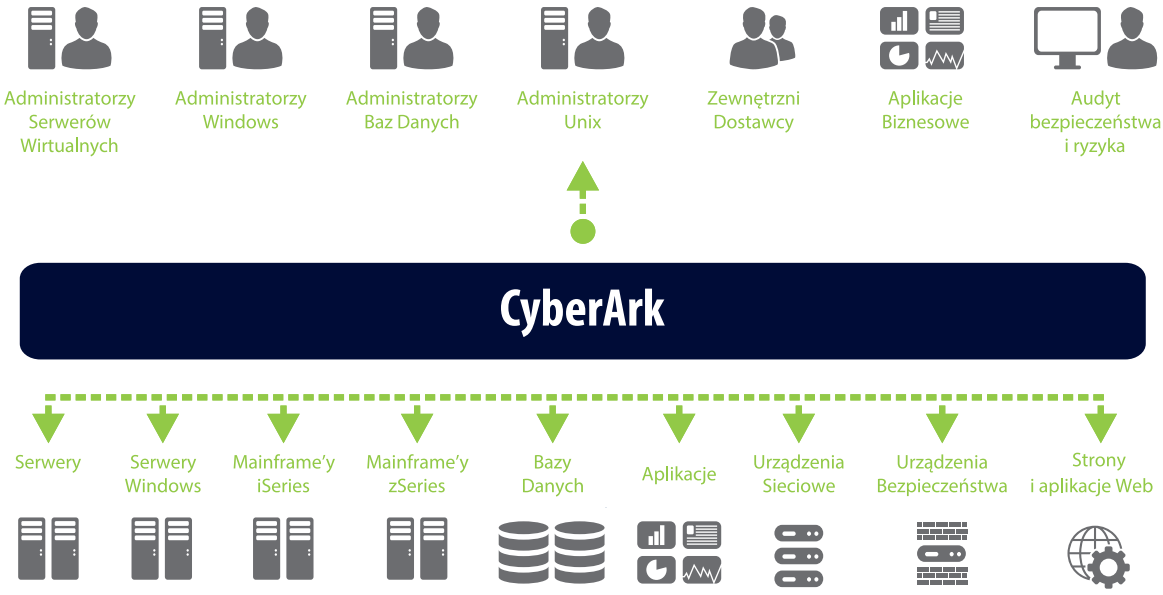
Trafford IT

CyberArk

ZARZĄDZANIE KONTAMI UPRZYWILEJOWANYMI, MONITOROWANIE, NAGRYWANIE

Infrastruktury firm są coraz większe i coraz bardziej złożone. Funkcjonuje w nich duża liczba urządzeń i systemów operacyjnych, zarządzanych przez wielu administratorów korzystających z kont uprzywilejowanych. Ochrona haseł do tych kont oraz brak ich regularnej zmiany stanowi źródło problemów wielu organizacji.

Rozwiązanie CyberArk służy do zarządzania hasłami użytkowników uprzywilejowanych w systemach operacyjnych, aplikacjach i urządzeniach sieciowych wykorzystywanych w dzisiejszych infrastrukturach teleinformatycznych. CyberArk zapewnia dodatkowo nagrywanie i monitorowanie sesji użytkowników uprzywilejowanych oraz zarządzanie poziomami uprawnień w systemach operacyjnych Windows i Linux.



Zalety rozwiązania:

- Możliwość instalacji zarówno w formie urządzeń fizycznych, jak i maszyn wirtualnych.
- Zarządzanie hasłami szerokiej gamy systemów, urządzeń i aplikacji.
- Łatwość tworzenia reguł zarządzania hasłami oraz dostosowania ich do polityk obowiązujących w organizacji.
- Możliwość nagrywania sesji do chronionych systemów, urządzeń i aplikacji.
- Zarządzanie uprawnieniami użytkowników w chronionych systemach Windows i Linux.
- API umożliwiające dostosowanie własnych aplikacji zapewniające integrację z systemem CyberArk.
- Możliwość kontroli, rozliczalności działań oraz identyfikacji administratorów logujących się na konta uprzywilejowane.
- Możliwość instalacji każdego z modułów w trybie High Availability, pozwalająca na osiągnięcie ciągłej dostępności całego systemu.
- Możliwość instalacji kluczowych elementów systemu w lokalizacjach rozproszonych (w trybie Disaster Recovery) pozwala na szybkie przywrócenie pełnej funkcjonalności systemu w przypadku awarii lokalizacji podstawowej.
- Modułowa struktura rozwiązania zapewnia dostosowanie systemu do indywidualnych potrzeb klienta oraz jego późniejszą modyfikację.

