LISTA KONTROLNA

Pięć niezbędnych elementów rozwiązania SASE

Udostępniane z chmury zabezpieczenia dla pracowników hybrydowych

Na przestrzeni ostatnich kilku lat organizacje rozszerzały swoje strategie sieciowe opierając je na obecności w wielu punktach brzegowych (multi-edge), aby umożliwiać obsługę pracy hybrydowej, w tym pracę zdalną z dowolnego miejsca (WFA) oraz wykorzystywanie aplikacji i środowisk chmurowych. W miarę jak proces ten postępuje i business adaptuje się do nowych warunków pracy, następuje jednocześnie zwiększenie powierzchni ataków.

W rezultacie rośnie luka między funkcjonalnością sieci a jej bezpieczeństwem, co z natury rzeczy zwiększa podatność organizacji na ataki i pogarsza środowisko pracy pracowników zdalnych, którzy nadal polegają na tradycyjnych metodach dostępu do sieci opartych wyłącznie na wirtualnej sieci prywatnej. Dzieje się tak zazwyczaj dlatego, że cały ruch aplikacji nadal musi być przesyłany do centrali na potrzeby uzyskania ochrony i realizacji kontroli dostępu.

W celu wyeliminowania tych problemów opracowano rozwiązania SASE (Secure Access Service Edge), które umożliwiają organizacjom szybką konwergencję i skalowanie dotychczasowych strategii w zakresie bezpieczeństwa i sieci. Dzięki nim można w bezpieczny sposób zarządzać rosnącą i dynamicznie zmieniającą się liczbą nowych punktów dostępu do sieci i spełniać nowe wymagania pracowników zdalnych i stacjonarnych, którzy pracują zarówno w ramach sieci firmowej, jak i poza nią.

Zdolność do realizacji tej nowej, rozproszonej i wymagającej dużej wydajności strategii ma obecnie fundamentalne znaczenie dla odniesienia sukcesu na dzisiejszym rynku cyfrowym. Wybór odpowiedniego dostawcy SASE może oznaczać różnicę między sukcesem operacyjnym a zmaganiem się z zapewnieniem odpowiedniego współdziałania wszystkich istotnych elementów tej strategii. Teoretycznie rozwiązanie SASE zapewnia użytkownikom WFA bezpieczny dostęp do chmury, nie wszystkie rozwiązania SASE są jednak równe pod względem skalowalności, bezpieczeństwa i orkiestracji. Najlepsze z nich nie powinny przyczyniać się bowiem do zwiększania kosztów ogólnych (wdrożenia, utrzymania), czy też do zwiększenia liczby pracowników IT odpowiedzialnych za takie wdrożenie i dalszą integrację z istniejącymi systemami.

Pięć najważniejszych wymagań związanych z wdrożeniem rozwiązania SASE

Rozważając wdrożenie każdego rozwiązania SASE, organizacje powinny kłaść nacisk na pięć następujących kluczowych elementów:

☑ Znalezienie pojedynczego dostawcy rozwiązań SASE zapewniającego elastyczność wdrożenia

Rozwiązanie SASE ma zapewniać bezpieczną łączność opartą na chmurze. Tymczasem bardzo mało sieci korporacyjnych działa wyłącznie w chmurze. Mimo że wiele przedsiębiorstw realizuje strategię wielochmurową, większość z nich nadal korzysta z sieci fizycznych. Oznacza to, że zabezpieczenie oparte wyłącznie na chmurze jest niepełne. Centrum danych i inne zasoby lokalne muszą być również chronione, a obowiązujące tam zasady bezpieczeństwa muszą być wdrażane i orkiestrowane w ramach ujednoliconej strategii bezpieczeństwa przy użyciu tych samych produktów i usług, które są stosowane w innych miejscach, w tym produktów i usług towarzyszących rozwiązaniu SASE.

