ManageEngine
ADAudit Plus

Inspekcja zmian z analizą zachowań użytkowników (UBA)

Zapewnij ochronę i zgodność usługi Active Directory, serwerów Windows, serwerów plików i stacji roboczych

www.adauditplus.com

Co to jest ADAudit Plus?

ManageEngine ADAudit Plus to działające w czasie rzeczywistym oprogramowanie do inspekcji i prawozdawczości o następujących funkcjach:

- Monitorowanie usługi Active Directory (AD), Azure AD, serwerów plików systemu Windows, serwerów członkowskich i stacji roboczych oraz pomoc w przestrzeganiu rozporządzeń, w tym ustawy o przenośności i odpowiedzialności w ubezpieczeniach zdrowotnych (HIPAA), RODO, ustawy Sarbanesa-Oxleya (SOX), kalifornijskiej ustawy handlowej o prywatności konsumentów (CCPA), ustawy Gramma–Leacha–Bliley'a (GLBA) oraz innych regulacji.

- Zamiana surowych i niejasnych danych dziennika zdarzeń w praktyczne i generowane po kilku kliknięciach raporty, które informują o działaniach poszczególnych użytkowników oraz o czasie i miejscu ich wykonania w ekosystemie Windows.

- Identyfikacja nieprawidłowej aktywności oraz wykrywanie potencjalnych zagrożeń dla przedsiębiorstwa za pomocą analizy zachowań użytkownika (User Behaviour Analytics, UBA).

Jak ADAudit Plus może pomóc organizacji?

Za pomocą ManageEngine ADAudit Plus można:

1. Wyświetlać szczegółowe raporty na temat zmian lokalnych oraz w usłudze Azure AD.
2. Uzyskać wgląd w aktywność logowania użytkownika Windows.
3. Raportować, analizować i usuwać blokady konta AD.
4. Uważnie monitorować aktywność użytkowników z uprawnieniami w domenie.
5. Śledzić proces logowania/wylogowywania, zmiany użytkowników, grup itp.
6. Przeprowadzać inspekcję aktywności plików w systemach pamięci Windows, NetApp, EMC i Synology.
7. Udoskonalać system wykrywania zagrożeń za pomocą metody analizy zachowań użytkownika (UBA).
8. Pozyskiwać wstępnie spakowane raporty inspekcji na potrzeby realizacji wymogów ustaw SOX, HIPAA, standardu PCI DSS, rozporządzenia RODO oraz innych regulacji.

Główne funkcje ADAudit Plus

1. Inspekcja i raportowanie zmian w AD i Azure AD.
2. Inspekcja serwera plików (Windows, NetApp, EMC, Synology).
3. Inspekcja zmian w ustawieniach zasad grupy.
4. Inspekcja i sprawozdawczość dla serwera Windows i serwera członkowskiego.
5. Inspekcja stacji roboczych.
6. Analiza zachowań użytkowników (UBA).
7. Monitorowanie użytkowników z uprawnieniami.

Inspekcja Active Directory

Raportowanie zmian w obiektach AD oraz obiektach zasady grupy (GPO); śledzenie aktywności logowania użytkownika, analiza blokad konta i nie tylko.

www.adauditplus.com

Inspekcja AD

- **Inspekcja wszystkich zmian w obiektach AD:** monitoruj zmiany w zakresie jednostek organizacyjnych, użytkowników, grup, komputerów oraz innych obiektów AD z wglądem w stare i nowe wartości zmienionych atrybutów.

- **Śledzenie zmian w obiektach GPO:** poddawaj inspekcji zmiany w obiektach GPO oraz ich ustawieniach, w tym modyfikacje dotyczące konfiguracji komputerów, zasad haseł i blokad konta itp.

- **Monitorowanie aktywności logowania użytkownika:** generuj szczegółowe raporty na temat skutecznych i nieskutecznych prób logowania.

