arcon

Predict | Protect | Prevent

Privileged Access Management

Wstęp

ARCON Privileged Access Management (PAM) na nowo definiuje istotę bezpieczeństwa informacji dzięki przełomowemu rozwiązaniu kontroli ryzyka, którego szuka większość specjalistów ds. bezpieczeństwa w dobie powszechnej digitalizacji.

Dlaczego organizacje potrzebują zarządzania dostępem uprzywilejowanym?

Infrastruktura IT organizacji nigdy nie jest statyczna. Wraz z jej rozwojem rośnie liczba aplikacji, serwerów, zasobów w chmurze i wielu innych krytycznych systemów, co z kolei prowadzi do wzrostu liczby kont uprzywilejowanych, które mają dostęp do określonych zasobów. Tożsamości uprzywilejowane są rozproszone w całym przedsiębiorstwie i dotykają każdego elementu infrastruktury IT, jak systemy operacyjne, bazy danych, serwery i urządzenia sieciowe, a tym samym mają dostęp do ściśle tajnych danych.

Ze względu na ich strategiczne znaczenie w całej strukturze IT, tożsamości uprzywilejowane są często podatne na nadużycia ze strony złośliwych podmiotów, niezadowolonych pracowników lub po prostu hakerów. Z przeprowadzonych badań wynika, że aż około 75% incydentów naruszenia bezpieczeństwa danych ma miejsce na skutek nieuprawnionego wykorzystania poświadczeń uprzywilejowanych.

Privileged Access Management (PAM) firmy ARCON to najlepsze w swojej klasie rozwiązanie, które wzmacnia mechanizmy kontroli dostępu uprzywilejowanego. Rozwiązanie to oferuje najlepsze praktyki zarządzania kontami z uprawnieniami i stanowi podstawę solidnego zarządzania tożsamością i dostępem. Oferuje wysoki poziom kontroli nad użytkownikami uprzywilejowanymi, silne uwierzytelnianie wieloskładnikowe oraz bezpieczne przechowywanie haseł dostępu w korporacyjnym centrum danych.

Obdarzony zaufaniem przez ponad 500 przedsiębiorstw na całym świecie, ARCON PAM oferuje najlepiej dopasowaną architekturę zapewniającą przedsiębiorstwom wysoką skalowalność, a także wsparcie dla platform chmurowych.

ARCON | PAM zapewnia doskonałą równowagę między bezpieczeństwem, zgodnością i wydajnością biznesową.

W dzisiejszych czasach firmy poszukują kompleksowego rozwiązania w zakresie bezpieczeństwa, które zapewni im wydajność biznesową, solidny mechanizm kontroli bezpieczeństwa i domyślną zgodność z normami bezpieczeństwa. Decydenci oczekują też przyzwoitego zwrotu z inwestycji (ROI) z przyznanego budżetu. ARCON PAM to narzędzie do bezproblemowej kontroli, monitorowania i zabezpieczania kont uprzywilejowanych, które nie tylko chroni zasoby danych przed złośliwymi działaniami, ale także zapewnia ciągłość biznesową w prawdziwym tego słowa znaczeniu. Spełnia kompleksowo wszystkie wymagania i zapewnia doskonałą równowagę między wydajnością operacyjną IT, bezpieczeństwem i zgodnością.

Narzędzia dla
bezpieczeństwa, monitorowania i zarządzania

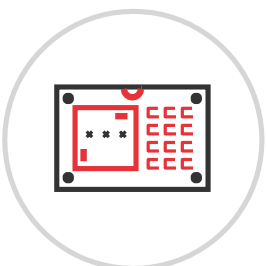
Precyzyjna kontrola dostępu

ARCON posiada unikalną strukturę technologiczną, która zapewnia szczegółową kontrolę dostępu dla uprzywilejowanych użytkowników, mimo że natywnie są super -użytkownikami i nie ma możliwości ograniczenia ich dostępu do żadnego systemu.

Jest to możliwe w przypadku kilku technologii, tj. systemów operacyjnych, baz danych, urządzeń sieciowych i zabezpieczających itp. Szczegółowa kontrola dostępu pomaga organizacjom chronić ich systemy przed nieautoryzowanym dostępem i niezamierzonymi błędami, jeśli takie występują. Umożliwia ograniczanie i kontrolowanie uprzywilejowanych użytkowników poprzez scentralizowaną politykę opartą na regułach i rolach.

Funkcjonalność ta zapewnia menedżerom ds. ryzyka IT możliwości ograniczania i filtrowania poleceń w celu zapewnienia bezpiecznego, autoryzowanego oraz kontrolowanego dostępu do systemów docelowych. Minimalizuje zakres ryzyka, zapewniając najgłębszy poziom szczegółowej kontroli nad administratorami danych i podmiotami przetwarzającymi dane.

Przechowywanie haseł



W niemal każdej większej organizacji istnieje wielu uprzywilejowanych użytkowników, co stwarza naturalne ryzyko powstawania nadużyć. Skuteczne ustawienie ręcznej kontroli procesu zmiany hasła, z zachowaniem jego bezpieczeństwa jest zawsze dużym wyzwaniem.

ARCON zapewnia sejf haseł, który generuje silne i dynamiczne hasła, a wbudowany silnik może automatycznie zmieniać hasła dla kilku urządzeń lub systemów jednocześnie. Hasła są przechowywane w wysoce zabezpieczonym sejfie elektronicznym. Metodologia przechowywania jest zastrzeżona oraz wysoce zabezpieczona kilkoma warstwami ochrony, które tworzą swego rodzaju wirtualną fortecę.

