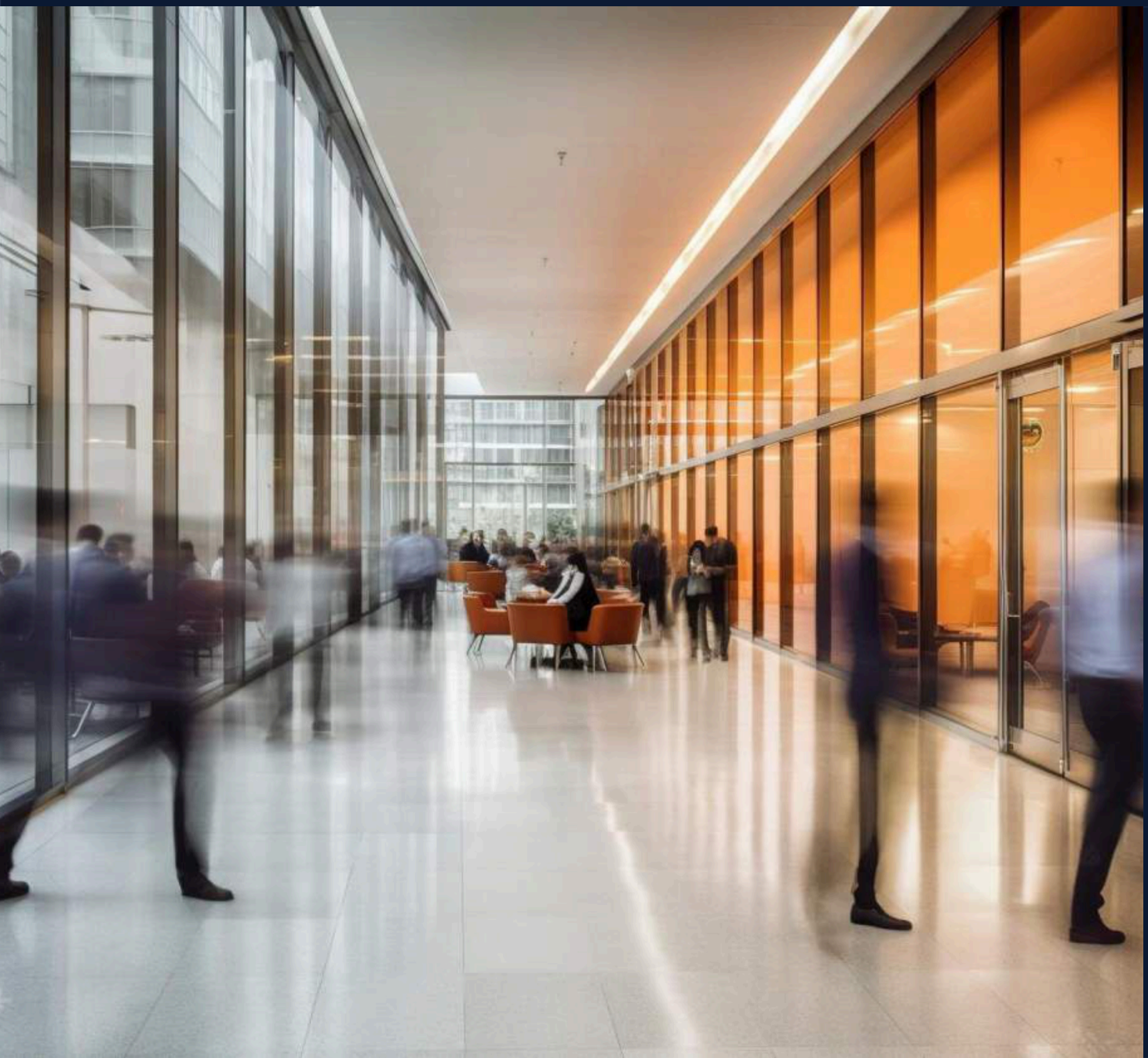
kuppingercole ANALYSTS

Rola PAM we współczesnym cyberbezpieczeństwie

Materiał przygotowany przez Paula Fishera, Głównego Analityka w Kuppinger Cole



Zarządzanie uprzywilejowanym dostępem (PAM) jest kluczowym filarem dotyczącym cyberbezpieczeństwa, chroniącym wrażliwe systemy i dane przed coraz bardziej wyspecjalizowanymi zagrożeniami cybernetycznymi. Uprzywilejowane dane uwierzytelniające — takie jak te używane przez administratorów, programistów lub skrypty automatyzacyjne — są często celem cyberataków ze względu na szeroki dostęp, jaki zapewniają. W związku z tym organizacje potrzebują solidnych rozwiązań PAM, które wykraczają poza tradycyjne granice ochrony, aby sprostać nowym wyzwaniom, takim jak chociażby Shadow IT, zagrożenia wewnętrzne czy bezpieczny dostęp zdalny.

