ZARZĄDZANIE UPRAWNIENIAMI ADMINISTRATORA Z ROZWIĄZANIEM

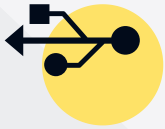
Admin By Request

SECURIVY

Spis treści

1. Po co odwoływać lokalne uprawnienia administratora użytkownikom końcowym?

Użytkownicy z uprawnieniami administratora mogą stać się celem ataku cyberprzestępców. Nadmierne możliwości konfiguracji systemu lub aplikacji krytycznych niosą za sobą również zagrożenia utraty danych oraz przestojów w pracy. Odpowiedzialne zarzadzanie dostępem jest zatem podstawą bezpieczeństwa firmy. Aby podnieść jego poziom należy kierować się zasadą najmniejszego uprzywilejowania (PoLP), zgodnie z którą użytkownicy powinni otrzymać tylko taki poziom dostępu, jaki jest im potrzebny do właściwego wykonywania swoich obowiązków zawodowych.



Odbieranie uprawnień administratora może wywoływać opór ze strony pracowników, którzy nabiorą przekonania, że wdrożenie PoLP jest oznaką braku zaufania ze strony kadry kierowniczej przedsiębiorstwa. Nic bardziej mylnego. Celem zarządzania dostępem nie jest utrudnianie pracy użytkownikom końcowym.

Nadanie uprawnień zgodnych z zajmowanym stanowiskiem to przede wszystkim sposób na zminimalizowanie powierzchni ataku, a także zmniejszenie prawdopodobieństwa jego wystąpienia.

Brak dostępu do krytycznych zasobów firmy takich jak aplikacje, dane i sieć pozwala również obniżyć dotkliwość cyberataku, gdy będzie miał miejsce. Kontrola portów USB zapobiega zaś zawirusowaniu sprzętu oraz ogranicza rozprzestrzenianie się złośliwego oprogramowania.

PoLP umożliwia również zapobieganie kopiowaniu poufnych danych na dyski zewnętrzne. Zasada najmniejszego uprzywilejowania zapewnia także większą stabilność pracy. Użytkownicy znajdujący się na niskich poziomach w hierarchii uprawnień nie są w stanie dokonać zmian w aplikacjach i systemach, co redukuje czas przestojów w pracy spowodowanych błędami po stronie użytkowników korzystających z krytycznych aplikacji

Odpowiednie zarządzanie dostępem pozwala wnieść nową jakość bezpieczeństwa w struktury organizacji. Profil PoLP powinien być jednak przemyślany i wdrożony przy pomocy nowoczesnych narzędzi. W ten sposób stworzone hierarchie uprawnień odpowiadają specyficznym potrzebom przedsiębiorstwa, a użytkownicy pozostają wydajni i produktywni bez stwarzania przestrzeni do ataków i nadużyć wewnętrznych.

2. Jak przygotować się do wdrożenia zarządzania dostępem?

Wdrożenie zasady najmniejszego uprzywilejowania wymaga podejścia procesowego. Audyt całego ekosystemu bezpieczeństwa pozwoli zlokalizować konta użytkowników posiadających nadmierne uprawnienia oraz wyznaczyć pracowników, którzy powinni mieć dostęp do konkretnych danych i zasobów firmowych.

Opracowanie profilu uprawnień użytkowników powinno być poprzedzone następującymi czynnościami:

A. Zlokalizuj wszystkich użytkowników, którzy posiadają uprawnienia administratora

Przed zastosowaniem zasady najmniejszego uprzywilejowania należy wykryć wszystkie konta, które dysponują rozszerzonym dostępem. Warto zwrócić uwagę również na uprawnienia, które są przypisane do użytkownika poprzez członkostwo w grupach lub strukturach organizacji. Takie działanie ma na celu zidentyfikowanie luk bezpieczeństwa, które należy usunąć. Wiedza o pracownikach i urządzeniach, na których możliwy jest dostęp do kluczowych zasobów firmy pozwala zweryfikować zasadność przyznanych przywilejów i dokonanie zmian w ich udzieleniu.

