One Identity Safeguard for Privileged Passwords

Automatyzacja, kontrola i zabezpieczenie procesu nadawania uprzywilejowanych poświadczeń

Korzyści

- Zapobieganie naruszeniom bezpieczeństwa dzięki pełnej kontroli kont uprzywilejowanych

- Zapewnienie zgodności z przepisami i regulacjami (compliance) w zakresie uprzywilejowanego dostępu

- Szybkie uzyskanie efektów dzięki uproszczonemu wdrożeniu i prostej obsłudze

- Maksymalizacja produktywności dzięki niewielkiej krzywej uczenia się i przejrzystemu interfejsowi użytkownika

- Proste i szybkie tworzenie raportów na potrzeby audytu

Wprowadzenie

Coraz częściej występujące i ujawniane incydenty naruszenia bezpieczeństwa w organizacjach pokazują, że hasła do kont uprzywilejowanych są najbardziej wrażliwym elementem systemów - przy tym bardzo podatnym na zagrożenia i najgroźniejszym dla bezpieczeństwa organizacji. Hasła te pokonują zabezpieczenia i otwierają wszystkie drzwi. Kiedy wpadną w ręce hakerów, dają im nieograniczony dostęp do systemów i danych. Skutki takiego działania mogą być katastrofalne dla organizacji, a koszty utraconej własności intelektualnej i reputacji ogromne.

Tradycyjnie, zabezpieczenie uprzywilejowanych poświadczeń powodowało konflikt między bezpieczeństwem a działalnością biznesową organizacji i spowalniało produktywność zarówno codziennych, jak i długoterminowych procesów. Zadanie to często stawiało menedżerów IT i specjalistów bezpieczeństwa w niefortunnym położeniu i zmuszało ich do dokonywania wyboru pomiędzy bezpieczeństwem a użytecznością. Tak było do teraz. Dzięki One Identity Safeguard for Privileged Passwords można mieć i jedno, i drugie.

Rozwiązanie automatyzuje, kontroluje i zabezpiecza proces nadawania uprzywilejowanych poświadczeń za pomocą zarządzania dostępem w oparciu o role oraz wykorzystując zautomatyzowane przepływy pracy. One Identity Safeguard for Privileged Passwords jest dostarczane w zabezpieczonym urządzeniu, co stanowi dodatkową ochronę przed nieautoryzowanym dostępem do samego rozwiązania oraz pomaga przyspieszyć integrację z systemami IT organizacji. Przejrzysty interfejs użytkownika wpływa na małą krzywą uczenia się i zapewnia możliwość zarządzania hasłami z dowolnego miejsca i przy użyciu praktycznie dowolnego urządzenia. W rezultacie rozwiązanie zapewnia uprzywilejowanym użytkownikom nowy poziom swobody i funkcjonalności, jednocześnie efektywnie zabezpieczając organizację.

Quest Dystrybucja Sp. z o.o.
ul. Ślężna 104, 53-111 Wrocław
tel. 71 356 49 40
Info@quest-pol.com.pl

Centrum Kompetencyjne
ul. Nabielaka 6, 00-743 Warszawa
tel. 22 160 51 77
www.quest-pol.com.pl

Główne cechy

Kontrola przydzielania haseł

Pozwala wydajnie zarządzać żądaniami haseł od uprawnionych użytkowników do kont, do których mają prawo dostępu. Proces ten odbywa się za pomocą bezpiecznego połączenia przeglądarki internetowej, również ze wsparciem urządzeń mobilnych.

Workflow Engine

Silnik przepływu pracy, który wspiera ograniczenia czasowe, rewidentów (reviewers), różne osoby zatwierdzające, dostęp awaryjny i wygaśnięcie polityk. Obejmuje również możliwość wprowadzania kodów przyczyny i/lub bezpośredniej integracji z systemami ticketowymi. Żądanie hasła może być zatwierdzone automatycznie lub manualnie z dodatkowymi poziomami uwierzytelnienia.

Wykrywanie

Umożliwia szybkie wykrywanie uprzywilejowanych kont lub systemów w sieci z dodatkowymi opcjami wykrywania hostów, katalogów i sieci.

Zatwierdzanie z dowolnego miejsca

Wykorzystując One Identity Starling, można z dowolnego miejsca zatwierdzić lub odrzucić żądanie hasła, bez konieczności logowania się do sieci VPN.

Ulubione (Favorites)

Bezpośrednio z ekranu logowania zapewnia szybki dostęp do często używanych haseł.

Zawsze online

Rozwiązanie zapewnia wysoką dostępność, ponieważ zostało zaprojektowane dla klasteryzacji rozproszonej. Ponadto funkcja równoważenia obciążenia gwarantuje wyższą przepustowość i krótsze czasy odpowiedzi na żądania haseł lub sesji realizowane z dowolnego urządzenia.

RESTful API

Safeguard for Privileged Passwords używa zmodernizowanego interfejsu API opartego na REST do łączenia się z innymi aplikacjami i systemami. Każda funkcja jest udostępniana za pośrednictwem interfejsu API, aby umożliwić szybką i łatwą integrację, niezależnie od tego, co chcesz zrobić lub w jakim języku są napisane Twoje aplikacje.

Centrum Aktywności (Activity Center)

Pozwala szybko i łatwo przeglądać całą aktywność za pomocą narzędzia do tworzenia zapytań. W zależności od tego, kto zażądał raportu (np. personel IT lub kierownictwo), można dodawać i usuwać dane, aby uzyskać tylko potrzebne informacje. Możliwe jest także ustalanie harmonogramów dla zapytań oraz zapisywanie lub eksportowanie danych w wielu różnych formatach.

