AT&T Cybersecurity

AT&T Business

bako tech

USM Anywhere

Skuteczne wykrywanie zagrożeń i reagowanie na incydenty dla całej infrastruktury krytycznej

USM Anywhere™ zapewnia wydajne wykrywanie zagrożeń, reagowanie na incydenty i zarządzanie zgodnością w ramach jednej ujednoliconej platformy. Łączy w sobie najważniejsze funkcje bezpieczeństwa niezbędne do skutecznego monitorowania bezpieczeństwa w środowiskach chmurowych i lokalnych: wykrywanie zasobów, ocenę podatności, wykrywanie włamań, wykrywanie punktów końcowych, monitorowanie behawioralne, zarządzanie logami SIEM oraz ciągłą analizę zagrożeń.

Dzięki USM Anywhere możesz skupić się na tym, co najważniejsze - na ochronie infrastruktury IT przed współczesnymi zagrożeniami.

Wiele istotnych funkcji bezpieczeństwa w jednej platformie SaaS

USM Anywhere zapewnia wiele podstawowych funkcji bezpieczeństwa w jednym rozwiązaniu SaaS, dając Ci to, czego potrzebujesz do wykrywania zagrożeń, reagowania na incydenty i zarządzania zgodnością - wszystko z poziomu jednego pulpitu. Dzięki USM Anywhere można skupić się na wykrywaniu zagrożeń i reagowaniu na nie, a nie na zarządzaniu oprogramowaniem.

USM Anywhere to elastyczne, oparte na chmurze rozwiązanie w zakresie bezpieczeństwa, które można łatwo skalować, aby sprostać potrzebom w zakresie wykrywania zagrożeń, jak również zmian i rozbudowy środowiska IT.

Wykrywanie aktywów

- Wykrywanie aktywów z wykorzystaniem API
- Wykrywanie zasobów sieciowych
- Wykrywanie oprogramowania i usług

Ocena podatności na zagrożenia

- Skanowanie podatności sieci
- Skanowanie podatności w chmurze
- Ocena infrastruktury w chmurze

Monitorowanie behawioralne

- Logi dostępu do zasobów
- Dzienniki dostępu i aktywności w chmurze (Microsoft Azure® Monitor, AWS®: CloudTrail®, CloudWatch, S3, ELB)
- Monitorowanie przepływu VPC AWS
- Logi dostępu do VMware® ESXi

Wykrywanie włamań

- Wykrywanie włamań do sieci (NIDS)
- Wykrywanie włamań w chmurze

Funkcjonalności EDR

- Wykrywanie włamań w oparciu o hosta (HIDS)
- Monitorowanie integralności plików
- Ciągłe monitorowanie punktów końcowych i proaktywne reagowanie

SIEM i zarządzanie logami

- Korelacja zdarzeń
- Zarządzanie logami
- Reagowanie na incydenty
- Zintegrowane informacje o zagrożeniach pochodzące od zespołu bezpieczeństwa AT&T Alien Labs™ i Alien Labs Open Threat Exchange® (OTX™)

Kluczowe cechy produktu i najważniejsze informacje

• Scentralizowane monitorowanie bezpieczeństwa dla chmury i środowisk lokalnych

USM Anywhere zapewnia potężne możliwości wykrywania zagrożeń w chmurze i środowisku lokalnym, pomagając wyeliminować martwe punkty w zabezpieczeniach i ograniczyć niezarządzane działania shadow IT. Nawet podczas migracji usług z centrum danych do chmury można korzystać z praktycznie bezproblemowej widoczności poziomu bezpieczeństwa.

• Zautomatyzowana orkiestracja odpowiedzi

USM Anywhere zapewnia zaawansowane reguły bezpieczeństwa, które automatyzują działania i reakcje i odpowiedzi zgodnie z potrzebami użytkownika, dzięki czemu praca staje się bardziej wydajna.