B. Przeprowadź audyt oprogramowania i plików na sprzęcie firmowym

Swoboda w instalowaniu programów i wtyczek przez pracowników może powodować zagrożenia. Dlatego istotne jest poznanie metod pobierania plików oraz sprawdzenie czy pochodzą one ze sprawdzonych źródeł. Kontrola portów USB oraz zarządzanie uprawnieniami do pobierania i instalacji narzędzi umożliwia ograniczanie zagrożenia ze strony złośliwego oprogramowania.

C. Stwórz profile stanowisk i dopasuj konieczne do wykonywanych obowiązków uprawnienia

Domyślnie każdy z pracowników powinien mieć przyznane najmniejsze uprawnienia. Warto też stworzyć opisy stanowisk wraz z przywilejami koniecznymi do realizacji obowiązków zawodowych pozwala zmniejszyć obciążenie działu IT.

Dzięki temu można również określić, które uprawnienia są konieczne, aby użytkownik mógł wykonywać swoją pracę komfortowo i bez zakłóceń. Trzymanie się wytycznych znacząco redukuje przestrzeń podatną na zagrożenia i usprawnia proces przyznawania uprawnień pracownikom.

D. Skorzystaj z narzędzi, które pozwolą na automatyzację zarządzania

Po zweryfikowaniu poziomu uprawnień udzielanych na każdym szczeblu organizacyjnym można przejść do wdrażania zasady najmniejszego uprzywilejowania. Istnieje jednak grupa użytkowników, którzy potrzebują dodatkowych uprawnień do wykonywania okresowych zadań. Wówczas trzeba dać im możliwość złożenia prośby o nadanie wyższych uprawnień, potrzebnych do realizacji konkretnych obowiązków.
Admin by Request pozwala usprawnić proces przyznawania przywilejów poprzez nadawanie dodatkowych praw na żądanie.

3. Jak sprostać wyzwaniom związanym z odebraniem uprawnień administratora?

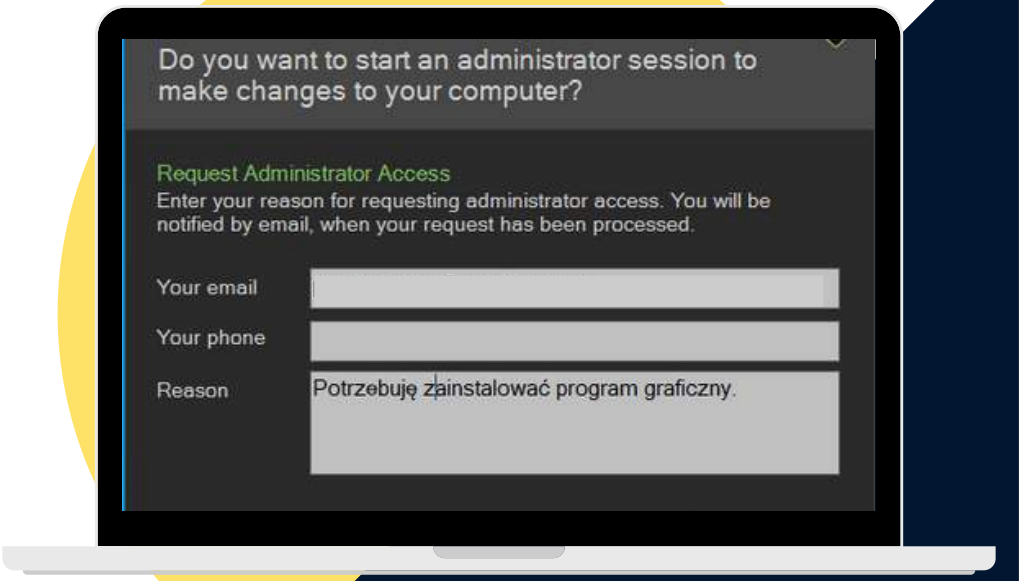
Przedsiębiorcy szukający rozwiązania pozwalającego na zarządzenie dostępem uprzywilejowanym powinni przede wszystkim wybrać narzędzia, które nie zakłócą produktywności zespołu. Użytkownicy muszą mieć możliwość żądania dodatkowych uprawnień a ich przyznawanie powinno odbywać się w czasie rzeczywistym. W ten sposób komfort pracy nie ulega pogorszeniu.