Zapotrzebowanie na rozwiązania PAM jest napędzane przez rosnącą złożoność środowisk IT, które obecnie obejmują infrastrukturę hybrydową, ekosystemy multi-cloud i zdalne modele pracy. Jednak wdrażanie i zarządzanie rozwiązaniami PAM wiąże się z konkretnym zestawem wyzwań operacyjnych. Organizacje muszą zintegrować narzędzia z istniejącymi systemami, zapewniając ich płynne funkcjonowanie, jednocześnie zarządzając uprzywilejowanymi tożsamościami w rozproszonych środowiskach.

Skuteczne rozwiązania PAM to dziś coś więcej niż tylko sejfy do przechowywania haseł — obecnie umożliwiają organizacjom egzekwowanie dynamicznych, czasowo ograniczonych kontroli dostępu, ciągłe monitorowanie aktywności użytkowników i generowanie kompleksowych ścieżek audytu. Te funkcjonalności są kluczowe nie tylko dla bezpieczeństwa, ale także dla spełniania wymagań regulacyjnych. Syteca, wcześniej znana jako Ekran System, dostosowała zakres funkcji, aby sprostać tym zmieniającym się wymaganiom, kładąc nacisk na funkcjonalność, użyteczność i praktyczne zastosowanie.

Rosnąca konkurencja na rynku PAM

Rynek PAM (Zarządzania Uprzywilejowanym Dostępem) ewoluował szybko w ciągu ostatniej dekady, z udziałem zarówno uznanych specjalistów, jak i nowych podmiotów konkurujących o znaczący udział w tym obszarze. Taki wzrost odzwierciedla szerszy trend w cyberbezpieczeństwie, ponieważ organizacje coraz częściej priorytetowo traktują ochronę uprzywilejowanych danych uwierzytelniających. Przejście na środowiska hybrydowe i multi-cloud dodało jednakże nowe wymiary tym wyzwaniom.

Organizacje nie szukają już wyłącznie narzędzi zabezpieczających dane uwierzytelniające; potrzebują rozwiązań PAM, które zapewniają elastyczność, skalowalność i łatwość użytkowania bez kompromisów w zakresie bezpieczeństwa. Funkcje takie jak dostęp „Just-in-Time" (JIT), płynna integracja z architekturami Zero Trust oraz zgodność z ciągle zmieniającymi się wymaganiami regulacyjnymi stały się standardowymi oczekiwaniami.

Dostawcy odpowiadają na to zapotrzebowanie, oferując zróżnicowane rozwiązania – od bogatych w funkcje systemów dla dużych przedsiębiorstw po wyspecjalizowane narzędzia dostosowane do konkretnych branż. Na tym zatłoczonym rynku kluczowe znaczenie ma wyróżnienie się. Rozwiązania, które dostosowują się do unikalnych potrzeb biznesowych, jednocześnie odpowiadając na szersze wyzwania, takie jak bezpieczny dostęp zdalny lub monitorowanie działań wewnętrznych, mają większe szanse na sukces. Niedawna transformacja Syteca oraz rozszerzone możliwości pozycjonują ją jako silnego konkurenta na tym dynamicznie rozwijającym się rynku.

Z czego wynika rebranding Ekran System na Syteca?

W maju 2024 roku Ekran System przeszedł rebranding i stał się Syteca – była to strategiczna decyzja, która symbolizuje rozwój firmy oraz jej zaangażowanie w rozwiązywanie problemów współczesnego cyberbezpieczeństwa. Nowa nazwa odzwierciedla poszerzone ukierunkowanie Syteca na dostarczanie innowacyjnych rozwiązań w zakresie zarządzania bezpieczeństwem systemów i technologią.