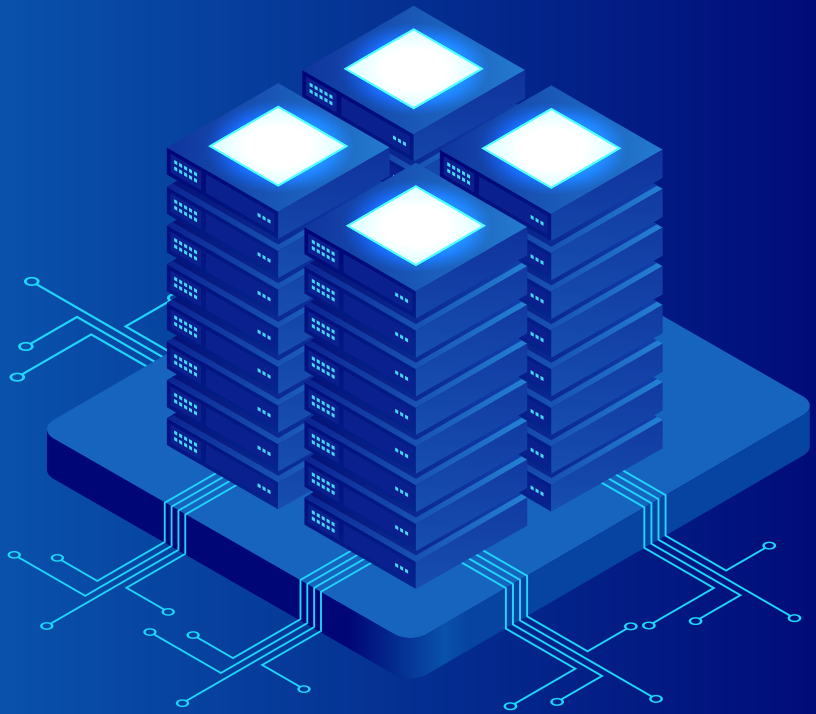
- **Usuwanie blokad kont:** szybko wykrywaj blokady konta za pomocą alertów oraz identyfikuj ich źródła dzięki obszernej liście składników systemu Windows.

- **Uzyskiwanie wglądu w wykorzystanie uprawnień:** uważnie kontroluj zakres wykorzystywania uprawnień w swoim przedsiębiorstwie, konsekwentnie przeprowadzając inspekcje kont użytkowników z uprawnieniami oraz zapisując szczegółowe dzienniki inspekcji.

- **Inspekcja hybrydowego środowiska AD:** generuj pojedynczy, skorelowany ogląd wszystkich działań w obrębie środowisk hybrydowych i otrzymuj alerty o kluczowych zdarzeniach.

Inspekcja serwera plików

Inspekcja i raporty na temat dostępu do plików i ich modyfikacji w urządzeniach pamięci masowej Windows, NetApp, EMC i Synology.



Inspekcja serwera plików

- **Monitorowanie dostępu do plików i folderów:** na bieżąco śledź aktywność wszystkich plików, w tym odczyty, usunięcia, modyfikacje, kopiowanie i wklejanie, przenoszenie i nie tylko.

- **Wykrywanie nieudanych prób dostępu do plików:** otrzymuj raporty na temat nieudanych prób dostępu, aby uzyskiwać dostęp do plików lub folderów.

- **Inspekcja zmian uprawnień:** śledź zmiany uprawnień do systemu plików NTFS i udostępniania wraz ze szczegółami, takimi jak stare i nowe wartości.

- **Monitorowanie integralności plików:** łatwo wykrywaj kluczowe zdarzenia, między innymi zmiany w określonym pliku wprowadzone przez konkretnego użytkownika, za pomocą wiadomości e-mail oraz alertów SMS poświęconych tym zdarzeniom.

- **Inspekcja udostępnień plików:** śledź każdą próbę dostępu i zmiany plików oraz folderów udostępnianych w domenie, a także pozyskuj szczegółowe informacje na temat tego kto uzyskał dostęp, do jakiej zawartości oraz kiedy i skąd to zrobił.

