

Krawędź Usługi Bezpiecznego Dostępu (SASE)

Przyspieszenie transformacji sieci i modernizacji zabezpieczeń

CO TO JEST SASE?

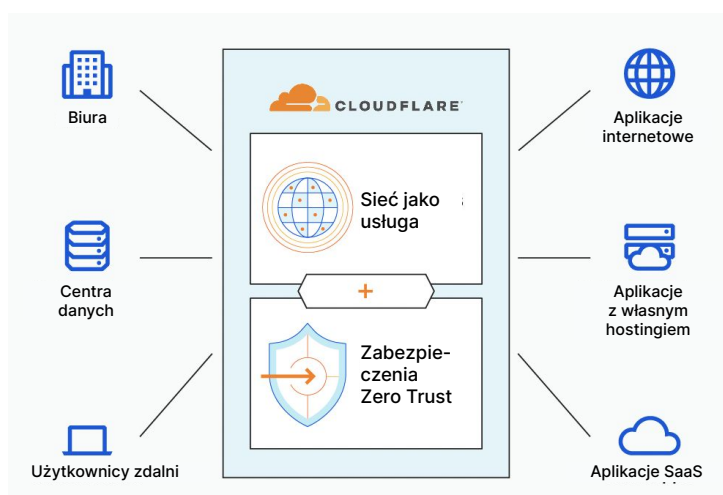
Pojawienie się inicjatyw cyfrowych i rozwiązań chmurowych spowodowało przesunięcie aplikacji ze scentralizowanych centrów danych do rozproszonych lokalizacji, takich jak chmura publiczna, chmura prywatna i SaaS. Użytkownicy pracują jednocześnie ze swojego domu, biura, hybrydowo lub zdalnie z dowolnej lokalizacji. Ten nowy wzorzec ruchu („każdy z każdym”) poszerzył obszar ataku architektury sieciowej, powodując zwiększone ryzyko cybernetyczne.

Wprowadzenie architektury SASE odnosi się do zmiany w dostępie do aplikacji. SASE to konwergencja sieci i funkcji jej bezpieczeństwa dla ruchu typu „każdy z każdym” z lepszą kontrolą bezpieczeństwa wykorzystując zasady Zero Trust. Gartner przewiduje, że „Do 2025 roku co najmniej 60% przedsiębiorstw będzie miało wyraźne strategie i harmonogramy przyjęcia SASE obejmujące użytkownika, oddział i dostęp do krawędzi sieci, w porównaniu z 10% w 2020 roku.”¹

W jaki sposób Cloudflare wdraża SASE

Platforma SASE firmy Cloudflare, Cloudflare One, to sieć jako usługa typu Zero Trust zbudowana na pojedynczej, ujednoliconej platformie sieciowej typu Internet-native. Umieszcza ona oparte na tożsamości kontrole bezpieczeństwa, zaporę sieciową, WAN jako usługę i inne elementy blisko użytkowników w każdym miejscu na świecie, pomagając im szybko i bezpiecznie łączyć się z dowolnym zasobem organizacji.

Zero Trust korzysta z opartej na proxy architektury odmowy domyślnej, która nakazuje weryfikację i autoryzację każdego żądania do, z i między podmiotami w sieci korporacyjnej, zamiast zapewniać pełne zaufanie i dostęp do aplikacji, gdy znajdują się one w sieci. Dzięki temu użytkownicy mogą dostać się tylko do tych aplikacji, do których mają pełny dostęp.



Przeszkody we wdrożeniu SASE

Według firmy Gartner jedną z przeszkód w SASE jest globalny zasięg. Firmy z listy Fortune 500 są obecne w 32 krajach, a wielu dostawców SASE oferuje usługi tylko w kilku regionach i krajach. Brak globalnego zasięgu powoduje niespójne egzekwowanie polityki bezpieczeństwa i problemy z wydajnością.

Dla firm dążących do pełnego ujednolichenia usług bezpieczeństwa i usług brzegowych sieci od jednego dostawcy, Cloudflare One zapewnia usługi zbudowane w naszej globalnej sieci ponad 275 miast w ponad 100 krajach i ~50ms dla 95% populacji korzystającej z Internetu.

„SASE zależy od dostarczania usług w chmurze, a ślad dostawcy w chmurze może uniemożliwić wdrożenie w niektórych lokalizacjach, takich jak Chiny, Rosja i Bliski Wschód, gdzie ich obecność w chmurze może być ograniczona.”²

Gartner

Komponowalność przyspiesza SASE

W zależności od istniejących inwestycji, klienci przechodzący na model SASE często mają kilku dostawców oferujących kompleksowe rozwiązanie. Korzystanie z usług więcej niż jednego czy dwóch dostawców prowadzi do zwiększenia całkowitego kosztu, złożoności operacyjnej, problemów z wydajnością i, co najważniejsze, zmniejszenia elastyczności biznesowej. Na rynku rozwiązań SASE jest kilkudziesięciu różnych dostawców. Niektórzy specjalizują się w bezpieczeństwie, inni w sieci, a bardzo niewielu jest ekspertami w obu tych dziedzinach.