Użytkowników końcowych należy wcześniej poinformować, że zostaną im odebrane prawa administratora. Domyślnym poziomem uprawnień powinien być najniższy, który pozwoli wykonywać zadania zawodowe.

Istotną kwestią jest również poinformowanie pracowników o celu wdrażanych zmian. Zrozumienie ryzyka i kosztów włamania do krytycznych zasobów firmy umożliwia szybszą adaptację użytkowników do usprawnień w obszarze bezpieczeństwa. Celem zasady najmniejszego uprzywilejowania jest ochrona poufnych danych, sprzętu oraz zapewnienie ciągłości prowadzonej działalności. Nie odbywa się to kosztem osłabienia komfortu pracy oraz wydajności użytkowników końcowych.

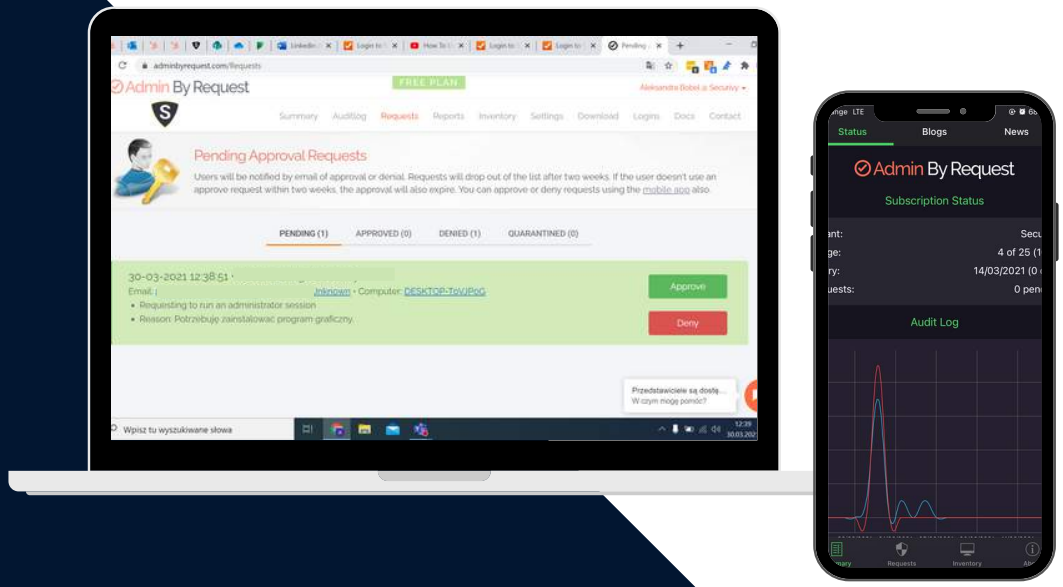
Skuteczne eliminowanie luk bezpieczeństwa jest możliwe dzięki nowoczesnym narzędziom do zarządzania dostępem. Admin by Request pozwala na nadawanie uprawnień użytkownikom, którzy tego potrzebują. Program umożliwia również wgląd w zmiany, których dokonał pracownik podczas sesji o podwyższanych uprawnieniach.

Zapisy logowań oraz dane dotyczące tego, jak z przyznanych uprawnień korzystają użytkownicy końcowi umożliwiają zlokalizowanie nieodpowiedniego używania wyższych przywilejów. W ten sposób narzędzie redukuje przestrzeń do nadużyć, wyłudzenia danych oraz pozwala szybko reagować w przypadku, gdy dostęp do konta użytkownika znajdzie się w posiadaniu osób nieuprawnionych.



4. Czym jest program Admin By Request?

Admin by Request to oprogramowanie do zarządzania dostępem uprzywilejowanym, za pomocą którego można usunąć lokalne uprawnienia administratora z kont użytkowników końcowych. W ten sposób możesz łatwo wdrożyć zasadę najmniejszego uprzywilejowania, wygodnie obsługując wyjątkowe potrzeby Twoich pracowników.



