekujemy, że będą one lepiej wspierać organizacje w doskonaleniu ich postawy poprzez identyfikację obszarów wymagających poprawy w oparciu o najlepsze praktyki i kontekst historyczny, umożliwią zmiany konfiguracji jednym kliknięciem oraz zaoferują ocenę wpływu w celu optymalizacji zasięgu i wdrożeń, które zwiększą produktywność użytkowników końcowych.

Kompetencje doradcze będą odgrywać istotną rolę w adaptacji i zwiększaniu skali Zero Trust. W sytuacji, gdy niemal każda organizacja wdraża lub przygotowuje się do wdrożenia architektury Zero Trust, usługi z zakresu bezpieczeństwa będą miały zasadnicze znaczenie w rozwiązywaniu problemów związanych z niedoborem umiejętności informatycznych, potencjałem kadrowym i wzmacnianiem postawy bezpieczeństwa. W miarę przełamywania silosów pomiędzy filarami bezpieczeństwa, usługi doradcze w zakresie bezpieczeństwa będą ewoluować w celu bardziej efektywnego dostosowania strategii Zero Trust do wymagań organizacji różniących się wielkością i branżą.

8. Wniosek

Zero Trust jest imperatywem dla biznesu, technologii i zespołów bezpieczeństwa pracujących nad ochroną wszystkiego, co jest i co mogłoby być. Jest to ciągła podróż dla specjalistów ds. bezpieczeństwa, ale rozpoczęcie jej zaczyna się od prostych pierwszych kroków, stałego poczucia pilności i ciągłych iteracyjnych ulepszeń. Oprócz wniosków i trendów przedstawionych w tym dokumencie, dołączone wskazówki techniczne i zasoby mogą pomóc zespołom w rozpoczęciu lub przyspieszeniu podróży w kierunku Zero Trust.

Wskazówki i zasoby techniczne

Poniższe materiały będą stanowiły rozwinięcie zasad, wniosków i wymagań omówionych wcześniej, w celu dostarczenia praktycznych wskazówek i wymagań omówionych wcześniej, aby dostarczyć praktycznych wskazówek i pomóc przyspieszyć osiągnięcie gotowości do Zero Trust:

- **Oceń swój stopień dojrzałości za pomocą naszej Oceny dojrzałości do Zero Trust**
- **Aby zapoznać się z repozytorium zasobów technicznych, sprawdź Zero Trust Guidance Center.**
- **Dla programistów i partnerów - sprawdź Zero Trust Guidance Center, gdzie znajdziesz zasoby dotyczące integracji partnerów technologicznych**
- **Dowiedz się o naszej własnej podróży związanej z wdrażaniem Zero Trust na stronie Microsoft Digital Inside Track**