• Zaawansowana analityka bezpieczeństwa w zasięgu ręki

Kiedy centralizujesz monitorowanie bezpieczeństwa wszystkich środowisk IT w chmurze i w siedzibie firmy, potrzebujesz wysoce wydajnego sposobu wyszukiwania i analizowania dużych ilości danych z całej złożonej i dynamicznie zmieniającej się infrastruktury IT. USM Anywhere zapewnia intuicyjny i elastyczny interfejs do wyszukiwania i analizowania danych związanych z bezpieczeństwem.

• Zbudowane natywnie w chmurze dla chmury

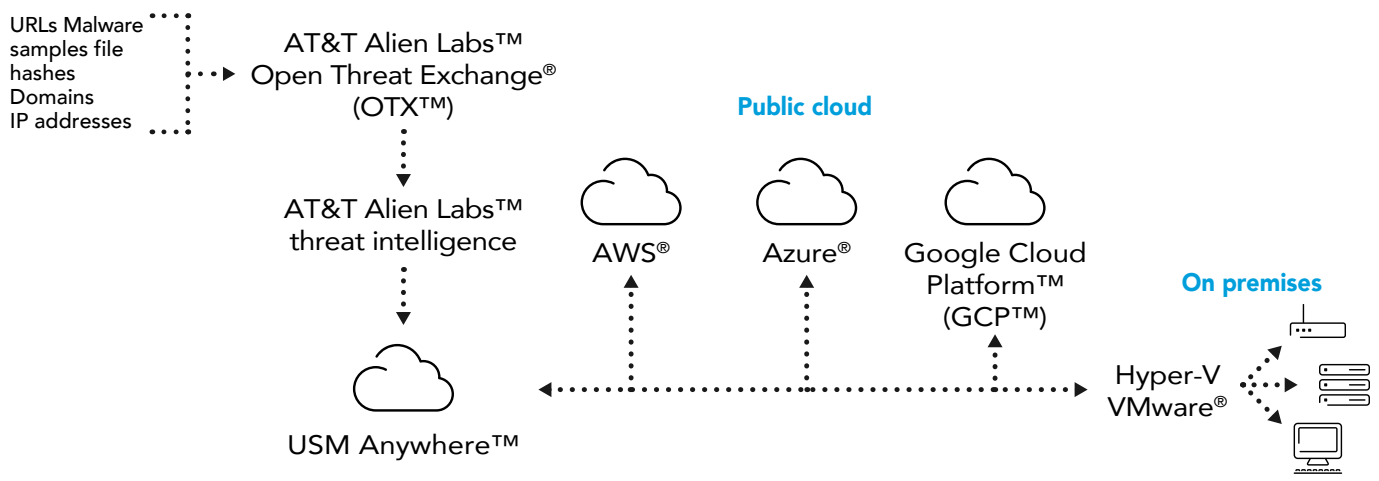
W przeciwieństwie do innych starszych rozwiązań bezpieczeństwa, które zostały zmodyfikowane do pracy w chmurze, USM Anywhere to prawdziwie natywne rozwiązanie do monitorowania bezpieczeństwa w chmurze, które wykorzystuje unikalne elementy bezpieczeństwa infrastruktury chmury publicznej. Wykorzystuje ono bezpośrednie połączenia z interfejsami API chmury, aby zapewnić bogatszy zestaw danych, większą kontrolę nad bezpieczeństwem infrastruktury chmury i aplikacji SaaS oraz bardziej natychmiastowy wgląd w całe środowisko już w ciągu kilku minut od instalacji.