Konsolidacja sprzętu i produktów punktowych może potrwać lata, ponieważ sprzęt jest odświeżany w cyklach 5-7 letnich. Odświeżenie sprzętu sieciowego w pierwszej kolejności może spowodować problemy ze współdziałaniem z istniejącymi usługami bezpieczeństwa i na odwrót. Aby przyspieszyć wdrażanie SASE we własnym tempie, klienci potrzebują platformy SASE, która jest komponowalna. Komponowalne usługi są dostępne na żądanie, działają na zasadzie plug and play i są interoperacyjne w ramach istniejącej infrastruktury.

Cloudflare One to komponowalna platforma SASE. Dzięki naszej platformie, usługi bezpieczeństwa i sieciowe działają w ramach tej samej infrastruktury i są ujednolicone architektonicznie na każdym poziomie — nie tylko pojedynczego monitora. Jedna płaszczyzna sterowania do jednej płaszczyzny danych z pojedynczą kontrolą jak najbliższą użytkownika, dzięki czemu nie ma dodatkowych opóźnień. Każda sieć z jednej płaszczyzny kontroli może połączyć się z dowolnym zasobem i zabezpieczyć ruch za pomocą jednorazowej integracji. Jeden interfejs zarządzania — UI, API i CLI.

„Staraj się nie korzystać z więcej niż dwóch dostawców dla wszystkich podstawowych usług, aby zminimalizować złożoność i poprawić wydajność...”²

Gartner

Jedna, globalna, kompleksowa usługa

Cloudflare



✓ Dostęp do sieci w modelu Zero Trust	✓ Tożsamość/Kontekst	✓ Zapobieganie zagrożeniom
✓ CASB	✓ Zasady dotyczące profilu urządzenia	✓ Zapobieganie utracie danych
✓ Bezpieczna bramka internetowa	✓ Kontrola dostępu oparta o rolę	✓ Wykrywanie aplikacji w chmurze
✓ Zapora sieciowa jako usługa	✓ Szyfrowanie/odszyfrowywanie	✓ Przyspieszenie SaaS
✓ WAN jako usługa	✓ Izolacja przeglądarki	✓ Ograniczenia geograficzne
✓ Buforowanie/CDN	✓ Ochrona DNS	✓ Zaciemnianie kodu/Prywatność
✓ Opcja middle mile cost	✓ WAF/WAAPaaS	✓ Ochrona Wi-Fi

Dlaczego klienci angażują Cloudflare do wdrożenia SASE

Prostota wdrożenia

Cloudflare dostarcza jednolitą i komponowalną platformę do łatwej konfiguracji i obsługi. Zgodne działanie usługi Cloudflare on-ramps oraz usług brzegowych wykorzystuje łączniki oparte wyłącznie na oprogramowaniu i jednorazowym integracjom. Daje to lepsze doświadczenia dla pracowników IT i użytkowników końcowych.

Odporność sieci

Nasza kompleksowa automatyzacja ruchu zapewnia niezawodną i skalowalną łączność sieciową ze stałą ochroną z dowolnej lokalizacji. W Cloudflare wszystkie usługi brzegowe są zbudowane tak, aby działały w każdej lokalizacji sieciowej, dostępnej dla każdego klienta, co wyróżnia Cloudflare na tle produktów innych dostawców zabezpieczeń.

Tempo innowacji

Architektura Cloudflare pozwala bardzo szybko tworzyć i dostarczać nowe funkcje zabezpieczeń i sieci, co daje pewność, że rozwiązania Cloudflare będą też dobre w przyszłości. Nasza przewaga w szybkim przyjmowaniu nowych standardów internetowych i bezpieczeństwa oraz budowaniu przypadków użycia dostosowanych do potrzeb klienta mówi sama za siebie, a nasza architektura zapewnia wyjątkowe możliwości wyboru.

Przejdź na szybszą, bardziej niezawodną i bezpieczniejszą sieć

Wypróbuj już teraz

Nie jesteś gotowy, aby wypróbować nasze usługi? Dowiedz się więcej o [Cloudflare One](#)

1. 2021 Gartner Strategic Roadmap for SASE Convergence 2. [Gartner Hype Cycle™ for Network Security, 2021](#)

GARTNER I HYPE CYCLE są zarejestrowanymi znakami towarowymi i znakami usługowymi firmy Gartner, Inc. i/lub jej spółek zależnych w Stanach Zjednoczonych i na całym świecie i są używane w niniejszym dokumencie za zgodą. Wszelkie prawa zastrzeżone.