Wsparcie uwierzytelniania dwuskładnikowego

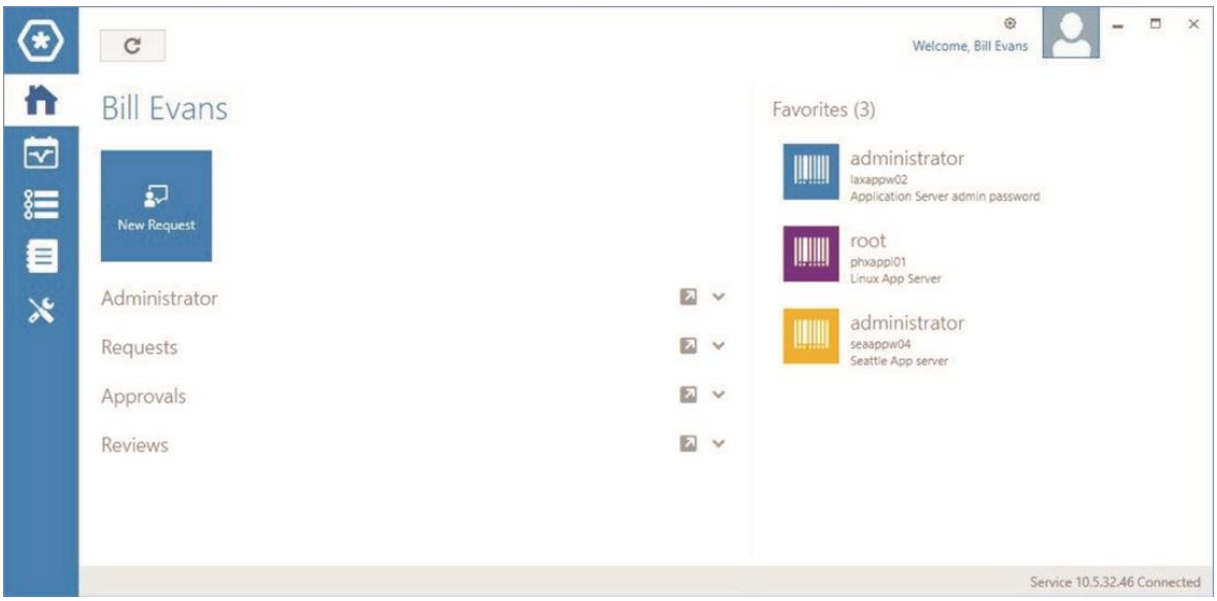
Ochrona dostępu do haseł za pomocą innego hasła nie jest wystarczająca. Dlatego One Identity Safeguard for Privileged Passwords zapewnia uwierzytelnianie dwuskładnikowe (2FA). Obsługuje wszystkie rozwiązania 2FA oparte na RADIUS i zawiera 25 darmowych licencji usługi uwierzytelniania 2FA One Identity - Starling TwoFactor Authentication.

Obsługa kart inteligentnych (smartcard)

Wsparcie dodatkowych, silnych metod uwierzytelniania, które zapewniają bezpieczny dostęp do systemów.

Quest Dystrybucja Sp. z o.o.
ul. Ślężna 104, 53-111 Wrocław
tel. 71 356 49 40
Info@quest-pol.com.pl

Centrum Kompetencyjne
ul. Nabielaka 6, 00-743 Warszawa
tel. 22 160 51 77
www.quest-pol.com.pl



Funkcja Favorites (Ulubione) zapewnia szybki dostęp do często używanych haseł bezpośrednio z ekranu logowania.

Rozwiązania One Identity do zarządzania uprzywilejowanym dostępem

One Identity oferuje w swoim portfolio produktowym najbardziej wszechstronny zestaw rozwiązań do zarządzania uprzywilejowanymi kontami, który można dostosować do potrzeb każdej organizacji. Wykorzystując szerokie możliwości zarządzania sesjami uprzywilejowanymi Safeguard for Privileged Sessions oraz dodatkowe funkcje Safeguard for Privileged Passwords do zarządzania hasłami uprzywilejowanymi, można zbudować kompletne rozwiązanie do kontroli, zabezpieczenia i analizowania dostępu uprzywilejowanego. Szeroka oferta produktowa One Identity obejmuje także rozwiązania do granularnej delegacji kont root systemu Unix oraz kont administratora Active Directory; wtyczki, które umożliwiają przygotowanie rozwiązań klasy enterprise w oparciu o rozwiązania open source sudo; Keylogger (rejestrowanie naciśnięć klawiszy) dla aktywności konta root Unix - wszystko to ściśle zintegrowane z wiodącym rozwiązaniem do połączenia z Active Directory.

One Identity

Rodzina rozwiązań One Identity do zarządzania tożsamością i dostępem zapewnia organizacjom pełne wsparcie w zakresie IAM, oferując modułowe, zintegrowane, skoncentrowane na celach biznesowych i gotowe na przyszłe wyzwania organizacji rozwiązania Identity Governance, Access Management i Privileged Account Management.

Quest Dystrybucja Sp. z o.o. jest Value Added Dystrybutorem oraz Partnerem Wsparcia Technicznego firmy One Identity na terenie Polski.

Quest Dystrybucja Sp. z o.o.
ul. Ślężna 104, 53-111 Wrocław
tel. 71 356 49 40
Info@quest-pol.com.pl

Centrum Kompetencyjne
ul. Nabielaka 6, 00-743 Warszawa
tel. 22 160 51 77
www.quest-pol.com.pl