Dyrygowanie na dużą skalę z SASE

Łączenie usług sieciowych i zabezpieczeń w jedną, harmonijną symfonię dostarczaną w chmurze.

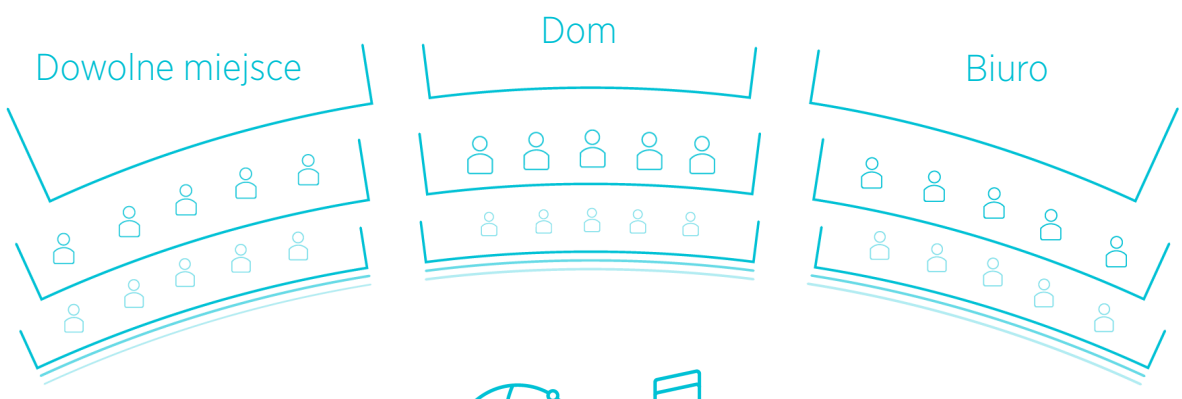
Secure Access Service Edge (SASE) to konwergencja sieci WAN i bezpieczeństwa w modelu usługi chmurowej, który umożliwia organizacjom połączenie użytkowników, aplikacji i zasobów – niezależnie od lokalizacji.

SASE zdobył uznanie wśród dostawców i użytkowników końcowych, otwierające przed nim rynek o wartości ponad 3 mld. USD.

*- Gartner**

Publiczność

Użytkownicy muszą w bezpieczny sposób łączyć się ze wszystkimi aplikacjami przedsiębiorstwa z dowolnego urządzenia, w dowolnym miejscu.



Orkiestra

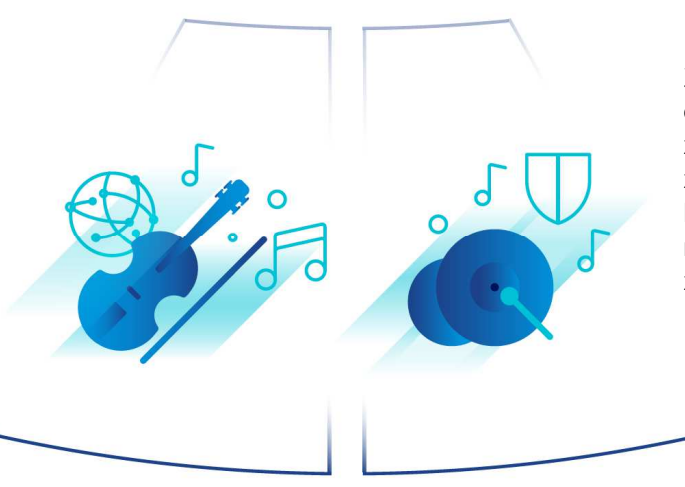
Elementy SASE harmonizują ze sobą jak sekcje orkiestry — wspólny koncert daje nowatorskie podejście w modelu chmurowym – dostarczanie aplikacji w najlepszej jakości, utrzymanie wewnętrznego bezpieczeństwa i prostota operacyjna.

SD-WAN

Software-Defined Wide Area Network (SD-WAN) rozdziela usługi sieciowe od infrastruktury bazowej, umożliwiając tym samym ruch aplikacji niezależnie od wykorzystywanych fizycznych lub transportowych komponentów.

Bezpieczny dostęp

Zero Trust Network Access (ZTNA) odejście od zabezpieczeń zorientowanych na brzegu sieci do zabezpieczeń opartych na tożsamości, lokalizacji i kontekście, które "nikomu nie ufa", udostępniając autoryzowane zasoby na żądanie.



Zabezpieczenia sieci Web w chmurze

Secure Web Gateway (SWG) wymusza kontrole oparte na zasadach/politykach w celu uzyskania dostępu do sieci, chroniąc tym samym przed złośliwym oprogramowaniem.

Cloud Access Security Broker (CASB) upewnia się czy wszystkie urządzenia końcowe są zgodne z polityką bezpieczeństwa przedsiębiorstwa w chmurze.

Data Loss Prevention (DLP) odnosi się do procesów i narzędzi, które chronią przed utratą i niewłaściwym wykorzystaniem danych wrażliwych lub przed dostępem przez nieautoryzowanych użytkowników.

Remote Browser Isolation (RBI) przenosi przeglądanie stron internetowych na zdalną lokalizację, a nie na urządzenie użytkownika, dzięki temu złośliwe oprogramowanie i wirusy nie mogą wejść do urządzenia lub sieci.

Zapora w chmurze

Intrusion Detection System (IDS) raportuje i sygnalizuje zagrożenia cyberbezpieczeństwa poprzez analizę ruchu sieciowego i kontrolę pakietów.

Intrusion Prevention System (IPS) proaktywnie zgłasza i zatrzymuje złośliwe oprogramowanie poprzez analizę pakietów sieciowych.

Firewall as a Service (FWaaS) zabezpiecza ruch sieciowy poprzez ustalone, scentralizowane polityki/zasady przedsiębiorstwa, występuje w formie usługi chmurowej.

Wykonawcy

Aplikacje są jak wykonawcy sceniczni – nawiązują kontakt z publicznością. Pełnię satysfakcji użytkowania można uzyskać tylko wtedy, gdy mamy bezproblemowy dostęp do aplikacji i są one bezpieczne.

Wraz z przeniesieniem usług do chmury i rozproszoną siłą roboczą komponenty SASE łączą się, aby zapewnić doskonałe bezpieczeństwo przedsiębiorstwa – od użytkownika do aplikacji — w dowolnym miejscu.

sdwan.vmware.com/sase

* Źródło: Gartner, Inc., Emerging Technologies: Applying SASE's Architectural Model to Secure Distributed Composite Apps, Joe Skorupa, Neil MacDonald, Anne Thomas, November 13, 2020

Autoryzowany Dystrybutor rozwiązań VMware w Polsce:

Arrow ECS Sp. z o.o.
ul. Sosnowiecka 79, 31-345 Kraków
tel. +48 12 616 43 00
e-mail: vmware.ecs.pl@arrow.com
www.arrow.com/ecs/pl/