Dodatek

1. Elementy architektury zero zaufania

Filar bezpieczeństwa	Definicja
Tożsamości	Tożsamości - niezależnie od tego, czy reprezentują ludzi, aplikacje, punkty końcowe, czy urządzenia IoT - definiują płaszczyznę kontrolną Zero Trust. Kiedy tożsamość próbuje uzyskać dostęp do zasobu, musimy zweryfikować tą tożsamość za pomocą silnego uwierzytelnienia i zapewnić, że dostęp jest zgodny i typowy dla tej tożsamości oraz zgodny z zasadami dostępu z najmniejszymi przywilejami.
Punkty końcowe	Gdy tożsamość uzyska dostęp do zasobu, dane mogą przepływać do wielu różnych urządzeń - od urządzeń IoT do smartfonów, od urządzeń BYOD do urządzeń zarządzanych przez partnerów oraz od aplikacji lokalnych do serwerów w chmurze. Ta różnorodność tworzy ogromną powierzchnię ataku, co wymaga od nas monitorowania i egzekwowania stanu urządzeń oraz zgodności z przepisami w celu zapewnienia bezpiecznego dostępu.
Sieci	Wszystkie dane są ostatecznie udostępniane za pośrednictwem infrastruktury sieciowej. Kontrola sieci może zapewnić krytyczną kontrolę "w rurze", aby zwiększyć widoczność i pomóc w uniemożliwieniu atakującym w przemieszczaniu się na boki w sieci. Sieci powinny być podzielone na segmenty (w tym głębsze mikrosegmenty wewnątrzsieciowe) i należy stosować ochronę przed zagrożeniami w czasie rzeczywistym, szyfrowanie end-to-end, monitorowanie i analizę.
Zastosowania	Aplikacje i interfejsy API stanowią interfejs, za pomocą którego dane są konsumowane. Mogą to być starsze aplikacje działające lokalnie, aplikacje przeniesione do chmury lub nowoczesne aplikacje SaaS. Do wykrywania shadow IT powinny być stosowane zabezpieczenia i technologie mające na celu zapewnianie odpowiednich uprawnień w aplikacjach, blokowanie dostępu w oparciu o analitykę w czasie rzeczywistym, monitorowanie nietypowych zachowań, kontrolowanie działań użytkowników oraz zatwierdzanie bezpiecznych opcji konfiguracyjnych.
Dane	Zasadniczo zespoły bezpieczeństwa koncentrują się na ochronie danych. Tam, gdzie jest to możliwe, dane powinny pozostać bezpieczne nawet wtedy, gdy opuszczają urządzenia, aplikacje, infrastrukturę i sieci kontrolowane przez organizację. Dane powinny być sklasyfikowane, oznakowane i zaszyfrowane, a dostęp do nich ograniczony w oparciu o ich atrybuty.
Infrastruktura	Infrastruktura (czy to serwery w siedzibie firmy, maszyny wirtualne w chmurze, kontenery czy mikrousługi) stanowi krytyczny wektor zagrożeń. Oceniaj dostęp do wersji, konfiguracji i JIT, aby wzmocnić obronę, wykorzystuj telemetrię do wykrywania ataków i anomalii oraz automatycznie blokuj i oznaczaj ryzykowne zachowania oraz podejmuj działania ochronne.
Optymalizacja polityki	Specyficzne dla organizacji polityki bezpieczeństwa stosowane w programach organizacji w całym środowisku cyfrowym. Polityki te są zoptymalizowane pod kątem procesów biznesowych, zarządzania, zgodności z przepisami i doświadczeń użytkowników końcowych.
Egzekwowanie polityki	Polityka Zero Trust przechwytuje żądanie i wyraźnie weryfikuje sygnały z wszystkich 6 podstawowych elementów w oparciu o konfigurację polityki i wymusza najmniej uprzywilejowany dostęp. Sygnały obejmują rolę użytkownika, lokalizację, zgodność urządzenia, wrażliwość danych, wrażliwość aplikacji i wiele innych. Oprócz informacji telemetrycznych i stanowych, ocena ryzyka wynikająca z ochrony przed zagrożeniami jest uwzględniana w polityce, aby automatycznie reagować na zagrożenia w czasie rzeczywistym. Zasady są egzekwowane w momencie dostępu i stale oceniane w trakcie sesji.
Ochrona przed zagrożeniami	Dane telemetryczne i analityczne z wszystkich 6 elementów fundamentalnych zasilają system ochrony przed zagrożeniami w naszej architekturze Zero Trust. Duże ilości danych telemetrycznych i analitycznych wzbogacone o inteligentne zagrożenia generują wysokiej jakości oceny ryzyka, które mogą być badane ręcznie lub zautomatyzowane. Ocena ryzyka jest przekazywana do mechanizmu polityk w celu zapewnienia zautomatyzowanej ochrony przed zagrożeniami w czasie rzeczywistym.

