AlienVault USM Anywhere jest zunifikowanym rozwiązaniem bezpieczeństwa – służy do wykrywania cyberzagrożeń i odpowiedzi na incydenty.

Zalety USM Anywhere:
• z jednego miejsca monitoruje chmurę, hybrydę i środowisko lokalne
• jedna chmurowa konsola zapewnia pięć podstawowych funkcjonalności bezpieczeństwa
• niski współczynnik TCO dzięki eliminacji kosztów utrzymania centrów danych
• nowe możliwości orkiestracji i odpowiedzi (AlienApps, w chwili obecnej do Cisco Umbrella i McAfee ePO)

Korzyści wynikające z wykorzystania USM Anywhere:
• ułatwia ochronę zapewniając pięć podstawowych funkcjonalności bezpieczeństwa
• dzięki Open Threat Exchange (OTX) i Integrated Threat Intelligence pomaga w skalowaniu wykrywania zagrożeń i odpowiedzi na incydent
• uruchomia wykrywania w ciągu kilku minut
• zapewnia oszczędność czasu i pieniędzy

USM Anywhere w porównaniu z USM Appliance:
• monitoruje środowisko chmurowe Amazon AWS i Microsoft Azure; jest rozwiązaniem stworzonym do pracy natywnej w tych środowiskach
• rozwiązanie dostępne w modelu SaaS
• niewygórowane roczne opłaty subskrypcyjne
• daje nowe możliwości orkiestracji i odpowiedzi
• wbudowana aktywna pamięć typu „hot" do przechowywania danych przez 3 miesiące, pamięć długookresowa na 12 miesięcy
• wydajny, zaawansowany, graficzny silnik analityczny stwarza nowe możliwości korelacji i analityki

USM Anywhere sprawdzi się znakomicie tam gdzie:
- zespoły bezpieczeństwa cierpią na brak ekspertów i niedostatek narzędzi do monitorowania środowiska
- zespoły bezpieczeństwa pracują pod silną presją czasu, brak jest go na identyfikację i inwestygację zagrożeń oraz odpowiedź na zagrożenia
- firmowa infrastruktura i centra danych nieustannie się zmieniają np. w związku z migracją do chmury
- istnieje przekonanie, że ewoluujące zagrożenia oraz coraz bardziej skuteczne ataki oznaczają kompromitację naszych systemów i kradzieży naszych danych

Funkcjonalności USM Anywhere:
- **Asset Discovery** – wykrywa wszystkie zasoby tak w chmurze jak i w środowisku lokalnym i daje obraz ich podatności oraz aktywnych zagrożeń
- **Network Vulnerability Assessment** – wbudowane oprogramowanie do oceny podatności, oferujące wszystko czego trzeba do wglądu w bezpieczeństwo chmury, hybrydy czy środowiska lokalnego

- **Intrusion Detection System (IDS)** – wydajny system wykrywania intruzów i zintegrowana baza wiedzy o zagrożeniach przyśpiesza wykrywanie incydentów zarówno w chmurze jak i w środowisku lokalnym
- **Behavioral monitoring** – zbieranie danych pomaga w określeniu normalnego stanu pracy systemu i sieci, co z kolei umożliwia odpowiednią reakcję na incydenty
- **SIEM i Log Management** – wykracza poza tradycyjne rozwiązanie SIEM dzięki wbudowanym funkcjom bezpieczeństwa oraz bazy wiedzy, co daje szansę szybszego wykrywania zagrożeń w chmurze, hybrydzie czy środowisku lokalnym

Bezpieczeństwo:

- Bezpieczeństwo przesyłu danych – wszystkie dane wysyłane z infrastruktury klienta do AlienVault Secure Cloud są transferowane szyfrowanym połączeniem z USM Anywhere Sensor do USM Anywhere
- AlienVault ma wdrożone wskaźniki zgodności w odniesieniu do swoich usług chmurowych pozwalających udowodnić, iż instancje klientów, środowisko i obsługująca je infrastruktura są bezpieczne
- Dane każdego klienta są przechowywane w AlienVault Secure Cloud w odrębnym magazynie danych i są całkowicie izolowane od danych pozostałych klientów; każdy klient posiada swój własny klucz SSH do danych uwierzytelniających
- AlienVault gwarantuje, że dane klienta nie opuszczą kraju ich przechowywania; USM Anywhere przechowuje logi i zdarzenia w regionie wybranym przez Klienta; każdy z regionów obsługuje wiele odrębnych lokalizacji centrów danych, co zapewnia niezawodność usług w przypadku lokalnej utraty zasilania
- AlienVault wdrożył odpowiednie wskaźniki bezpieczeństwa konieczne do osiągnięcia zgodności z PCI DSS Service Provider Level 1 (SPL1)