Inspekcja zmian w ustawieniach zasad grupy

Przeprowadzaj inspekcję zmian w ustawieniach zasad grupy, w tym kontroluj modyfikacje zasad haseł i blokad konta, zmiany komputerów itp.

Inspekcja zmian w ustawieniach zasad grupy

- **Inspekcja obiektów zasad grupy:** poddawaj inspekcji tworzenie, usuwanie, modyfikacje i inne działania związane z obiektami zasad grupy (GPO) i twórz na ten temat raporty.

- **Śledzenie zmian w ustawieniach obiektów GPO:** uważnie kontroluj, kto wprowadza zmiany do ustawień obiektów GPO oraz kiedy i skąd to robi, używając w tym celu kompleksowych raportów.

- **Konfiguruj alerty dotyczące krytycznych zmian:** otrzymuj błyskawiczne alerty e-mail i wiadomości SMS dotyczące krytycznych zmian, takich jak zmiany konfiguracji komputerów, zmiany zasad haseł oraz blokad konta itp.

- **Prowadzenie dzienników inspekcji:** generuj raporty na temat wartości ustawień GPO sprzed zmiany i po jej wprowadzeniu, aby natychmiast dostrzegać niechciane modyfikacje.

Inspekcja serwerów Windows

Monitorowanie serwerów członkowskich, za pomocą raportów i alertów w czasie rzeczywistym, w celu kontrolowania aktywności w sieci Windows.

Inspekcja serwerów Windows

- **Inspekcja serwerów Windows:** monitoruj zmiany lokalnych grup administracyjnych, lokalnych użytkowników, praw użytkowników, zasad lokalnych i nie tylko.

- **Śledzenie zaplanowanych zadań i procesów:** poddawaj inspekcji tworzenie, usuwanie i modyfikowanie zaplanowanych zadań i procesów.

- **Monitorowanie korzystania z urządzeń wymiennych:** identyfikuj przypadki podłączania nośników USB oraz przesyłania plików na wymiennych urządzeniach pamięci masowej.

- **Inspekcja procesów PowerShell:** monitoruj procesy PowerShell przebiegające na serwerach Windows wraz z realizowanymi w ich ramach poleceniami.

- **Usługi federacyjne Active Directory (ADFS):** raportuj udane oraz nieudane próby uwierzytelnienia ADFS w czasie rzeczywistym.

Inspekcja stacji roboczych

Śledzenie logowania i wylogowywania się użytkowników, aktywnych godzin pracy, danych historii logowania, korzystania z wymiennych urządzeń pamięci masowej i nie tylko.

Inspekcja stacji roboczych

- **nspekcja aktywności logowania i wylogowywania:** śledź aktywność logowania i wylogowywania w całej sieci Windows, rejestruj okres zalogowania oraz identyfikuj użytkowników, którzy są aktualnie zalogowani.

- **Śledzenie historii logowania użytkowników:** rejestruj każdy przypadek logowania, identyfikuj użytkowników zalogowanych do wielu urządzeń, monitoruj logowanie RADIUS i nie tylko.

- **Identyfikacja błędów logowania:** śledź wszystkie nieudane próby logowania z informacjami o tym, kto próbował się zalogować, na który komputer próbowano się zalogować, kiedy miało to miejsce i jaka była przyczyna niepowodzenia.

- **Monitorowanie integralności plików:** pozyskuj szczegółowe raporty na temat wszystkich zmian wprowadzonych do systemu i plików programu.

- **Pomiar wydajności pracowników:** śledź czas bezczynności pracowników oraz godziny aktywnej pracy, aby zapewnić wysoki poziom wydajności w całym przedsiębiorstwie.

Analiza zachowań użytkowników

Wykrywanie i ograniczanie ryzyka zagrożeń, takich jak nieuczciwe logowanie, penetracja sieci, nadużywanie przywilejów, naruszanie zabezpieczeń danych czy złośliwe oprogramowanie.

Wyszukiwanie zagrożeń za pomocą analizy UBA

- **Przetwarzanie dzienników w ramach całego środowiska:** zbieraj i przetwarzaj dzienniki ze skonfigurowanych kontrolerów DC, serwerów członkowskich oraz stacji roboczych.