Skarbiec elektroniczny zintegrowany z ARCON PAM zapewnia autoryzowany dostęp do haseł. Umożliwia on przedsiębiorstwom obsługę złożonych i dynamicznych zmian haseł w celu spełnienia rygorystycznych wymagań prawnych.

Klucze SSH

Klucze SSH usprawniają zarządzanie kontrolą uwierzytelniania w przedsiębiorstwie. Klucze SSH to cenne dane uwierzytelniające umożliwiające dostęp do kont uprzywilejowanych. Zapewniają one dodatkową warstwę bezpieczeństwa kontroli dostępu.

Klucze SSH są bezpieczniejszą alternatywą dla haseł, które z wykorzystaniem dużej mocy obliczeniowej w połączeniu z automatycznymi skryptami można stosunkowo łatwo złamać. Pary kluczy SSH to dwa klucze kryptograficzne, które można użyć do bezpiecznego uwierzytelniania klienta na serwerze SSH.

Uwierzytelnianie wieloskładnikowe

Uprzywilejowany dostęp do kont wymaga ugruntowanych referencji tożsamości (walidacji) dla wszystkich użytkowników uzyskujących dostęp do krytycznych zasobów IT. Uwierzytelnianie wieloskładnikowe (MFA) zapewnia taki niezawodny mechanizm walidacji. Funkcjonalność MFA rozwiązania działa jako strategiczny punkt wejścia do systemów zarządzania tożsamością i pomaga w zarządzaniu użytkownikami.

ARCON oferuje natywną walidację jednorazowego hasła (OTP) w oparciu o własne oprogramowanie, aby rozpocząć uprzywilejowaną sesję, a narzędzie bezproblemowo integruje się z różnymi rozwiązaniami uwierzytelniającymi innych firm, takimi jak: Gemalto, RSA, Vasco, 3M, Precision, SafeNet i Safran.

Monitorowanie sesji

Monitorowanie sesji umożliwia zespołowi ds. bezpieczeństwa IT wykrywanie wszelkich podejrzanych działań wokół uprzywilejowanego konta. Live Dashboard sprawia, że wszystkie krytyczne działania wykonywane przez administratorów w infrastrukturze IT są przeglądane w czasie rzeczywistym.

Uzgadnianie haseł

Dzięki funkcji uzgadniania haseł codzienne zadania administracyjne stają się łatwiejsze. Po otrzymaniu najnowszych poświadczeń z ARCON PAM, takich jak adres IP, port, nazwa użytkownika i hasło dla danej usługi, następuje automatyczne połączenie z urządzeniem docelowym.

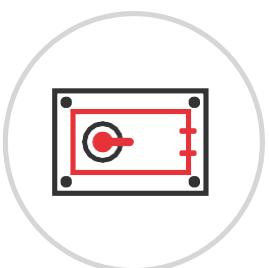
Po pomyślnym połączeniu ARCON PAM otrzymuje informację, że dana usługa jest aktywna i ma zaktualizowane hasło. Wszystkie stany powodzenia czy błędu są aktualizowane oraz widoczne w raporcie stanu usług. Dzięki takiej automatyzacji możliwe jest doskonalenie najlepszych praktyk w zakresie zarządzania kontami uprzywilejowanymi.

Przywilej Just-In-Time

ARCON PAM Just-In-Time (JIT) to potężne narzędzie, które zapewnia, że każdy uprzywilejowany dostęp jest dozwolony zgodnie z procesem zatwierdzania, przy jednoczesnym przestrzeganiu skonfigurowanych zabezpieczeń. Dzięki tej praktyce zespół ds. ryzyka IT w przedsiębiorstwie może mieć pewność, że wszyscy użytkownicy będą działać jako użytkownicy standardowi, a nie jako użytkownicy uprzywilejowani. Po zgłoszeniu każdego żądania administratorzy przyznają danemu użytkownikowi uprzywilejowane prawa do wykonania jedynie określonego zadania w ściśle określonym czasie.

ARCON PAM JIT usuwa stałe uprawnienia, ograniczając dostęp do systemów/aplikacji oraz liczbę pracowników administracyjnych/operacyjnych. Ogranicza on dostęp na poziomie szczegółowym, a nawet może odmówić stałego dostępu do wewnętrznych systemów/aplikacji.

My Vault



My Vault jest integralną częścią ARCON PAM, która zabezpiecza niejawne i poufne dokumenty organizacji, umożliwiając ograniczone udostępnianie poufnych zasobów danych.

Aby spełnić ten wymóg, My Vault nie tylko skutecznie go realizuje, ale także dba o tajemnice wszystkich serwerów, które nie są rotowane przez rozwiązanie PAM. Dzięki temu My Vault i PAM razem umożliwiają bezproblemowe zarządzanie wszystkimi uprzywilejowanymi serwerami i zasobami oraz ochronę tajemnic organizacji.

Zarządzanie hasłami

Zarządzanie hasłami aplikacji do aplikacji ARCON PAM odbywa się za pośrednictwem jednego terminala w infrastrukturze IT. Jest to zautomatyzowany proces, w którym zmiana hasła jest realizowana poprzez podanie wymaganych szczegółowych danych serwerów, adresów IP oraz nowych haseł.

Jest to płynny proces, który synchronizuje zmiany w całej sieci, aby zapobiec przerwom w świadczeniu usług. Wszystkie zmiany są sprawdzane w pliku konfiguracyjnym przed i po wykonaniu zadania.

