sectona

bako tech

Sectona Security Platform

Lekkie, zintegrowane podejście do zarządzania dostępem uprzywilejowanym

Sectona Security Platform pomaga przedsiębiorstwom ograniczać ryzyko ataków ukierunkowanych na konta uprzywilejowane. Sectona dostarcza zintegrowane komponenty do zarządzania uprawnieniami, które rozwiązują wyzwania związane z dostępem do nowoczesnej, dynamicznej komunikacji między pracownikami i maszynami w infrastrukturze IT oraz zarządza uprawnieniami dla stacji roboczych rozsianych po środowiskach lokalnych, wirtualnych lub w chmurze.

Zarządzanie uprawnieniami z dowolnego miejsca

Zabezpieczenie haseł za pomocą zintegrowanej platformy dla punktów końcowych i aplikacji.

Skalowalne zarządzanie sesjami

Międzyplatformowa technologia do zarządzania sesjami dla punktów końcowych, w przeglądarce lub na serwerze terminalowym.

Budowa z myślą o skali i bezpieczeństwie

Wdrażanie i zarządzanie platformą z wbudowanymi opcjami wysokiej dostępności, modułowymi komponentami i wsparciem dla rozproszonej architektury.

Zastosowanie

Bezpieczny dostęp dla osób uprzywilejowanych

Izolacja sesji uprzywilejowanych, zarządzanie złożonymi zasadami dostępu z dynamicznym grupowaniem, obsługa użytkowników uzyskujących dostęp z nieznanej sieci.

Usuwanie uprawnień administratora

Blokowanie uprawnień na punktach końcowych, zwiększanie uprawnień na żądanie, blokowanie uruchamiania nieznanych aplikacji.

Bezpieczne środowiska chmurowe

Zarządzanie tożsamością i uwierzytelnianiem, przyspieszenie procesu onboardingu, umożliwienie zdalnego dostępu bez VPN.

Automatyzacja przeglądów uprawnień

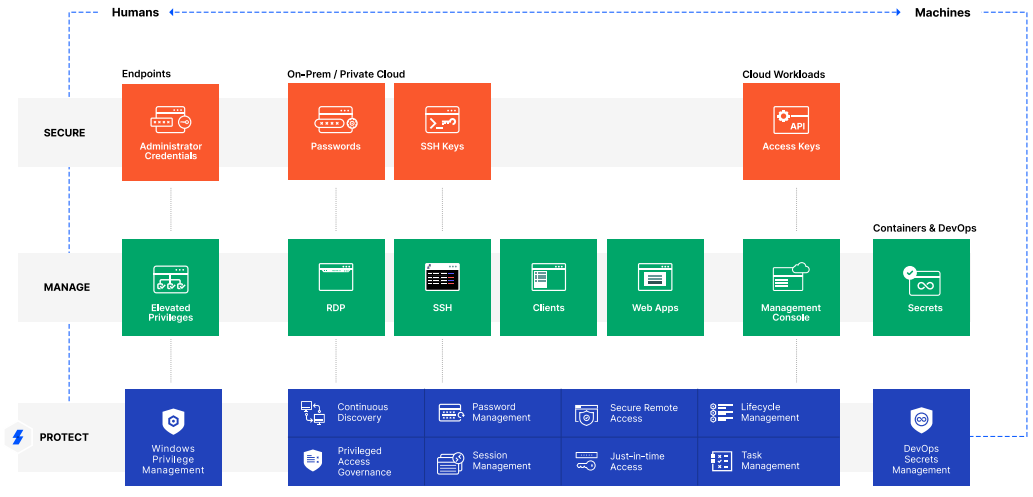
Scentralizowany monitoring przydziału i wykorzystania uprawnień, ustalanie własności kluczowych kont.

Uproszczenie dostępu do uprawnień

Automatyzacja dostarczania kont uprzywilejowanych, elastyczne operacje zarządzania kontami.