- **Identyfikacja bezpiecznych schematów:** przetwarzane dane dziennika są wykorzystywane do tworzenia typowych dla użytkownika schematów logowania, plików, zarządzania użytkownikiem oraz działań procesowych.

- **Identyfikacja nieprawidłowości oraz ostrzeganie administratorów:** przychodzące dane dziennika oraz przetwarzane schematy są porównywane w celu wykrywania nieprawidłowości oraz powiadamiania administratorów, aby mogli prowadzić dalsze dochodzenie.

- **Wykrywanie potencjalnych zagrożeń bezpieczeństwa:** szybko dostrzegaj potencjalne przypadki nieuczciwego logowania, nadużywania uprawnień, eskalacji uprawnień, eksfiltracji danych, ataków złośliwego oprogramowania i nie tylko.

- **Automatyzacja reakcji na zdarzenia:** skracaj czas niezbędny do ograniczenia zakresu szkód, błyskawicznie wyłączając urządzenia i zamykając sesje użytkownika na podstawie zdarzeń bezpieczeństwa.

Monitorowanie użytkowników z uprawnieniami

Inspekcja kont użytkownika w domenie i rejestrowanie dzienników inspekcji, aby szybko wykrywać podejrzane zachowania.

Monitorowanie użytkowników z uprawnieniami

- **Inspekcja aktywności administratora:** śledź działania administracyjne użytkowników usługi Active Directory, między innymi w zakresie schematów, konfiguracji, użytkowników, grup, jednostek organizacyjnych (OU), zasad grupy obiektów (GPO).

- **Analiza aktywności użytkowników z uprawnieniami:** zachowuj zgodność z różnymi regulacjami IT, rejestrując dzienniki inspekcji dotyczące działań wykonywanych przez użytkowników z uprawnieniami w domenie.

- **Wykrywanie eskalacji uprawnień:** identyfikuj eskalację uprawnień dzięki raportom dokumentującym pierwsze skorzystanie z uprawnień przez użytkownika i weryfikuj, czy są one niezbędne w kontekście funkcji i obowiązków danego użytkownika.

- **Obserwuj nietypowe zachowania:** identyfikuj działania odbiegające od normalnych schematów dostępu, aby odnajdować atakujących, którzy wykorzystują ukradzione lub udostępnione poświadczenia uprawnionych kont.