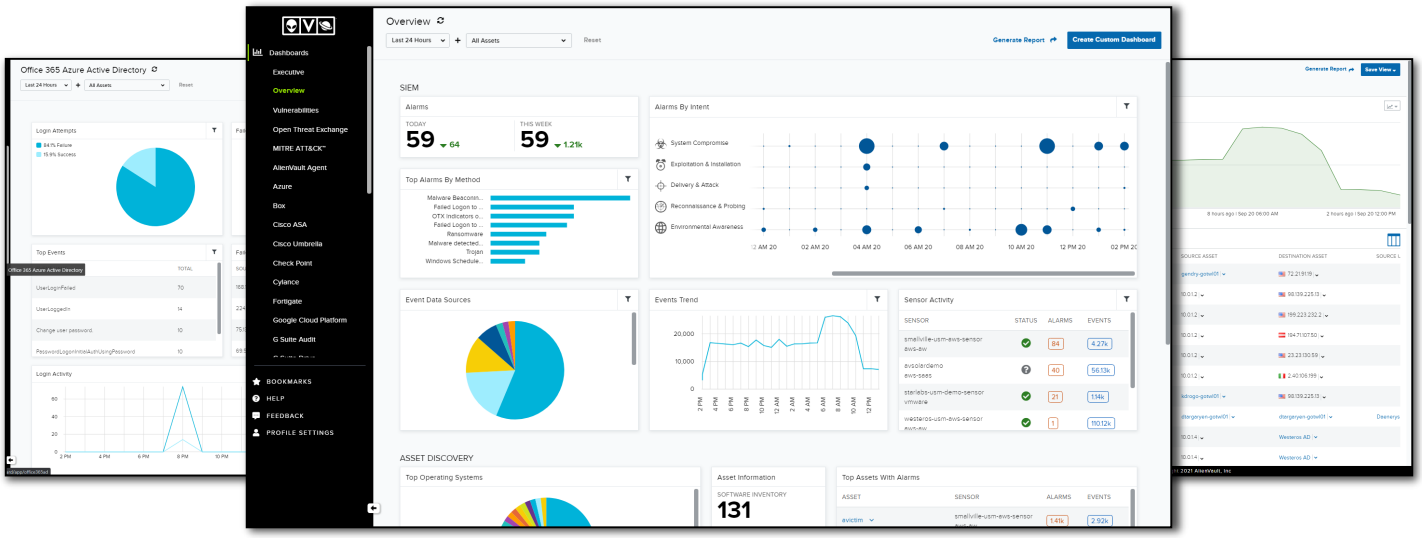
• Zaawansowany silnik analityczny

USM Anywhere to udoskonalone podejście do korelacji zdarzeń SIEM, które sprawia, że analiza bezpieczeństwa jest szybsza, bardziej elastyczna i skuteczniejsza niż kiedykolwiek.

• Rozszerzona orkiestracja bezpieczeństwa z AlienApps

USM Anywhere to platforma, która wykorzystuje AlienApps™, czyli integracje z narzędziami bezpieczeństwa i produktywności innych firm - w celu rozszerzenia możliwości orkiestracji zabezpieczeń.





Wdrażanie USM Anywhere jest szybkie i łatwe

USM Anywhere składa się z wysoce skalowalnej, dwupoziomowej architektury do zarządzania i monitorowania bezpieczeństwa w chmurze i w siedzibie firmy. Czujniki USM Anywhere i agenci USM Anywhere zbierają i normalizują dane z chmury i środowisk lokalnych, a następnie przesyłają je do USM Anywhere w celu scentralizowanego gromadzenia, analizy bezpieczeństwa, wykrywania zagrożeń i zarządzania logami zgodnymi z regulacjami. Jedyną rzeczą, którą wdrażasz w swoim środowisku są sensory i agenci. AT&T Cybersecurity automatycznie utrzymuje i aktualizuje USM Anywhere.

Od instalacji do wglądu w bezpieczeństwo w 3 prostych krokach:

1. Wdrażanie czujnika USM Anywhere w chmurze lub w środowisku lokalnym. Wprowadź klucz licencyjny sensora dostarczony przez AT&T Cybersecurity, a następnie skieruj sensor na dedykowany adres URL USM Anywhere.