Przegląd platformy

Sectona Security Platform łączy elementy zabezpieczające uprawnienia na rosnących powierzchniach ataków organizacji. Ścisła integracja w ramach platformy dla zespołów ds. operacji IT, bezpieczeństwa i zarządzania zapewnia spójne zarządzanie uprawnieniami w chmurze, środowisku wirtualnym i dla punktów końcowych. Kompletna platforma opracowana od podstaw, domyślnie zintegrowana, zapewniająca niezwykłą łatwość użytkowania i prostotę administracji.



Możliwości platformy

Dostosuj się do dynamicznych potrzeb i wyzwań, korzystając z prostej i skalowalnej, zintegrowanej platformy. Sectona Security Platform składa się z podstawowych funkcji zarządzania hasłami i sesjami dla zespołów ds. operacji i bezpieczeństwa IT. Zaawansowane funkcje ukierunkowane są na zarządzanie uprawnieniami dla punktów końcowych.

Funkcjonalności podstawowe

Stałe monitorowanie
Zabezpiecz i kontroluj nowo dodane zasoby i ukryte konta uprzywilejowane.

Zarządzanie hasłami
Przechowuj hasła, by zabezpieczyć tożsamości uprzywilejowanych i kluczy SSH.

Bezpieczny dostęp zdalny
Włącz zdalny dostęp bez VPN dla pracowników, niezależnie od miejsca ich pracy.

Nagrywanie sesji i analiza zagrożeń
Monitoruj sesje dla wszystkich uprzywilejowanych działań z profilowaniem ryzyka i analizą opartą na zachowaniu.

Uwierzytelnianie wieloskładnikowe (MFA)
Zneutralizuj ryzyko związane z naruszonymi danymi uwierzytelniającymi, korzystając z szerokiego zestawu mechanizmów.

Dostęp Just-In-Time
Usuń stałe uprawnienia i wykorzystaj możliwość wdrożenia zasad JIT.

Zarządzanie uprawnieniami
Automatycznie nadawaj i zarządzaj uprawnienie.

Zarządzanie cyklem życia konta
Usprawniaj zarządzanie cyklem życia uprzywilejowanych kont grup w heterogenicznej infrastrukturze.

Funkcjonalności zaawansowane

Zarządzanie dostępem uprzywilejowanym
Zarządzaj uprawnieniami uprzywilejowanymi i dostępem do platformy, aby zabezpieczyć i zachować zgodność.

Zarządzanie uprawnieniami okien
Kontroluj i chroń użycie konta administratora w systemie Windows, kontroluj podwyższone uprawnienia dla użytkowników Windows.

Zarządzanie sekretami DevOps
Chroń sekrety zespołów poprzez stosowanie praktyk DevOps, by uzyskać dostęp do aplikacji i usług, wyeliminować zakodowane poświadczenia i rejestrować wszystkie uprzewilejowane sesje.

Kluczowe cechy

- Integracja więcej niż RDP i SSH, integracja specjalistycznych klientów i narzędzi z DIY Plugin Development Kit.
- Wykorzystanie technologii zarządzania sesjami, aby zabezpieczyć każdą sesję, izolując punkty końcowe dla sesji uprzywilejowanych.
- Zintegrowane zarządzanie dostępem uprzywilejowanym.
- Zabezpieczanie haseł, kluczy SSH i sekretów w specjalnie zbudowanym skarbcu obsługiwanym tylko przez autoryzowany dostęp za pośrednictwem PAM i interfejsów API.
- Wbudowane opcje wysokiej dostępności i skalowalności mogą pomóc w zaprojektowaniu środowiska najlepiej dopasowanego do potrzeb.
- Sectona MFA zapewnia większe bezpieczeństwo konfiguracji PAM, wymagając drugiego zweryfikowanego kroku wygenerowanego przez aplikację Sectona lub SMS.
- Łatwe wdrażanie systemu klasy PAM w różnych lokalizacjach, zarówno w chmurze, jak i lokalnie, dzięki elastycznym i niezależnym komponentom stworzonym dla środowisk chmurowych.
- Bezpieczne hasła i sekrety w pasywnej i szyfrowanej, uwierzytelnionej aplikacji do scenariuszy typu break-glass.

bakotech®
sectona

Bakotech Sp. z o.o.
ul. Drukarska 18/5 Kraków

sectona@bakotech.pl
12 340 90 30