Komponenty rozwiązania CyberArk

Enterprise Password Vault (EPV) to podstawowy element systemu, odpowiedzialny za przechowywanie w bezpieczny sposób zarówno haseł do chronionych systemów, jak i dowolnych plików. W ramach dodatkowego zabezpieczenia EPV umożliwia przechowywanie w sejfie określonej liczby wersji obiektów historycznych oraz ich odtworzenie w razie potrzeby. Wszystkie obiekty przechowywane w sejfie są szyfrowane przy pomocy algorytmu AES256. Dostęp do poszczególnych obiektów jest ograniczony na poziomie uprawnień konkretnego użytkownika. Komponent ten zapewnia także możliwość autoryzacji użytkowników sejfu w zewnętrznych systemach, takich jak LDAP, czy Active Directory.

Central Policy Manager (CPM) to element rozwiązania odpowiedzialny za realizację polityki zarządzania hasłami chronionych systemów. CPM umożliwia tworzenie polityk dotyczących zmiany haseł w chronionych systemach, zgodnych z wymaganiami organizacji. Wymusza także regularną zmianę haseł, zarówno w chronionych systemach, jak i w odpowiadających im obiektach przechowywanych w EPV.

Password Vault Web Access (PVWA) to element systemu dostarczający przyjazny, webowy interfejs użytkownika, pośredniczący w dostępie do obiektów przechowywanych w sejfie oraz odpowiedzialny za zestawienie sesji z docelowym systemem. PVWA pozwala również na dostęp uprawnionych użytkowników do przeglądania zarejestrowanych połączeń, a także monitorowania, współdzielenia oraz przerywanie trwających sesji. Autoryzacja w PVWA może być przeprowadzana w samym EPV lub w systemach zewnętrznych, takich jak LDAP, czy Active Directory.

Application Identity Manager (AIM) to element systemu umożliwiający wyeliminowanie konieczności wykorzystania stałych haseł użytkowników technicznych pomiędzy aplikacjami klienckimi a serwerami. CyberArk udostępnia API pozwalające na dostosowanie kodu własnych aplikacji, zapewniając możliwość ich autoryzacji z wykorzystaniem haseł zapisanych w EPV.

Privileged Session Manager (PSM) to element systemu odpowiedzialny za rejestrowanie sesji realizowanych przez użytkowników uprzywilejowanych do chronionych systemów. PSM działa na zasadzie serwera przesiadkowego: sesje nawiązywane są do serwera PSM, który następnie zestawia i rejestruje sesję z serwerem docelowym. Serwer PSM potrafi nagrywać sesje do serwerów Windows (RDP), Linux (SSH), sesje do urządzeń sieciowych, wirtualizatorów oraz baz danych.

On-Demand Privilege Manager (OPM) to komponent umożliwiający ograniczenie użytkownikowi dostępu do określonego zestawu poleceń i aplikacji w chronionym systemie operacyjnym Windows lub Linux. Dzięki OPM użytkownik nie musi być administratorem docelowego systemu, aby móc wykonywać polecenia, czy uruchamiać aplikacje do tej pory zarezerwowane dla administratorów. Musi jedynie mieć przyznane przy pomocy OPM uprawnienia do wykonania określonych działań w systemie. Jest to przewaga nad standardowymi mechanizmami różnicowania uprawnień zaimplementowanymi w systemach operacyjnych, działającymi w większości przypadków na zasadzie „wszystko albo nic".

Endpoint Privilege Manager (EPM, Viewfinity) umożliwia organizacjom wprowadzenie zestawów reguł opartych na zasadzie minimum uprawnień dla użytkowników biznesowych i administracyjnych, a także wdrożenie kontroli aplikacji. Taka koncepcja ochrony ma na celu ograniczenie powierzchni podatnej na ataki bez strat na produktywności. Rozwiązanie pomaga działom IT w odbieraniu praw administratora lokalnego użytkownikom biznesowym, ale też zwiększa ich zakres, gdy wymaga tego praca z zaufanymi aplikacjami. Rozwiązanie nie tylko uzupełnia ustawienia uprawnień, ale też oferuje możliwość zarządzania aplikacjami i określania, które z nich mogą być uruchamiane przez Użytkowników stacji roboczych i serwerów bez narażania środowiska na penetrację przez złośliwe oprogramowanie.