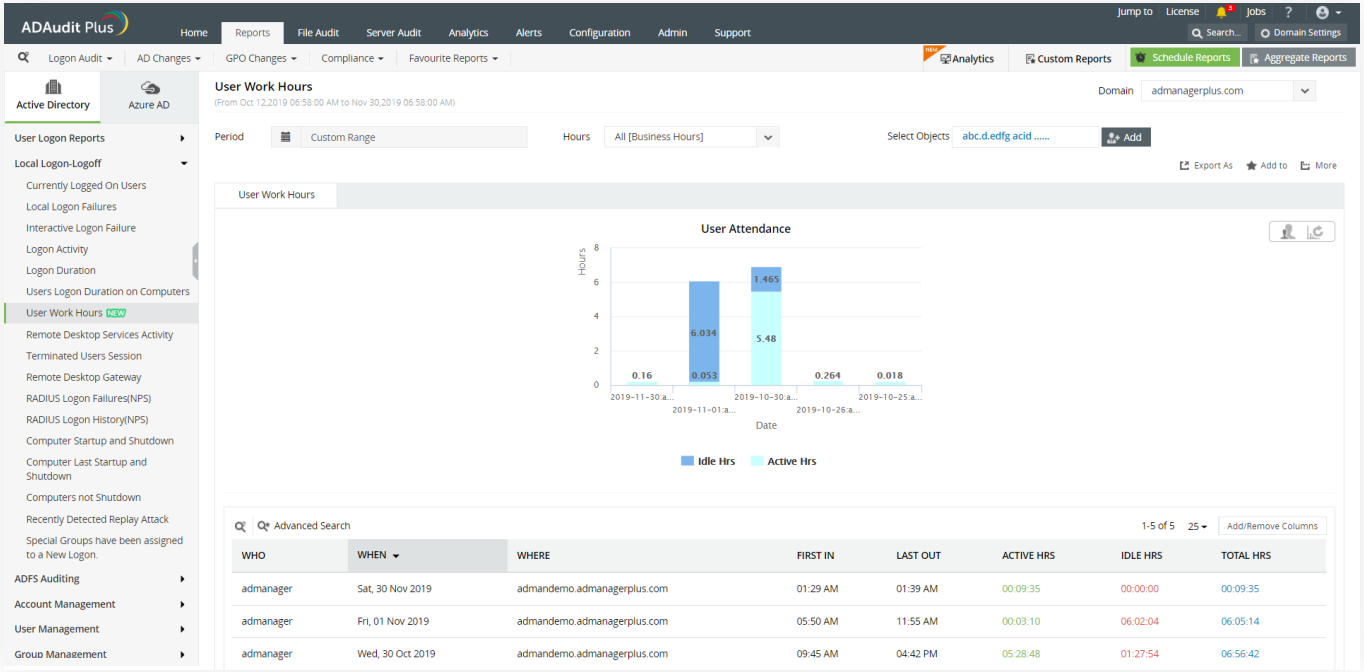
- **Otrzymywanie alertów o podejrzanej działalności:** szybko diagnozuj kluczowe zdarzenia, takie jak czyszczenie dzienników inspekcji albo uzyskiwanie dostępu do kluczowych danych poza godzinami pracy, a następnie reaguj na nie dzięki skonfigurowanym alertom.

Najpopularniejsze funkcje

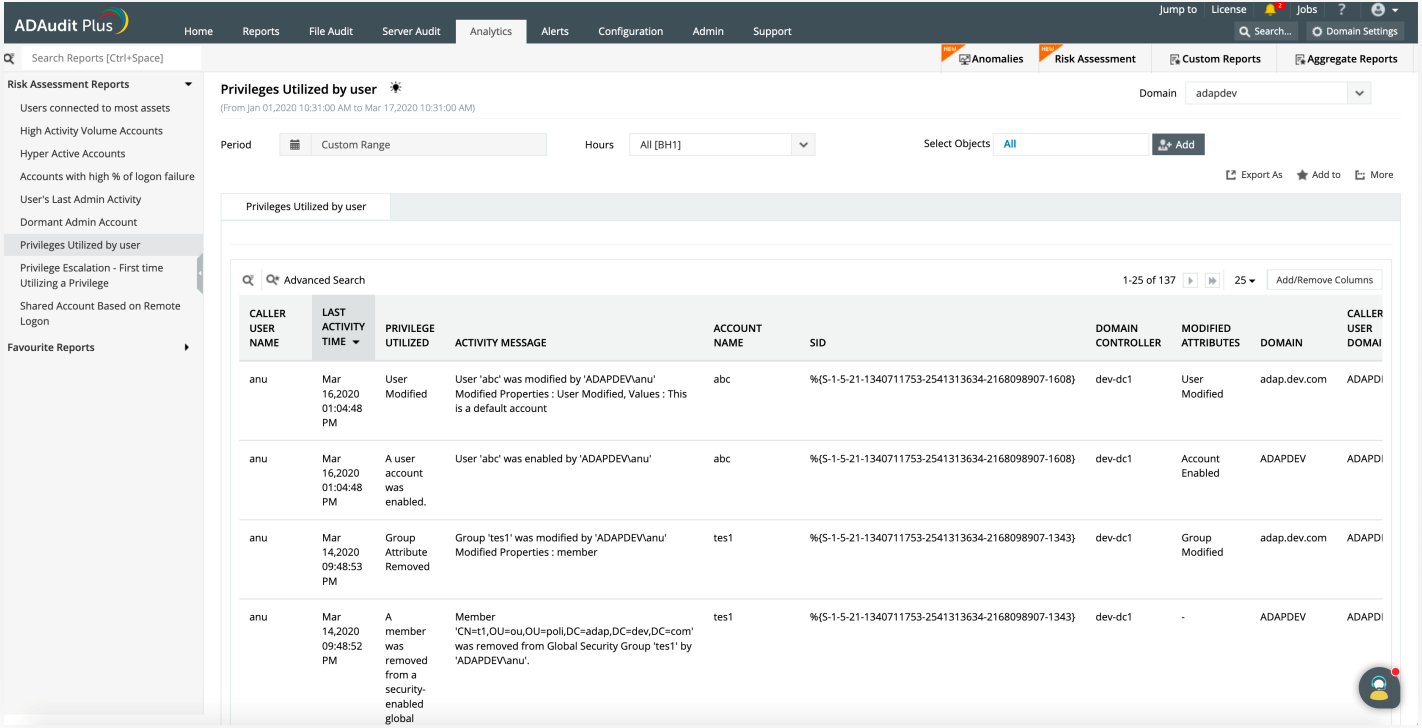
Przegląd funkcji najczęściej wybieranych przez klientów.