2. Tabela modelu dojrzałości, część 1 z 2

	Początkowy	Zaawansowany	Optymalny
Tożsamość	• Uwierzytelnianie przy użyciu słabych danych uwierzytelniających, takich jak hasło • Tożsamość w chmurze federuje z systemem w siedzibie firmy i niektórymi aplikacjami połączonymi z dostawcą tożsamości w chmurze • Ręczne tworzenie rezerw, zarządzanie i ograniczona widoczność ryzyka	• Uwierzytelnianie przy użyciu silnego uwierzytelniania, takiego jak MFA • Większość aplikacji jest sfederowana z tożsamością w chmurze w celu uwierzytelniania, autoryzacji, dostarczania i usuwania danych. • Wgląd w tożsamość i ryzyko sesji	• Uwierzytelnianie przy użyciu metod bezhasłowych i odpornych na phishing • Wszystkie aplikacje są nowoczesne i sfederowane z tożsamością w chmurze dla uwierzytelniania, autoryzacji, dostarczania i usuwania danych. • Zautomatyzowane przeglądy dostępu zapewniają właściwe zarządzanie członkostwem w grupach, dostępem do aplikacji i przypisywaniem ról
Punkty końcowe	• Zarządzanie w siedzibie firmy przy użyciu podstawowej ochrony punktów końcowych (EPP) • Ustawienia konfiguracyjne zarządzane za pomocą Group Policy • Ograniczona widoczność w zakresie zgodności	• Zarządzanie w siedzibie firmy połączone z chmurą MDM w celu konfiguracji zabezpieczeń i urządzeń zarejestrowanych z tożsamością w chmurze • Egzekwowanie zgodności w oparciu o stan urządzenia przy pierwszym dostępie • EPP + EDR obejmujące monitorowanie i reagowanie po włamaniu, podstawowe podręczniki automatycznego remediacji	• Stan urządzenia, status oprogramowania antymalware i zabezpieczenia są stale monitorowane i sprawdzane. • Ustawienia zabezpieczeń urządzeń wymuszane są na wszystkich urządzeniach za pomocą linii bazowych • EPP + EDR + TVM do zarządzania postawą, zaawansowane, automatyczne playbooki remediacji i integracja XDR
Sieć	• Uprawnienia są zarządzane ręcznie i są statyczne • Niektóre zasoby Internetu są dostępne dla użytkowników bezpośrednio; VPN i sieci otwarte zapewniają dostęp do większości zasobów. • Aplikacje robocze są monitorowane pod kątem znanych zagrożeń i statycznego filtrowania ruchu; Część ruchu wewnętrznego i zewnętrznego jest szyfrowana.	• Uprawnienia są zarządzane zgodnie z polityką i dostosowywane na podstawie zaleceń • Dostęp do wrażliwych obciążeń roboczych jest odizolowany na podstawie sesji; aplikacje w chmurze, zasoby internetowe i wrażliwe sieci prywatne są dostępne bez zakładanego zaufania do lokalizacji. • Ruch jest monitorowany; większość ruchu wewnętrznego i zewnętrznego jest szyfrowana	• Adaptacyjne polityki dostępu wyraźnie sprawdzają automatycznie zmieniające się uprawnienia do zasobów w oparciu o ryzyko i wykorzystanie. • Wszystkie sesje są stale oceniane pod kątem naruszeń polityki, a dostęp do nich jest dynamicznie cofany na podstawie sygnałów dostarczanych przez usługę opartą na chmurze. • Ruch jest monitorowany w celu identyfikacji potencjalnych zagrożeń i dynamicznej sygnalizacji; Wszystkie dane i ruch sieciowy są szyfrowane od początku do końca
Zastosowania	• Ocena ryzyka związanego z chmurą shadow IT oraz monitorowanie i kontrola krytycznych aplikacji. • Niektóre krytyczne aplikacje w chmurze są dostępne dla użytkowników	• Aplikacje on-premises są skierowane do internetu • Aplikacje w chmurze są skonfigurowane z SSO	• Wszystkie aplikacje są dostępne przy użyciu dostępu o najniższych uprawnieniach z ciągłą weryfikacją • Dynamiczna kontrola wszystkich aplikacji z monitorowaniem i reagowaniem w trakcie sesji