Serwer bramy aplikacji

Serwer ARCON Application Gateway (AG) może zatrzymać ataki na najbardziej wrażliwą infrastrukturę IT przedsiębiorstwa. Wykorzystuje on nakładki sieciowe, szyfrowanie, zdefiniowaną programowo granicę i agenty oparte na hoście, aby ustanowić bezpieczne połączenie bez VPN. Narzędzie jest wystarczające do działania w ramach Zero Trust Network Access (ZTNA). Dostęp do systemów opiera się na „tożsamości" z innymi atrybutami i kontekstami, takimi jak: adresy IP, geolokalizacja, używane urządzenia, godzina i data. Ogólna wydajność operacyjna jest maksymalizowana przez AG wraz z solidnym monitoringiem dostępu.

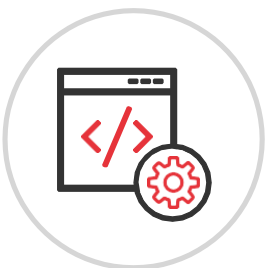
Zdalna pomoc

Remote Assist pomaga administratorom systemów w zdalnym dostępie i rozwiązywaniu problemów z urządzeniami końcowymi z dowolnego miejsca na świecie. Pomaga w natychmiastowym rozwiązywaniu zgłoszeń pomocy technicznej lub problemów z pulpitem. To bezpieczne rozwiązanie zdalnego pulpitu zapewnia szczegółową kontrolę nad siecią i umożliwia łączenie się z określonymi użytkownikami w sieci korporacyjnej i poza nią, zapewniając jednocześnie bezpieczeństwo IT i zgodność z polityką bezpieczeństwa.

Guard

ARCON Guard to narzędzie oparte na serwerze SSH, które jest instalowane centralnie na serwerze. Może być zintegrowane z ARCON PAM w celu ograniczania określonych poleceń. Guard ogranicza wszystkie polecenia, gdy jest zainstalowany na serwerze SSH i może być również dostępny za pośrednictwem aplikacji firm trzecich.

Taka konfiguracja umożliwia ograniczenie poleceń i monitorowanie sesji nawet w przypadku niedostępności ARCON PAM. Funkcja monitorowania plików wykrywa, kiedy i kto dokonał modyfikacji w krytycznych plikach konfiguracyjnych systemu na serwerze.



Menedżer skryptów

Menedżer skryptów pomaga użytkownikowi końcowemu zarządzać i kontrolować różne skrypty systemowe oraz monitorować ich wykonanie. Zgodnie z tym, ARCON PAM Automation Script Manager oferuje model kontroli dostępu oparty na rolach, gdzie modyfikacje skryptów automatyzacji oraz uprawnienia do ich wykonywania można konfigurować w oparciu o role użytkowników. W ten sposób ARCON PAM Automation Script Manager pomaga administratorom w uruchamianiu skryptów oraz ciągłym monitorowaniu wielu baz danych.

Obserwacja danych

Co by się stało, gdybyśmy mogli śledzić i kontrolować zapytania do bazy danych i mapować je z powrotem do uprzywilejowanej sesji za pośrednictwem PAM? Monitorowanie sesji może nie zawsze być najlepszym sposobem śledzenia poleceń lub zapytań. ARCON DataWatch po zintegrowaniu z ARCON PAM działa jako brama dla wszystkich połączeń z bazą danych, przechwytuje wszystkie zapytania i odpowiedzi a następnie mapuje je z powrotem do sesji.

Inteligentne monitorowanie sesji

Zaawansowany moduł monitorowania sesji o nazwie Smart Session Monitoring (SSM) pomaga w szybkim przeglądzie zarejestrowanych filmów poprzez podkreślanie krytycznych wydarzeń w nagraniach. Ponadto bezproblemowo monitoruje działania wykonywane na serwerze, takie jak: czynności użytkownika, kliknięcia myszą, naciśnięcia klawiszy, uruchomione procesy wraz z optycznym rozpoznawaniem znaków.

Skarbiec cyfrowy – zarządzanie tajemnicami

ARCON PAM Secrets Management wykorzystuje interfejs REST API do uwierzytelniania i zapewniania kontrolowanego dostępu do tożsamości innych niż osobowe dla aplikacji firm trzecich lub aplikacji opracowanych na zamówienie w celu pobierania poufnych danych wykorzystywanych do autoryzacji. W związku z powszechnym wykorzystywaniem interfejsów API w dostępie do uprawnień PAM, powstało wiele różnych metod uwierzytelniania. ARCON PAM skrupulatnie zbadał te metody i zintegrował się z większością z nich, dostosowując się do procesu ewolucji skarbca cyfrowego.

Skarbiec cyfrowy dla DevOps

DevOps to jeden z obszarów bezpieczeństwa IT, w którym ARCON PAM działa jako zaufana awangarda, aby zapewnić kontrolę dostępu oraz chronić skrypty i inne tajne wpisy funkcjonujące w potoku DevOps.

W czasach, gdy przedsiębiorstwa IT dążą do automatyzacji poprzez ciągłe doskonalenie i ciągły rozwój (CI/CD), ARCON PAM umożliwia bezproblemowy rozwój środowisk DevOps, zapewniając przedsiębiorstwom dodatkową warstwę zabezpieczeń, kontrolę dostępu oraz ochronę skryptów i innych wrażliwych danych.

Globalne rozwiązanie zdalnego dostępu

ARCON Global Remote Access Solution (GRAS) to najważniejsza funkcja uruchomiona w związku z pandemią. GRAS oferuje zdalnym użytkownikom bezpieczne nawiązanie zdalnego połączenia z przypisanym komputerem stacjonarnym lub laptopem spoza własnego środowiska infrastruktury IT.