Więcej funkcji, które uwielbiają nasi klienci

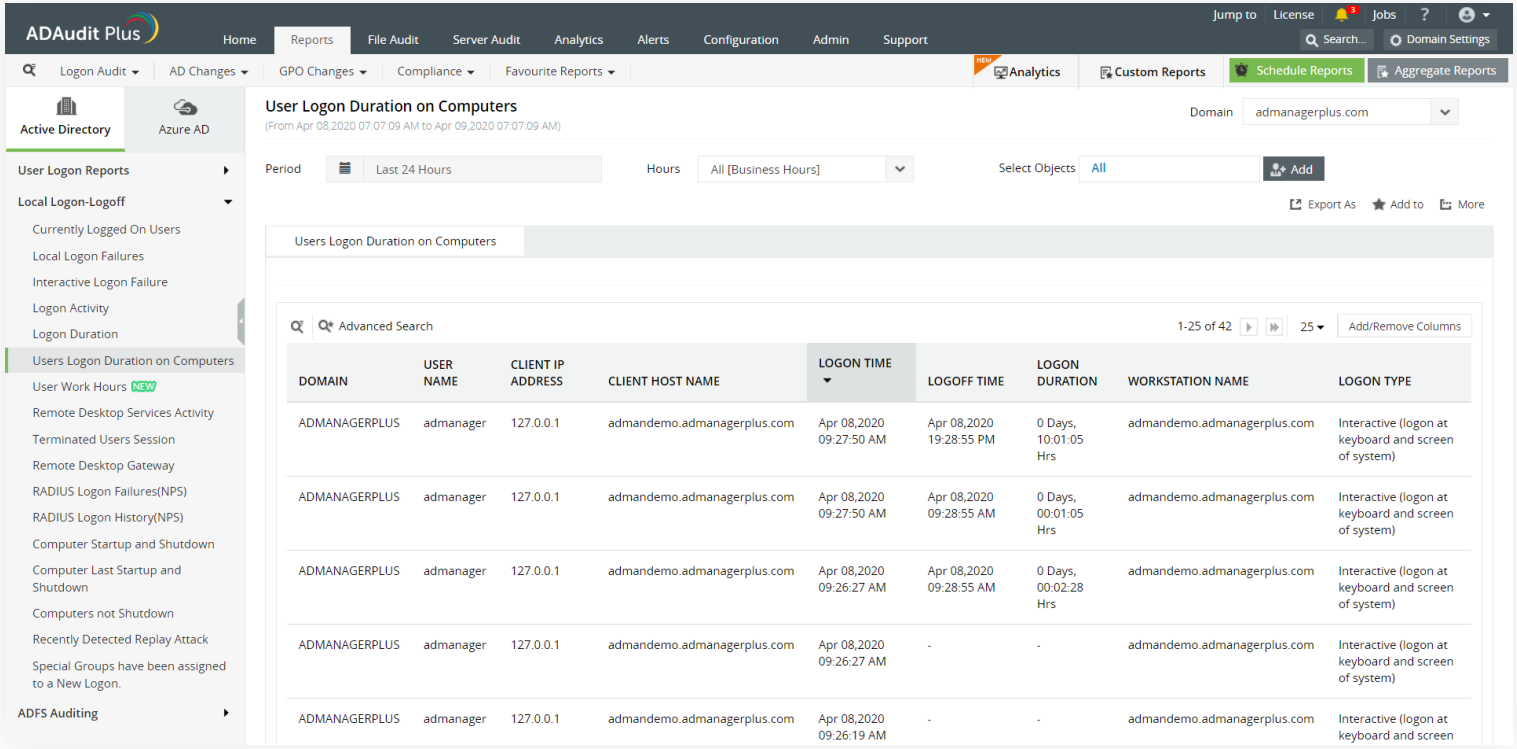
- **Monitorowanie godzin roboczych użytkownika:** monitoruj obecność, czas aktywności, czas bezczynności oraz czas wydajnej pracy pracowników używających dowolnego komputera w środowisku firmowym.