3. Tabela modelu dojrzałości, część 2 z 2

	Rozpoczęcie pracy	Zaawansowane	Optymalny
Dane	• Metody oparte na regułach i słowach kluczowych są wykorzystywane do wykrywania i klasyfikowania danych wrażliwych w niektórych lokalizacjach, aplikacjach, usługach • Dostęp jest regulowany przez kontrolę obwodu, a nie wrażliwość danych • Etykiety wrażliwości są stosowane ręcznie, co powoduje niespójność klasyfikacji danych.	• Zautomatyzowane odkrywanie i klasyfikacja we wszystkich lokalizacjach, aplikacjach i usługach oraz heterogeniczne typy danych • Dostęp jest regulowany bez względu na granicę lub granicę aplikacji. • Ograniczanie przepływu danych wrażliwych	• Ciągłe odkrywanie i korelacja sygnałów z wykorzystaniem uczenia maszynowego w celu identyfikacji ryzyka eksfiltracji danych • Decyzje o dostępie są regulowane przez mechanizm polityki bezpieczeństwa w chmurze • Proaktywne zarządzanie danymi i ocena ryzyka
Infrastruktura	• Uprawnienia są zarządzane ręcznie w różnych środowiskach • Zarządzanie konfiguracją maszyn wirtualnych i serwerów, na których uruchomione są obciążenia robocze	• Aplikacje są monitorowane i alarmowane o nietypowych zachowaniach • Każdej aplikacji przypisana jest tożsamość • Ludzki dostęp do zasobów wymaga just-in-time	• Nieautoryzowane wdrożenia są blokowane i wywoływany jest alarm • Granularny wgląd i kontrola dostępu są dostępne dla wszystkich aplikacji • Dostęp użytkowników i zasobów jest podzielony na segmenty dla każdego aplikacji roboczej
Ochrona przed zagrożeniami	• Reaktywne wykrywanie zagrożeń i podatności • Ochrona przed włamaniem przy użyciu narzędzi takich jak AV dla punktów końcowych, EOP dla poczty elektronicznej • Odizolowane lub wyizolowane zabezpieczenia i reagowanie • Podstawowe monitorowanie punktów końcowych	• Proaktywne wykrywanie zagrożeń i podatności oraz reagowanie po ich wystąpieniu • Zautomatyzowane dochodzenie i usuwanie skutków (AIR) dla grup testowych i podstawowych zagrożeń • Możliwości XDR w zakresie co najmniej dwóch filarów bezpieczeństwa oraz pewna integracja z systemem zarządzania informacjami i zdarzeniami związanymi z bezpieczeństwem (SIEM)	• AIR został w pełni włączony • Aktywnie wykorzystuje analizy zagrożeń, informacje o zagrożeniach oraz zalecane środki zaradcze w celu wyeliminowania luk i błędnych konfiguracji • Możliwości XDR zastosowane we wszystkich filarach i w pełni zintegrowane z SIEM w celu polowania na zaawansowane zagrożenia, wykrywania, reagowania i zapobiegania im
Egzekwowanie polityki	• Decyzje dotyczące dostępu są oparte na ograniczonych sygnałach • Decyzje dotyczące dostępu nie są scentralizowane • Decyzje dotyczące dostępu są podejmowane wyłącznie w momencie uzyskania dostępu i nie mają charakteru ciągłego	• Decyzje dotyczące dostępu opierają się na sygnałach pochodzących z co najmniej dwóch filarów • Scentralizowany silnik polityki używany do podejmowania decyzji o dostępie	• Decyzje dotyczące dostępu są oparte na sygnałach z wszystkich filarów • Decyzje są stale oceniane, a polityka jest egzekwowana w czasie rzeczywistym • Ocena zagrożeń w czasie rzeczywistym wykorzystywana przy podejmowaniu decyzji o dostępie

Przyspiesz swoją podróż już dziś dzięki zasoby firmy Microsoft.

aka.ms/zerotrust/