Ponadto użytkownicy końcowi mogą unikać przestojów lub rozwiązywać problemy z daną maszyną w kontrolowanym środowisku bez konieczności instalowania i konfigurowania kosztownych sieci VPN. Rozwiązanie jest proste w użyciu, będąc natywną aplikacją chmurową.

Przegląd dostępu użytkownika

Dział IT pomaga administratorom w regularnej weryfikacji dostępu do usług przyznanego użytkownikom. Administratorzy mogą zdefiniować proces przeglądu dostępu dla nowego użytkownika, dla którego proces przeglądu jest inicjowany za pośrednictwem wiadomości e-mail w celu jego zatwierdzenia.

Proces konfiguracji harmonogramu ma zdefiniowaną datę rozpoczęcia, a liczbę dni wymagających zatwierdzenia można przejrzeć przed ustawieniem. W tym konkretnym dniu osoba zatwierdzająca otrzymuje wiadomość e-mail ważną przez liczbę dni określoną przez administratora. Administratorzy mogą modyfikować szczegóły skonfigurowanego dostępu użytkownika i zakończyć dostęp przed jego zainicjowaniem.

Dostęp efemeryczny

Jest to uprzywilejowany dostęp interaktywny Just-In-Time, który automatycznie generuje tymczasowe prawa dostępu oparte na regułach i rolach. Konsola Amazon Web Services (AWS) lub komponent interfejsu wiersza poleceń (CLI), który współdziała z usługą AWS Secure Token Service (STS) umożliwia administratorowi dostosowywanie kont za pomocą unikalnych ról AWS. Kiedy użytkownik loguje się do konsoli zarządzania AWS, jest przypisywany do określonej pozycji i regulacji AWS oraz może wykonywać jedynie zatwierdzone operacje w sieci AWS.

Narzędzia dla efektywności w IT

Automatyczne wykrywanie

Infrastruktura IT stoi w obliczu ogromnego ryzyka w środowisku współdzielonych i rozproszonych kont uprzywilejowanych. Identyfikacja i śledzenie własności uprawnień to duże wyzwanie dla zespołu ds. bezpieczeństwa i zarządzania ryzykiem. Aby sprostać temu wyzwaniu, funkcja automatycznego wykrywania ARCON umożliwia zespołowi zarządzania ryzykiem wykrywanie współdzielonych kont, kont oprogramowania i usług w całej infrastrukturze IT. Identyfikacja i śledzenie przynależności uprawnień ogranicza ryzyko związane z cyklem życia kont uprzywilejowanych.

Wirtualne grupowanie

Zarządzanie różnymi systemami przez różne zespoły przy zachowaniu pełnej kontroli to bardzo złożone zadanie. ARCON PAM zapewnia dynamiczne ustawienie grup z relacją "jeden do wielu" i grupowaniem wirtualnym użytkowników.

W ten sposób można tworzyć grupy funkcjonalne różnych systemów i ułatwić utrzymanie relacji oraz zakresu odpowiedzialności. Funkcja ta bardzo dobrze odpowiada dynamicznie zmieniającym się strukturom organizacyjnym, rolom, odpowiedzialnościom, a nawet pozwala na zarządzanie wieloma spółkami zależnymi i firmami.

Wprowadzenie nowych użytkowników

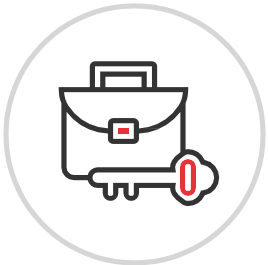
Wprowadzanie nowych użytkowników umożliwia administratorom bezproblemowe dodawanie nowych grup serwerów, kont użytkowników z powiązanymi uprawnieniami, a następnie mapowanie nowych użytkowników utworzonych na poziomie ARCON PAM. Umożliwia to administratorom automatyczne udostępnianie i anulowanie obsługi użytkowników lub urządzeń poprzez bezpośrednią interakcję z usługą Active Directory. Dzięki takiemu mechanizmowi wprowadzania użytkowników organizacje mogą być pewne, że wszystkie informacje zebrane podczas wdrażania pozostaną poufne i zablokowane w wirtualnej bazie danych oraz będą poza zasięgiem wszelkiego rodzaju fizycznego lub nieautoryzowanego dostępu.

Jednokrotne logowanie

Logowanie jednokrotne zapewnia jednorazowy dostęp administracyjny do wszystkich podstawowych aplikacji. Infrastruktura IT składa się z wielu warstw urządzeń umożliwiających dostęp do systemów, co z kolei prowadzi do konieczności ustanawiania wielu administratorów, a to stanowi duży problem z punktu widzenia bezpieczeństwa. Wielu administratorów systemu oznacza wiele identyfikatorów użytkowników, wiele haseł i wiele procesów zatwierdzania.

Funkcja jednokrotnego logowania pozwala przezwyciężyć to wyzwanie. Ułatwia ona administratorom systemowym zarządzanie wieloma hasłami na różnych urządzeniach, takich jak urządzenia sieciowe, bazy danych itp. Gdy administratorzy systemowi używają konektorów do łączenia wszystkich tych komponentów, możliwe jest korzystanie z pojedynczego logowania, bez konieczności zapamiętywania indywidualnych identyfikatorów użytkownika i haseł dla różnych systemów i urządzeń.

