Zaawansowane uwierzytelnianie dla Twojej firmy

Zaawansowane uwierzytelnianie w kilku słowach:

+ jeden system spełniający wszystkie potrzeby związane z uwierzytelnianiem;
+ elastyczność łączenia dzięki metodzie „mix-and-match";
+ obsługa wielu różnorodnych integracji (RADIUS, VPN, OpenID, OATH, FIDO, RACF Windows, Mac OS, Linux, Citrix, VMWare itp.).

Elastyczna konstrukcja dopasowana do Twojego środowiska

Firmy korzystające z wielu zaawansowanych rozwiązań uwierzytelniających muszą utrzymywać wiele infrastruktur i nimi zarządzać. Takie podejście jest bardzo kosztowne i powoduje wiele trudności z administrowaniem, a także jest mniej bezpieczne. Potrzebujesz jednego rozwiązania do wszystkiego. Korzystanie z jednego systemu umożliwia kontrolowanie uwierzytelniania za pomocą łatwych do skonfigurowania zasad w jednej konsoli, co jest istotne, jeśli użytkownik lub grupa użytkowników zmienia stanowiska lub odchodzi z firmy.

Dzięki różnorodnym, gotowym do użycia integracjom aplikacji (m.in. RADIUS, VPN, OpenID, OATH, FIDO, RACF Windows, Mac OS, Linux, Citrix i VMware) zaawansowane uwierzytelnianie zapewnia wiele możliwości zastosowania dla Twojego środowiska. Co więcej, obsługa wielu czytników i metod uwierzytelniania pozwala osiągnąć niespotykaną dotąd elastyczność. Nasz system zaawansowanego uwierzytelniania został zaprojektowany z myślą o wysokiej dostępności i wewnętrznym równoważeniu obciążenia, co zapewnia ciągłe działanie niezależnie od wielkości środowiska. Replikacja pomiędzy głównymi i pomocniczymi serwerami umożliwia integrację danych i odtwarzanie po awarii (poprzez sieci LAN lub WAN).

Bezpieczne udostępnianie informacji

W związku ze zmianami dokonywanymi przez firmy w architekturze wewnątrz skomplikowanych środowisk hybrydowych łatwość wdrażania aplikacji i ich dystrybucja są ważniejsze niż kiedykolwiek. Właśnie dlatego system zaawansowanego uwierzytelniania jest teraz dostępny w postaci kontenerów Docker. Wszystkie zależności znajdują się w małych zestawach kontenerów Docker, dzięki czemu przenoszenie nie powoduje żadnych problemów ze zgodnością. Z tego powodu kontenery Docker to zalecane urządzenia dla środowisk chmurowych, takich jak Amazon Web Services (AWS). System zaawansowanego uwierzytelniania w formie kontenerów wykorzystuje technologie wirtualizacji i technologie oparte na chmurze, które najlepiej odpowiadają Twoim potrzebom. System ten można również skonfigurować w specjalistycznych modelach zoptymalizowanych pod kątem wydajności lub dostępności. Podsumowując, nasz system Advanced Authentication w wersji 6 lub nowszej umożliwia:

- łatwiejsze wdrożenie;
- prostsze śledzenie wersji i przywracanie określonych wcześniejszych wersji;
- łatwiejszą konserwację dzięki wyeliminowaniu większości trudności związanych z problemami z zależnościami aplikacji.

Zaawansowane uwierzytelnianie dla osób poza siecią

Osoby pracujące mobilnie często znajdują się w miejscach, w których nie mogą podłączyć się do standardowych źródeł uwierzytelniania. Choć bezpieczeństwo jest niezwykle istotne, wydajność ma jeszcze większe znaczenie. Nie może dochodzić do sytuacji, w których użytkownicy nie mają możliwości wykonywania swoich zadań lub świadczenia usług klientom. System zaawansowanego uwierzytelniania obsługuje uwierzytelnianie offline, które umożliwia użytkownikom przeprowadzanie dwuskładnikowego uwierzytelniania – lub jakiegokolwiek innego silnego uwierzytelniania – w dowolnym miejscu, niezależnie od tego, czy są podłączeni, czy nie.