Większość dostawców, którzy zapewniają tylko usługi bezpieczeństwa na brzegu sieci (SSE), ma ograniczone możliwości całościowego rozwiązywania kwestii bezpieczeństwa, ponieważ zajmują ich tylko kwestie związane z bezpieczeństwem dostępu do chmury. Organizacje muszą natomiast szukać usług SASE, które są zintegrowane z rozszerzoną siecią lub mogą być wdrażane jako jej płynne rozszerzenie (na przykład zabezpieczenia SD-WAN lub nawet integracja z sieciami LAN w celu zabezpieczenia mniejszych lokalizacji). Należy zatem nawiązać współpracę z takim dostawcą rozwiązań SASE, który od podstaw tworzy komponenty sieciowe i zabezpieczające. Uzyskana w ten sposób ujednolicona struktura bezpieczeństwa obniży całkowity koszt posiadania i poprawi użyteczność sieciową rozwiązania SASE.

Zapewnienie w całej sieci bezpieczeństwa klasy korporacyjnej

Skuteczne zabezpieczenia są podstawą każdego rozwiązania SASE. Organizacje muszą szukać takich funkcji, jak FaaS (Firewall-as-a-Service), która obsługuje różne protokoły, lub szybka inspekcja SSL. Ponadto niezbędny jest kompleksowy zestaw komponentów bezpieczeństwa do ochrony przed szerokim zakresem cyberzagrożeń. Komponenty te powinny obejmować:

- Ochronę DNS
- System ochrony przed włamaniami (IPS)
- Ochronę przed utratą danych (DLP)
- Bezpieczną bramę sieciową (SWG)
- Dostęp do sieci oparty na zasadzie zerowego zaufania (ZTNA)
- Bezpieczne środowisko testowe (Sandbox)
- Brokera zabezpieczeń dostępu do chmury (CASB)

Te środki bezpieczeństwa powinny być skalowalne i zapewniać zaawansowaną ochronę bez uszczerbku dla wydajności lub środowiska użytkownika.

Ujednolicona architektura z ujednoliconym agentem

Uproszczenie środowiska użytkownika przyczynia się do powszechnej akceptacji i przestrzegania procedur bezpieczeństwa. Ujednolicony agent, który konsoliduje funkcje zabezpieczeń punktów końcowych i ułatwia bezpieczne połączenia z aplikacjami w chmurze, usprawnia operacje i zwiększa zadowolenie użytkowników. Ujednolicone podejście zmniejsza złożoność i zapewnia spójne egzekwowanie zasad bezpieczeństwa we wszystkich punktach końcowych, niezależnie od ich lokalizacji lub metody dostępu.

Pełna konwergencja technologii sieciowych i zabezpieczających

Integracja funkcji sieciowych z funkcjami bezpieczeństwa ma kluczowe znaczenie dla płynnego działania rozwiązania SASE. Organizacje powinny priorytetowo traktować rozwiązania, które oferują płynną interoperacyjność między lokalną infrastrukturą bezpieczeństwa, taką jak SD-WAN lub zapory następnej generacji, a komponentami bezpieczeństwa opartymi na chmurze. Taka konwergencja ułatwia poprawę wydajności operacyjnej, zapewnienie zgodności z przepisami i osiągnięcie spójnego stanu bezpieczeństwa w rozproszonych sieciach.

Monitorowanie jakości pracy w środowisku cyfrowym w celu optymalizacji wydajności

Oprócz kwestii bezpieczeństwa, organizacje muszą priorytetowo traktować monitorowanie i optymalizację środowisk cyfrowych użytkowników końcowych. Obejmuje to monitorowanie wydajności w czasie rzeczywistym, śledzenie doświadczeń użytkowników końcowych i analizę wydajności aplikacji. Organizacje mogą proaktywnie identyfikować i eliminować wąskie gardła wydajności, aby zapewnić optymalną produktywność i zadowolenie użytkowników we wszystkich środowiskach sieciowych.

17 października 2024 3:53
2633753-0-0-EN