Umożliwia to bezproblemowy dostęp do różnych technologii za pomocą jednego kliknięcia. Zapobiega też ewentualnym nadużyciom kont uprzywilejowanych, realizując zasadę najmniejszych uprawnień.

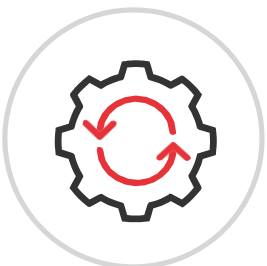


Kontrola jednego administratora

Bez względu na to, jak złożona jest infrastruktura IT Twojego przedsiębiorstwa, każdy dostęp do krytycznych systemów odbywa się za pośrednictwem jednej konsoli administracyjnej. Bezpieczny Gateway Server stanowi scentralizowany punkt kontrolny, do którego kierowane są wszystkie połączenia sieciowe i ruch w celu zarządzania oraz monitorowania.

ARCON PAM zapewnia zunifikowany silnik polis, który oferuje dostęp do systemów docelowych w oparciu o role i reguły. Mechanizm autoryzacji zapewnia wdrożenie założonych zasad kontroli dostępu dla ludzi oraz odpowiednie polityki dostępu dla systemów. Dzięki temu dostęp do kont uprzywilejowanych przyznawany jest na zasadzie „trzeba wiedzieć" i „trzeba zrobić", co stanowi podstawę niezawodnego zarządzania tożsamością oraz skutecznej kontroli dostępu.

Zarządzanie przepływem pracy



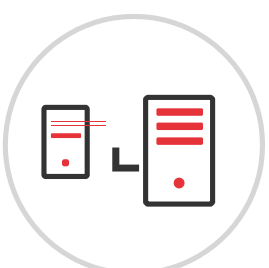
Koniec ze żmudnym i długim procesem zatwierdzania dostępów. Macierz przepływu pracy ułatwi życie administratorom. Umożliwia ona skonfigurowanie procesu zatwierdzania dla uprzywilejowanych użytkowników, grup użytkowników i usług. Mechanizm przepływu zapytań serwisowych i haseł przyspiesza proces przypisywania serwerów docelowych do uprzywilejowanych użytkowników.

Uprzywilejowane zarządzanie podnoszeniem uprawnień i delegowaniem (PEDM)

Podczas gdy ARCON PAM pozwala przedsiębiorstwu na zbudowanie warstwy bezpieczeństwa wokół kont uprzywilejowanych poprzez przyznanie praw dostępu pełnym użytkownikom administracyjnym w oparciu tylko o wstępnie zdefiniowane zasady kontroli dostępu, Privileged Elevation and Delegation Management (PEDM) uzupełnia zarządzanie uprzywilejowanymi użytkownikami poprzez kontrolowanie i monitorowanie działań użytkowników niebędących administratorami, którzy wymagają tymczasowego uprzywilejowanego dostępu do systemów.

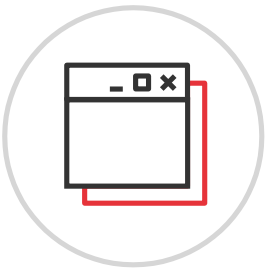
PEDM zasadniczo odrzuca niepotrzebną eskalację kont uprzywilejowanych. Ich nadmierna liczba, zwłaszcza w rozproszonym środowisku IT, zwiększa potencjalne zagrożenia nieuprawnionego dostępu do informacji poufnych. Narzędzie to jest rozszerzeniem podejścia granularnego, które umożliwia przedsiębiorstwu ograniczanie ryzyka poprzez przyznawanie tymczasowych uprawnień administracyjnych tylko na zasadzie „trzeba wiedzieć" i „trzeba zrobić".

Mostkowanie AD



Active Directory Bridging to pomost między komputerem z systemami Linux a serwerami Windows AD. Jest to aplikacja webowa, która umożliwia użytkownikom (administratorom i nie-administratorom) logowanie się do komputera z systemem LINUX przy użyciu poświadczeń Windows Active Directory.

Automatyzuje to także różne zadania na poziomie administracyjnym, takie jak instalowanie protokołu Kerberos, konfigurowanie plików i ponowne uruchamianie usług w celu aktualizacji konfiguracji. Ponadto czynności wykonywane na maszynie LINUX mogą być dodatkowo rejestrowane. ARCON PAM oferuje wszystkie możliwości modułów Session Manager, Password Manager i Access Manager, aby w przejrzysty sposób łączyć wyłącznie głównych użytkowników ich systemu operacyjnego. Użytkownicy mogą uwierzytelniać się za pomocą tylko jednego wpisu, nawet bez modyfikowania konfiguracji Active Directory.



Zarządzanie sesją (znane również jako Multi-tab)

Funkcja Multi-tab umożliwia użytkownikom/administratorom otwieranie wielu sesji na różnych kartach w tym samym oknie i przełączanie się między sesjami zgodnie z ich wymaganiami. Funkcja Multi-tab jest obsługiwana przez usługi typu SSH i RDP. Wiele sesji usług, o ile otwierane są z wykorzystaniem kart w jednym oknie, ułatwia użytkownikowi przełączanie się między usługami i centralne sterowanie wszystkimi sesjami użytkownika.

Desk Insight

Obsługa zgłoszeń pochodzących z wielu stacji staje się czasem poważnym wyzwaniem dla działu helpdesk. Desk Insight firmy ARCON to skuteczne narzędzie, które umożliwia administratorowi zarządzanie zgłoszeniami z dowolnej stacji podłączonej do sieci firmowej. Umożliwia to także inżynierom pomocy technicznej rozwiązywanie problemów z daną stacją bez przechodzenia z jednego pulpitu na drugi. Desk Insight umożliwia również użytkownikom końcowym podniesienie uprawnień administratora, zmianę haseł i dostęp do powiązanych zadań w kontrolowanym środowisku.