2. Zaloguj się na swoje konto USM Anywhere, aby wdrażać agentów USM Anywhere i zarządzać nimi, uruchamiać wykrywanie zasobów i skanowanie podatności oraz wiele innych funkcji.

3. Rozpocznij monitorowanie zagrożeń i złośliwych działań. Z poziomu USM Anywhere można wyszukiwać i analizować dane oraz zarządzać reakcjami bezpieczeństwa i alarmami.

Rozwiązanie USM Anywhere, stworzone z myślą o współczesnych zespołach ds. bezpieczeństwa IT dysponujących ograniczonymi zasobami, jest bardziej przystępne cenowo, szybsze do wdrożenia i łatwiejsze w obsłudze niż tradycyjne rozwiązania. Eliminuje konieczność wdrażania, integrowania i utrzymywania wielu punktowych rozwiązań bezpieczeństwa. USM Anywhere to platforma oparta na chmurze, dostarczana jako usługa, która oferuje niski całkowity koszt posiadania (TCO) oraz elastyczne, skalowalne opcje wdrażania dla zespołów o dowolnej wielkości i budżecie.

Zintegrowane informacje o zagrożeniach dla lepszej ochrony

USM Anywhere otrzymuje ciągłe aktualizacje informacji o zagrożeniach od zespołu badawczego do spraw bezpieczeństwa Alien Labs. Ten dedykowany zespół spędza niezliczone godziny na badaniu i analizowaniu różnych typów ataków, pojawiających się zagrożeń, luk w zabezpieczeniach i exploitów, dzięki czemu Ty nie musisz tego robić.

Dodatkowo, Alien Labs wykorzystuje informacje o zagrożeniach pozyskiwane przez społeczność z Open Threat Exchange (OTX). OTX™ to największa na świecie giełda informacji o zagrożeniach pozyskiwanych przez społeczność, zapewniająca Ci bezpieczeństwo, które jest zasilane przez globalną społeczność badaczy zagrożeń i specjalistów ds. bezpieczeństwa.

AlienLabs analizuje feedy OTX za pomocą potężnego silnika, który jest w stanie badać potencjalne zagrożenia w czasie rzeczywistym. Sam OTX zapewnia otwarty dostęp do globalnej społeczności badaczy zagrożeń i profesjonalistów zajmujących się bezpieczeństwem. Obecnie zrzesza ponad 100 000 uczestników w 140 krajach, którzy codziennie dostarczają ponad 19 IoC.

W rezultacie Twoje środowisko USM Anywhere korzysta z najnowszych informacji o pojawiających się zagrożeniach, aby pomóc w zapewnieniu ochrony Twojej organizacji.

Bakotech | Oficjalny Dystrybutor AT&T Cybersecurity

Bakotech Sp. z o.o. z siedzibą w Krakowie, jest częścią międzynarodowej grupy dystrybucyjnej Bakotech®.

Jako specjalizowany dystrybutor rozwiązań IT w zakresie bezpieczeństwa, sieci i infrastruktury IT, spółka koncentruje się na dostarczaniu najwyższej jakości produktów i usług w centralnej i wschodniej Europie, w szczególności w: Polsce, Bułgarii, Rumunii, Słowacji, Chorwacji i na Węgrzech, a także w krajach nadbałtyckich. Firma zajmuje się sprzedażą w kanale partnerskim, poprzez rozbudowaną sieć partnerów. Bakotech posiada w swoim portfolio innowacyjne produkty, które odniosły sukces międzynarodowy, a dzięki dystrybutorowi wchodzą nie tylko na rynek Polski, ale również do krajów Europy Środkowo-Wschodniej.

Skontaktuj się z nami:

www.bakotech.pl
alienvault@bakotech.pl
+48 12 340 90 30

Drukarska 18/5
30-348 Kraków

bako tech®

@bakotechpl
@bakotechpl
Bakotech Poland&CEE