Ta transformacja to coś więcej niż tylko zmiana nazwy – oznacza również nowe podejście firmy do zarządzania uprzywilejowanym dostępem (PAM). Syteca dąży do dostosowania swoich narzędzi do praktycznych potrzeb organizacji, kładąc nacisk na użyteczność i efektywność. Udoskonalone funkcje, takie jak wykrywanie zagrożeń w czasie rzeczywistym, zaawansowane nagrywanie sesji i zoptymalizowane przepływy pracy, podkreślają cel firmy: dostarczanie kompleksowych, a jednocześnie intuicyjnych rozwiązań.

Dzięki rebrandingowi Syteca umacnia swoją pozycję jako nowoczesny uczestnik na rynku PAM. Produkt nie tylko odpowiada na aktualne wyzwania stojące przed organizacjami, ale także przewiduje ich przyszłe potrzeby, zapewniając, że jego funkcjonalności będą niezmiennie istotne w stale zmieniającym się środowisku.

Przykłady użycia Syteca wyróżniające możliwości, jakie daje narzędzie

Podejście Syteca do funkcjonalności PAM najlepiej zrozumieć poprzez praktyczne zastosowania modułu. Poniższe przypadki użycia pokazują, w jaki sposób rozwiązanie odpowiada na kluczowe wyzwania związane z bezpieczeństwem w różnych branżach i w odniesieniu do różnych scenariuszy.

01 Wykrywanie i zabezpieczanie ukrytych kont

Konta IT tworzone bez autoryzacji lub poza centralnym nadzorem stanowią istotne zagrożenie dla bezpieczeństwa. Często są pomijane, co sprawia, że stają się podatne na ataki. Syteca automatyzuje wykrywanie takich ukrytych kont w środowiskach Windows Server oraz Active Directory, a następnie bezpiecznie włącza je do systemu zarządzania poufnymi danymi.

Po ich integracji hasła są rotowane, co zapobiega nieautoryzowanemu dostępowi i zapewnia zgodność z wymaganiami bezpieczeństwa. Zespoły ds. bezpieczeństwa mogą następnie ocenić i zdecydować, czy nieautoryzowane konta należy dezaktywować bądź też całkowicie usunąć , ograniczając tym samym ryzyko potencjalnych zagrożeń.

02 Minimalizacja ryzyka dzięki monitorowaniu kont uprzywilejowanych

Zagrożenia wewnętrzne stanowią poważne wyzwanie dla organizacji, zwłaszcza w kontekście kont uprzywilejowanych. Syteca odpowiada na to zagrożenie poprzez ciągłe monitorowanie Active Directory w celu wykrywania nowych uprzywilejowanych kont.

Odnalezione konta są zabezpieczane za pomocą uwierzytelniania dwuskładnikowego (2FA), nagrywania sesji oraz kontroli dostępu opartej na rolach (RBAC). Dzięki tym mechanizmom tylko autoryzowani użytkownicy mogą uzyskiwać dostęp do wrażliwych systemów, a wszystkie działania są rejestrowane i podlegają audytowi. Takie proaktywne podejście pozwala organizacjom wcześnie wykrywać podejrzane zachowania i skutecznie minimalizować ryzyko.

03 Zabezpieczanie „uśpionych” kont

Nieaktywne lub porzucone konta często pozostają niezauważone, co czyni je wysoce przystępnym celem dla cyberprzestępców. Na przykład - konto byłego pracownika może nadal być aktywne i podatne na wykorzystanie.

Zautomatyzowane narzędzia Syteca identyfikują takie uśpione konta, integrują je z systemem zarządzania poufnymi danymi i rotują poświadczenia, aby odciąć nieautoryzowany dostęp. W rzeczywistych scenariuszach ta funkcjonalność pomogła organizacjom eliminować luki w zabezpieczeniach wynikające z przeoczenia, zapewniając, że żadne nieaktywne konto nie pozostaje narażone na zagrożenia.

04 Zarządzanie zewnętrznymi administratorami baz danych (DBA)

Organizacje często polegają na zewnętrznych wykonawcach, takich jak administratorzy baz danych (DBA) pracujący na zasadzie outsourcingu, aby utrzymać krytyczne systemy. Tacy kontraktorzy wymagają tymczasowego, ale bezpiecznego dostępu do odizolowanych sieci. Syteca ułatwia ten proces poprzez połączenie serwerów pośredniczących (Jump Servers), integrację z systemami zgłoszeń (system Help-Desk) oraz mechanizmy kontrolowanego dostępu. Kontraktorzy mogą uzyskiwać dostęp wyłącznie do określonych zasobów za pośrednictwem uprzednio zatwierdzonych procedur, a hasła są rotowane po każdym użyciu. Nagrywanie sesji zapewnia pełną rejestrację wszystkich działań, gwarantując transparetność i jasno przedstawiany audyt.

