

PASM

PEDM

DSM

CM



**CHROŃ FIRME PRZED
NIEUPRAWNIONYM
DOSTĘPEM**

CHROŃ FIRME PRZED NIEUPRAWNIONYM DOSTĘPEM



Gartner Challenger 2020

Senhasegura to rozwiązanie klasy PAM (Privileged Access Management), czyli system do zarządzania dostępem uprzywilejowanym. Zapewnia najwyższy poziom bezpieczeństwa w fundamentalnym filarze cyberbezpieczeństwa, jakim jest kontrola dostępu oraz ochrona poświadczeń.

Rozwiązanie w zautomatyzowany i prosty sposób pozwala wprowadzić w życie wszystkie dobre praktyki dotyczące przydzielania dostępów, tworzenia haseł, czy też ich cyklicznego resetowania. System umożliwia monitorowanie oraz nagrywanie wszystkich sesji zarówno wewnętrznych, jak i tych przychodzących z zewnątrz. Senhasegura posiada wiele dodatkowych modułów pozwalających na wdrożenie zgodnie z wymogami swoich Klientów (przechowywanie kluczy SSH, zarządzanie certyfikatami, ochrona tajemnic i wiele innych).

Senhasegura jest dostępna w ponad 40 krajach na całym świecie, a w Magicznym Kwadrancie Gartnera zaklasyfikowana została jako Challenger. Ponadto rozwiązanie posiada bardzo wysoką ocenę 4,9 / 5 w badaniu „Gartner Peer Insights” przeprowadzonym z użytkownikami produktu.

ZARZĄDZANIE POŚWIADCZENIAMI



Za pomocą mechanizmu Grup Dostępu określ, którzy użytkownicy mogą korzystać z określonych haseł i uzyskać zdalny dostęp do urządzenia lub usługi.

AUDYT I ZAPEWNIENIE ZGODNOŚCI Z REGULACJAMI



Generuj łatwe do wyeksportowania zbiory dowodów za pomocą rozbudowanego menu raportów, zaprojektowanego na potrzeby audytów oraz instytucji nadzorczych. Na potrzeby regularnych audytów można utworzyć dedykowany profil audytora.

KONTROLA PODMIOTÓW ZEWNĘTRZNYCH



Za pomocą grup i profili dostępu możesz w kontrolowany sposób dopuścić do swojej sieci podmioty zewnętrzne, np. dostawców usług, nadając im uprawnienia wyłącznie do określonych urządzeń i usług oraz w określonym przedziale czasu.

ZBIERANIE LOGÓW



Określ, którzy użytkownicy będą korzystali z sesji logowanych, monitorowanych oraz w pełni nagrywanych, także w przypadku sesji równoległych.

DZIELENIE POŚWIADCZEŃ



Rozdziel hasła na kilku użytkowników, tak aby każdy z nich był wymagany, by uzyskać dostęp do danego urządzenia, usługi lub aplikacji.

NAGRYWANIE SESJI



Nagrywaj wszystkie zdalne sesje, w tym sesje równoległe, za pomocą Senhasegura i zapisuj je w postaci plików wideo o bardzo dobrej jakości obrazu, przy zachowaniu niewielkiego rozmiaru.

AUTOMATYCZNA ZMIANA HASEŁ



Zmieniaj automatycznie hasła za każdym razem, kiedy zakończona zostanie sesja z wykorzystaniem jednorazowych poświadczeń.

AUDYT POLECEŃ



Skonfiguruj alarmy w ramach sesji SSH, Telnet i baz danych dla wszystkich użytkowników, także z uprawnieniami administratora.

MECHANIZM PRYZNAWANIA DOSTĘPU



Kontroluj dostęp do zarządzanych urządzeń i poświadczeń za pomocą wielopoziomowego mechanizmu przyznawania dostępu.

ANALIZA ZAGROZEŃ



Śledź na bieżąco potencjalne zagrożenia i podejrzaną aktywność, monitorując tym samym wszystkie operacje wykonywane w ramach uprzywilejowanego dostępu, chroniąc organizację przed wyciekiem danych oraz umożliwiając szybką reakcję w przypadku ataku.

MODUŁ AAPM



Załaduj podatności w postaci poświadczeń zapisanych w kodzie źródłowym i plikach konfiguracyjnych, chroniąc tym samym krytyczne dane. Poświadczenia będą wprowadzane do aplikacji za pośrednictwem API Senhasegura, a osoby niepowołane nie będą miały do nich dostępu.

JUMP SERVER



Dostęp za pomocą Putty lub RDP może się odbyć w ramach sesji monitorowanej, bez potrzeby ujawniania hasła użytkownikom.