Analiza zachowania (Knight Analytics)

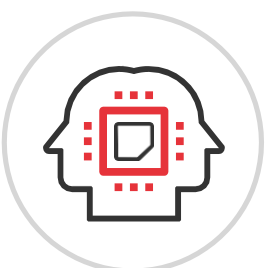
Knight Analytics to system wykrywania zagrożeń typu deep learning opracowany przez specjalistów ARCON PAM. Technologia ta jest oparta na sztucznej inteligencji i służy do wykrywania, przewidywania i wyświetlania wszelkich anomalii w zarejestrowanych danych.

Wykorzystuje algorytmy uczenia maszynowego, które uczą się zachowania każdego użytkownika na podstawie danych historycznych i przewidują ryzyko na podstawie podejmowanych przez niego działań. Istnieje sześć różnych wykresów, które przedstawiają administratorom procent potencjalnego ryzyka. Są to analizy użytkowników, analizy usług, analizy grup użytkowników, analizy grup usług, analizy użytkowników w ramach grupy i analizy usług w zakresie grup.

Zarządzanie incydentami

Mechanizmy reagowania na incydenty mają dziś ogromną wagę. Kluczowe znaczenie ma jak najszybsze reagowanie na wszelkie dane dotyczące incydentów, aby uniknąć poważnych strat. Po incydencie zespoły IT potrzebują umiejętności analizy przyczyn, działań po incydencie oraz zidentyfikowania obszarów zagrożeń do lepszego reagowania w przyszłości.

Jeśli ten proces jest zautomatyzowany, wytwarza się niezbędna synergia użytkowników z zespołem reagowania na incydenty, co pomaga zaoszczędzić wiele cennego czasu. Dzięki funkcji zarządzania incydentami uprzywilejowany użytkownik może zidentyfikować i zgłosić incydent dotyczący dowolnej aktywności, która wydaje się być podejrzana.



Zrobotyzowana automatyzacja procesów (RPA)

Wykonywanie regularnych, przyziemnych zadań IT jest zawsze przyjmowane z niechęcią przez wszystkich użytkowników IT. Robotic Process Automation (RPA) pomaga zautomatyzować takie zadania z dużą łatwością, wydajnością i dokładnością. ARCON PAM oferuje możliwość dostosowania poszczególnych kroków do użytkowników końcowych dla dowolnej aktywności SSO. Może to być rozpoznawanie na podstawie obrazu, skrótów klawiszowych lub identyfikatorów ID. Technologia RPA może być wykorzystana we wszystkich przypadkach użycia zastosowanych konektorów.

vRA

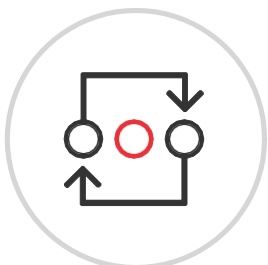
Wraz z rosnącym znaczeniem usług chmurowych oraz możliwości technologicznych, takich jak VMware, organizacje dążą do zwiększania elastyczności, produktywności i wydajności poprzez automatyzację chmury, upraszczane środowiska IT, usprawnianie procesów i dostarczanie platformy automatyzacji dostosowanej do środowisk DevOps.

vRA zapewnia zarządzanie operacjami w środowiskach fizycznych, wirtualnych i chmurowych. Automatyzację vRA (VMware vRealize Automation) można wykorzystać do automatyzacji świadczenia usług PAM po utworzeniu nowej maszyny wirtualnej. ARCON PAM zapewnia integrację z rozwiązaniami automatyzacji, takimi jak vRA, aby umożliwić dołączanie i usuwanie uprzywilejowanych kont oraz urządzeń/systemów.

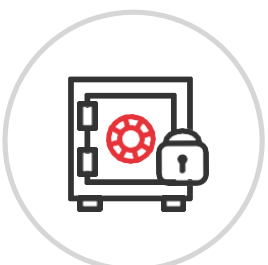
Dedykowana wtyczka do przeglądarki

Jest to niezależne od przeglądarki rozszerzenie dostępne dla wszystkich platform, które oferuje punktowe rozwiązanie do ochrony wszystkich "tajemnic" i poufnych zasobów Twojej organizacji w jednym miejscu. Dzięki wtyczce do przeglądarki użytkownicy mogą automatycznie logować się do szeregu aplikacji oferowanych przez ARCON PAM bez ręcznego wprowadzania danych uwierzytelniających, a nawet zapamiętywania ich za każdym razem, gdy uzyskują dostęp do aplikacji bezpośrednio z dowolnej przeglądarki dostępnej na ich komputerze.

Connector Framework



Wraz z rosnącym zapotrzebowaniem organizacji na nowe mechanizmy IT, ochrona systemów poprzez ich integrację z ARCON PAM staje się niezbędna. ARCON Connector Framework automatyzuje proces tworzenia konektorów, eliminując konieczność ręcznego gromadzenia danych autoryzacyjnych. Upraszcza również proces udostępniania każdej nowej aplikacji, która nie jest dostępna w PAM.



Vault Broker Suite

Vault Broker Suite jest przeznaczony dla tożsamości osobowych lub systemowych, które wymagają uprzywilejowanych haseł oraz bezpiecznych kanałów do łączenia się z różnymi systemami. Jest on wymagany tylko wtedy, gdy aplikacje docelowe nie są w stanie nawiązać bezpośredniego połączenia z systemami docelowymi.