05 Poprawa bezpieczeństwa w sektorze opieki zdrowotnej

W środowisku opieki zdrowotnej kluczowe znaczenie ma zabezpieczenie dostępu do elektronicznej dokumentacji medycznej (EDM). Szpitale i kliniki wykorzystują rozwiązania Syteca do egzekwowania rygorystycznych kontroli dostępu, takich jak uwierzytelnianie dwuskładnikowe (2FA) oraz ograniczenia czasowe dostępu, dzięki czemu tylko upoważniony personel może uzyskać dostęp do danych pacjentów w godzinach pracy. Dodatkowo, funkcje audytu pozwalają administratorom monitorować i przeglądać wszystkie działania związane z danymi wrażliwymi, pomagając organizacjom w utrzymaniu zgodności z regulacjami branżowymi, takimi jak HIPAA.

06 Bezpieczny transfer plików dla agencji marketingowych

Współpraca z zewnętrznymi dostawcami często wymaga tymczasowego dostępu do wrażliwych systemów. W przypadku agencji marketingowej Syteca umożliwia bezpieczny transfer plików za pośrednictwem serwera FTP. Dostęp jest przyznawany wyłącznie za pośrednictwem systemu zarządzania danymi poufnymi (zarządzanie sekretami), a każda prośba przechodzi ręczny proces zatwierdzania, zapewniający jej dokładną weryfikację. Hasła są rotowane po każdym użyciu, a sesje nagrywane do celów audytowych. Takie podejście umożliwia agencjom bezpieczną współpracę bez narażania poufnych danych klientów na niepotrzebne ryzyko.

Przyszłość PAM

Krajobraz cyberbezpieczeństwa szybko się zmienia, a zarządzanie uprzywilejowanym dostępem (PAM) znajduje się na czele tych zmian. Organizacje stoją przed rosnącą presją, by zabezpieczać swoje dane uwierzytelniające, jednocześnie poruszając się w złożonych ekosystemach IT oraz spełniając wymagania regulacyjne. Transformacja Syteca i jej zdolność do obsługi różnorodnych przypadków użycia pokazują zaangażowanie firmy w rozwiązywanie tych wyzwań.

Koncentrując się na użyteczności, skalowalności i praktycznych zastosowaniach, Syteca dostarcza organizacjom narzędzia do eliminowania kluczowych luk w zabezpieczeniach. Niezależnie od tego, czy chodzi o wykrywanie kont Shadow IT, minimalizowanie zagrożeń wewnętrznych czy zabezpieczanie dostępu dla podmiotów trzecich, Syteca pokazuje, jak rozwiązania PAM mogą ewoluować, by sprostać wymaganiom współczesnych organizacji dbających o bezpieczeństwo.

W miarę nasilającej się konkurencji na rynku PAM, rozwiązania takie jak Syteca odegrają kluczową rolę w pomaganiu organizacjom w osiąganiu celów w zakresie bezpieczeństwa. Dzięki kompleksowemu zestawowi funkcji i nowatorskiemu podejściu Syteca jest doskonale przygotowana do redefinicji zarządzania uprzywilejowanym dostępem w XXI wieku.

Autor materiału

Paul Fisher

Paul Fisher jest Głównym Analitykiem, który prowadzi badania głównie w zakresie cyberbezpieczeństwa oraz zarządzania tożsamością i dostępem (IAM). Studiuje również trendy w AI, IoT i zarządzaniu danymi dla różnych sektorów przemysłu, w tym motoryzacyjnego. Paul jest odpowiedzialny za zarządzanie odpowiednimi badaniami ilościowymi w KuppingerCole. Jest także dziennikarzem i analitykiem IT od 1991 roku. W tamtym czasie pełnił funkcję redaktora naczelnego kilku ważnych tytułów IT i biznesowych w Wielkiej Brytanii. Pracował również jako konsultant ds. komunikacji z IBM, HP Enterprise Security Services, Sky UK i innymi wiodącymi firmami w projektach dotyczących bezpieczeństwa danych i IT.

Zarządzaj dostępem uprzywilejowanym z Syteca