- **Wykrywanie zagrożeń wewnętrznych:** natychmiast wykrywaj przesłanki o zagrożeniach wewnętrznych, takie jak nieuczciwe logowanie, nadużywanie uprawnień, penetracja sieci, nieprawidłowe wykorzystanie danych i nie tylko.



- **Śledzenie logowania/wylogowania:** pozyskuj charakterystyczne dla danego użytkownika informacje na temat czynności logowania i wylogowywania, sprawdzaj użytkowników zalogowanych na wielu komputerach i wyświetlaj adresy IP oraz czasy logowania.



Dlaczego ADAudit Plus się wyróżnia?

- **Natychmiastowe alerty:** otrzymuj błyskawiczne powiadomienia e-mail i SMS na temat kluczowych zdarzeń i działań związanych z krytycznym użytkownikiem.

- **Wykrywanie zagrożeń i reagowanie na nie:** silnik UBA szybko wykrywa nadużywanie uprawnień, ataki wewnętrzne, złośliwe oprogramowanie i inne zagrożenia oraz pozwala odpowiednio na nie reagować.

- **Ponad 250 raportów:** ułatw zachowanie zgodności z wieloma wymogami prawnymi, w tym ze standardem PCI DSS, ustawami HIPAA, SOX i GLBA, rozporządzeniem RODO, normą ISO 27001 oraz z innymi aktami legislacyjnymi, a wszystko dzięki raportom gotowym do inspekcji.

- **Archiwizacja dzienników i analiza dochodzeniowa:** archiwizuj dane logowania w lokalizacji wyznaczonej przez użytkownika i generuj na jej podstawie raporty, gdy zajdzie taka potrzeba.

- **Pierwszorzędny zespół wsparcia klienta:** nasz wydajny zespół wsparcia odpowiada na pytania w wiadomości e-mail, podczas rozmowy telefonicznej lub za pomocą chatu.

Obsługiwane platformy

Inspekcja DC oraz serwera członkowskiego	File auditing	Other components
Wersja serwera Windows: • 2003/2003 R2 • 2008/2008 R2 • 2012/2012 R2 • 2016/2016 R2 • 2019	• Windows Server 2003 i nowsze wersje • Inspekcja EMC: VNX, VNXe, Celerra, Unity, Isilon • Inspekcja Synology: DSM 5.0 i nowsze wersje • Inspekcja użytkownika archiwizującego NetApp Filer: Data ONTAP 7.2 i nowsze wersje • Inspekcja klastra NetApp Cluster: Data ONTAP 8.2.1 i nowsze wersje	• Inspekcja AD FS: AD FS 2.0 i nowsze wersje • Inspekcja stacji roboczych: Windows 10, 8, 7, Vist oraz XP • Inspekcja PowerShell: PowerShell wersje 4.0, 5.0