Zamiast zmuszać klienta do autoryzacji poprzez ARCON PAM Vault, istnieją moduły do przesyłania uwierzytelnionego połączenia do klienta, eliminując potrzebę pobierania danych uwierzytelniających przez klienta. Vault Broker nie tylko może bezpiecznie połączyć się z ARCON PAM Vault, ale także ze skarbcami innych firm.

Integracje

ARCON PAM zapewnia bezproblemową integrację z różnymi narzędziami typu: SIEM, ITSM, RPA, DevOps CI/CD, IDAM, Automation Solutions, Containers i nie tylko. Inne narzędzia, które można zintegrować z ARCON to m.in.: Symantec, RSA, Arcsight, Rapid7, BMC Remedy, Precision, ServiceNow, Nessus Manager, Tenable.io/Tenable.sc, Qualys, Ansible, Jenkins, Chef, Kubernetes, Red Hat OpenShift , AWS Elastic Container Service (ECS), Microsoft AD, Azure AD, G-Suite, AWS IAM, Okta, Sailpoint czy 1Kosmos.

Narzędzia dla zgodności i raportowania

Niestandardowe raporty

Standardy regulacyjne wymagają od zespołów ds. zarządzania ryzykiem IT dostarczania szczegółowych informacji na temat aktualnych zasad kontroli dostępu do krytycznych informacji. Co więcej, regulatorzy wymagają często kompleksowych raportów audytowych dotyczących każdej aktywności użytkownika uprzywilejowanego w krytycznych systemach. Aby spełnić ten wymóg prawny, przedsiębiorstwa muszą generować i utrzymywać kompleksowe ścieżki audytu dla każdej uprzywilejowanej sesji.

Zaawansowany silnik raportowania ARCON sprawi, że Twój zespół ds. bezpieczeństwa będzie gotowy do audytu, dysponując zawsze szczegółową analizą każdego uprzywilejowanego konta, co ułatwi podejmowanie decyzji przez uprzywilejowanych użytkowników IT. Rozwiązanie to umożliwia menedżerom i audytorom ocenę stanu zgodności organizacji z przepisami w dowolnym momencie.

Dzienniki tekstowe i wideo

ARCON PAM proaktywnie zabezpiecza wszystkie bazy danych i aplikacje, ponieważ każde polecenie/zapytanie wykonywane przez użytkowników końcowych może być rejestrowane w celu oceny bezpieczeństwa. W ten sposób zespół ds. oceny bezpieczeństwa i ryzyka może bezproblemowo zarządzać cyklem życia każdego uprzywilejowanego konta, ponieważ każda czynność wykonywana przez uprzywilejowanych użytkowników może być rejestrowana zarówno w formacie wideo, jak i tekstowym.

Narzędzie do raportowania Analytics (znane również jako Spection)

Spection rozszerza systemową platformę analityczną do generowania dynamicznych raportów z prezentacją statystyczną i graficzną. Narzędzie daje swobodę wyboru raportu i sposobu jego przeglądania zgodnie z indywidualnymi wymaganiami. Wszystkie niezbędne encje i elementy są filtrowane i porządkowane w celu wygenerowania dynamicznego raportu.

Zgodność – standardy prawne

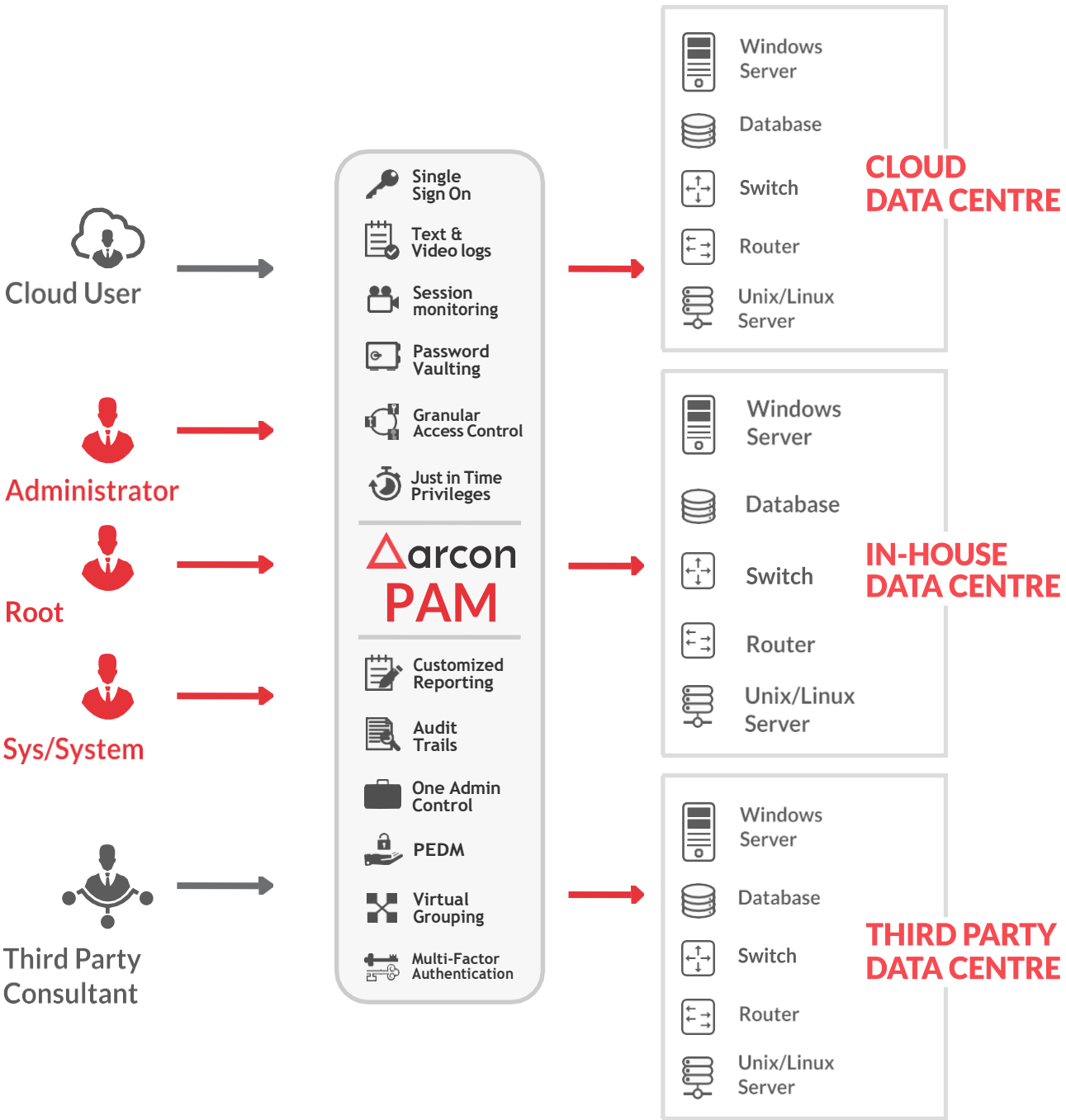
ARCON PAM umożliwia organizacjom spełnienie wymagań regulacyjnych z poziomu jednej platformy. Wytyczne Unii Europejskiej (RODO), PCI-DSS, SWIFT, ISO-27001, BASELIII, HIPAA, SOX itp. nałożyły na organizacje obowiązek posiadania niezbędnej infrastruktury bezpieczeństwa IT, która chroniłaby konta uprzywilejowane przed nieautoryzowanymi działaniami.