Połączenie systemu zaawansowanego uwierzytelniania z Twoimi obecnymi aplikacjami pozwala na pewne potwierdzanie tożsamości użytkowników. Skorzystaj z uwierzytelniania, które zapewnia ochronę dopasowaną do ryzyka.

Obsługa U2F

Firma Micro Focus to aktywny członek organizacji FIDO (Fast Identity Online). Standard FIDO U2F (Universal 2nd Factor) umożliwia firmom obsługę środowisk, w których użytkownicy zarządzają swoimi własnymi urządzeniami do uwierzytelniania. Advanced Authentication to stabilny system zapewniający obsługę aplikacji bez konieczności ich zmieniania. Pozwala uniknąć kosztów związanych z wykorzystywaniem tokenów, a użytkownicy cenią to rozwiązanie za zwiększenie bezpieczeństwa innych aspektów ich cyfrowego życia. System zaawansowanego uwierzytelniania zapewnia wszechstronne wsparcie dla aplikacji oraz niskie całkowite koszty użytkowania. Nie istnieje lepszy system zapewniający środowisko uwierzytelniania U2F.

Skuteczne uwierzytelnianie na wszystkich platformach

W świecie, w którym użytkownicy korzystają z szerokiej gamy urządzeń, skuteczne uwierzytelnianie na wielu platformach jest ważniejsze niż kiedykolwiek wcześniej. System Advanced Authentication zapewnia wieloskładnikowe uwierzytelnianie dla platform z systemami Windows (komputery stacjonarne / serwery), OS X i Linux. Można również skorzystać z metod uwierzytelniania opartych na systemach iOS, Android i Windows Mobile w celu zabezpieczenia dostępu do tych systemów.

Skuteczne uwierzytelnianie dla oprogramowania Active Directory Federation Services (ADFS)

Jako że firmy coraz częściej wybierają platformy Office 365 i Microsoft Azure, ADFS cały czas się rozwija. To ważne, aby firmy dopasowywały siłę uwierzytelniania do ryzyka. W takich sytuacjach system Advanced Authentication chroni dostęp do Twojego środowiska za pomocą konsolidacji i integracji, ułatwiając użytkownikom korzystanie z tego rozwiązania oraz umożliwiając bardziej zaawansowaną weryfikację dzięki wieloskładnikowemu uwierzytelnianiu (MFA). Oznacza to, że oprogramowanie Advanced Authentication pozwala lepiej chronić systemy ADFS przed nieupoważnionym dostępem, niezależnie od tego, czy aplikacje działają lokalnie, czy w chmurze.

Dlaczego warto nas wybrać

Dzięki zastosowaniu skonsolidowanego podejścia polegającego na wieloskładniowemu uwierzytelnianiu obsługa i konserwacja systemu Advanced Authentication są łatwiejsze niż w przypadku innych rozwiązań. Naszą mocną stroną są również nieszablonowe integracje zapewniające wiele opcji uwierzytelniania. Cała Twoja firma będzie czerpała korzyści ze zwiększonego bezpieczeństwa i łatwiejszej obsługi. Możesz swobodnie tworzyć nowe infrastruktury MFA lub zastępować i konsolidować starsze. Umożliwia to kontrolowanie wydatków i maksymalizację zwrotu z inwestycji. Niższe koszty i zwiększona ochrona sprawiają, że system Advanced Authentication to wiodące na rynku rozwiązanie.

Więcej informacji o systemie Advanced Authentication firmy Micro Focus® oraz oprogramowanie do testów można znaleźć na stronie **www.netiq.com/advanced-authentication**

Skontaktuj się z nami:
www.microfocus.com