Dostępne wersje

Standard	Professional	Free
Pobierz 30-dniową wersję próbną	Pobierz 30-dniową wersję próbną	Pobierz bezpłatną edycję
Raporty i alerty dotyczące danych dziennika zdarzeń zebranych z niżej wymienionych licencjonowanych składników: • Kontrolery domeny • Dzierżawy usługi Azure AD • Serwery Windows • Stacje robocze • Serwery plików systemu Windows • Serwery Synology NAS • Użytkownicy archiwizujący NetApp • Serwery plików EMC	Zawiera wszystkie funkcje wersji standardowej, a także: • Analizę blokady konta • Śledzenie zmian w ustawieniach zasad grupy • Wartości wcześniejszych i późniejszych zmian obiektów/atrybutów AD • Inspekcja zmian uprawnień AD • Śledzenie zmian DNS • Śledzenie zmian w schematach i konfiguracji AD itp.	Zawiera wszystkie funkcje wersji profesjonalnej i jest ważna przez 30 dni od daty instalacji. Ponadto: • Nie wygasa • Oferuje raporty inspekcyjne dla maksymalnie 25 stacji roboczych • Umożliwia generowanie raportów z danymi dziennika zdarzeń zebranymi w okresie ewaluacji/licencjonowania

Szczegóły licencji

Licencja ADAudit Plus na składnik inspekcyjny Active Directory jest uzależniona od liczby kontrolerów domeny.

Inne dodatki zależą od liczby niżej opisanych elementów:

- Dzierżawy usługi Azure AD
- Serwerów plików
- Serwerów plików EMC/ Użytkowników archiwizujących NetApp Filers/ Serwerów Synology NAS
- Serwerów członkowskich
- Stacji roboczych

Pomoc przy ocenie

Istnieje wiele sposobów, jak możemy pomóc użytkownikowi w ocenie ADAudit Plus. Oto one:

- Bezpłatna, w pełni funkcjonalna 30-dniowa wersja próbna.
- Przedłużenie licencji ewaluacyjnej, o ile jest to potrzebne.
- Wsparcie techniczne 24x5 oraz wersje demonstracyjne z instrukcjami.
- Aktywna wersja demonstracyjna hostowana w witrynie demo.adauditplus.com.
- Szczegółowe wskazówki dotyczące instalacji i konfiguracji.
- Obszerna baza wiedzy.

Dziewięć z dziesięciu spółek z listy Fortune 100 powierzyło nam zarządzanie swoimi rozwiązaniami IT.

Ponadto mamy dowody na swoją skuteczność

narzędzie ADAudit Plus zostało uznane za najczęściej wybierane przez klientów rozwiązanie SIEM w rankingu Gartner Peer Insights Customer's Choice z 2019 roku.

ManageEngine
ADAudit Plus

Jak sami mówią

To skuteczne rozwiązanie internetowe w dobrej cenie. Podoba nam się funkcja inspekcji użytkownika archiwizującego
NetApp Filer. Ponadto, wybór częściowo ułatwił nam fakt, że jesteśmy zadowoleni z innych doskonałych produktów ManageEngine".

Ricky Chand,
inżynier ds. systemów, Bank of South Pacific, Fiji

TZanim zaczęliśmy korzystać z ADAudit Plus, nie mieliśmy wglądu w naszą infrastrukturę AD. Teraz możemy monitorować wszystkie transakcje AD pod kątem zmian grup, tworzenia użytkowników, zabezpieczeń, dzienników uwierzytelnień i innych elementów".

Callixtus Muanya,
administrator systemu Windows, Harvard Medical School

Read more of our customers' testimonials here.

Kontakt

Telefon
+48 61 622 23 94

Wyślij wiadomość e-mail do zespołu wsparcia
sprzedaz@mwtsolutions.eu

Odwiedź naszą witrynę
www.manageengine.com/pl/active-directory-audit/

Adres pocztowy
MWT SOLUTIONS S.A. ul. Szyperska 14, 61-754 Poznań

Bezpłatna, w pełni funkcjonalna 30-dniowa wersja próbna.

Pobierz ADAudit Plus