ARCON | PAM

Kluczowe cechy

- Pomaga spełnić wymagania regulacyjne i standardy IT
- Zapewnia uprzywilejowany dostęp do systemów docelowych wyłącznie na zasadzie „trzeba wiedzieć” i „trzeba zrobić”
- Zwiększa ogólną wydajność IT i zapewnia bezpieczeństwo poufnych danych
- Wysoce dojrzały skarbiec haseł umożliwia losowe przydzielanie uprzywilejowanych haseł, zarządzanie tajnymi obiektami na dużą skalę, w tym dla środowisk DevOps i CI/CD
- Oferuje najgłębszy poziom szczegółowych kontroli, aby wymusić zasadę najniższego przywileju
- Zapewnia uprawnienia Just-In-Time (JIT) dla docelowych urządzeń
- Oferuje funkcje podnoszenia uprawnień i zarządzania delegowaniem (PEDM)
- Obsługuje współczesne przypadki użycia, jak: Cloud Access, DevOps, obciążenia API czy boty
- Umożliwia globalny bezpieczny dostęp zdalny w celu sprostania wyzwaniom w zakresie kontroli dostępu w tzw. "nowej normalności"
- Posiada rozbudowaną paletę konektorów do obsługi narzędzi firm trzecich i ich szybkiej implementacji
- Wykorzystuje AI/ML do zaawansowanej analizy zagrożeń
- Wysoce skalowalny i konfigurowalny
- Pozwala na uprzywilejowane zarządzanie sesjami z niezawodnym uwierzytelnianiem wieloskładnikowym, scentralizowanym pulpitem nawigacyjnym, monitorowaniem sesji i raportowaniem

Architektura produktu



Wnioski

ARCON PAM to kompleksowe rozwiązanie do zarządzania dostępem uprzywilejowanym, umożliwiające monitorowanie i kontrolowanie bezpieczeństwa wszelkich kont uprzywilejowanych. Takie wzmacnianie bezpieczeństwa tożsamości uprzywilejowanych umożliwia firmom spełnienie wielu wymogów regulacyjnych z poziomu jednej platformy. Wytyczne dostarczone przez Unię Europejską (RODO), PCI-DSS, SWIFT, ISO 27001, BASELIII, HIPAA, SOX itp. nałożyły na organizacje obowiązek posiadania niezbędnej infrastruktury bezpieczeństwa IT, która będzie szczególnie chroniła konta uprzywilejowane przed nieautoryzowanymi działaniami.

Rozwiązanie to zapewnia dodatkową warstwę abstrakcji nad podstawową tkanką infrastruktury IT, dzięki czemu wymusza na użytkownikach logowanie się przy użyciu identyfikatora użytkownika, haseł i unikatowego hasła jednorazowego (OTP). Dodatkowo, ARCON PAM zapewnia wymagany dostęp na zasadzie „trzeba zrobić" i „trzeba mieć" oraz może precyzyjnie śledzić działania użytkowników, nawet jeśli są to użytkownicy uprzywilejowani.

Rozwiązanie PAM nie tylko zapewnia bezpieczny parasol dla podstawowej infrastruktury IT i danych, ale także udostępnia pełną ścieżkę audytu działań powiązanych z kontami uprzywilejowanymi. Narzędzie skutecznie identyfikuje słabe punkty i ocenia ryzyko na różnych poziomach infrastruktury, takich jak systemy operacyjne, bazy danych i serwery.

Connect with us