Admin by Request daje możliwość, aby:

- **Użytkownik końcowy uzyskał podwyższone uprawnienia do wykonania żądanej czynności, tylko wtedy, kiedy jest to konieczne**
- **Zainteresowany mógł uruchomić krytyczną aplikację na swoim komputerze**
- **Grupa użytkowników uzyskała dostęp do wyższych uprawnień (np. pracownicy działu IT)**
- **Użytkownik uzyskał dostęp do sesji o podwyższonych uprawnieniach na czas określony**

Rozszerzenie dostępnych uprawnień odbywa się ze ścisłym uwzględnieniem poniższych zasad:

- **Izolacja uprawnień: Konto wykorzystywane do wykonywania codziennych czynności powinno mieć najmniejsze uprawnienia**
- **Dostęp „just in time”: Uprzywilejowany dostęp można uzyskać tylko wtedy, gdy jest to konieczne do wykonywania obowiązków zawodowych**
- **Adekwatne uprawnienia: dostęp uprzywilejowany powinien być wystarczający do wykonania konkretnego zadania, bez nadawania zbyt wysokich przywilejów**
- **Dostęp ograniczony czasowo: uprawnienia należy przyznawać tylko na czas potrzebny do wykonania zadania**
- **Uzasadnione żądania: dostęp uprzywilejowany powinien być dobrze uzasadniony, aby zostać zatwierdzony**
- **Audyt wykonywanych aktywności: zapisy logowań oraz dane dotyczące tego, jak z przyznanych uprawnień korzystają użytkownicy końcowi**

Admin By Requst wyróżnia się spośród innych produktów Privileged Access Management (PAM), ponieważ jego zaimplementowanie nie wymaga zmian w architekturze sieciowej. Narzędzie jest proste i intuicyjne, dzięki czemu korzystanie z niego jest możliwe bez wielogodzinnych szkoleń pracowników. Dział IT nie musi także spędzać czasu na instalacjach zdalnych. Definiowanie białych list oraz polityki dozwolonych aktywności jest o wiele prostsze niż dotychczas. Łatwość wdrożenia Admin by Request i jego przystępna cena są cenione przez użytkowników, dzięki czemu należy on do najszybciej rozwijających się rozwiązań PAM na rynku.

Admin By Request

5. Wdrożenie programu Admin By Request

Twórcy Admin By Request zadbali o to, aby korzystanie z programu było intuicyjne na każdym etapie jego użytkowania. Wdrożenie tego rozwiązania jest bardzo proste. Wystarczy uruchomić plik instalacyjny. Proces nie wymaga żadnej dodatkowej konfiguracji, można go również przeprowadzić za pomocą narzędzi do instalacji zdalnej, takich jak SCCM, Intune, i innych. Rozwiązanie integruje się także z usługami domenowymi Active Directory i Azure AD. Pakiet instalacyjny waży 1.3 MB, co sprawia, że jest on możliwy do wdrożenia nawet na infrastrukturze o ograniczonych zasobach. Zarządzanie Admin By Request odbywa się w chmurze, dzięki czemu z narzędzia mogą korzystać przedsiębiorstwa o różnej wielkości i odmiennych profilach prowadzonej działalności.

6. Funkcje programu Admin By Request

A. Zezwól użytkownikom na uzyskanie wyższych uprawnień

Administrator może udzielić dostępu pracownikom, którzy tego potrzebują.
Jest to podstawowa funkcja Admin By Request, która pozwala odciążyć pracowników IT od bezpośredniego przeprowadzania wielu instalacji. Żądana aktywność jest przechwytywana przez program, który udziela dostępu do jej wykonania bez nadawania pracownikowi pełnych praw administratora lokalnego. Działalność użytkownika końcowego, który korzysta z podwyższonych uprawnień jest monitorowana w czasie rzeczywistym, co pozwala chronić zasoby firmy przed nadużyciami.

Admin By Request umożliwia również nadanie uprawnień do wykonywania działań na oprogramowaniu, które jest już zainstalowane na komputerze. Użytkownik może poprosić o odpowiednie uprawnienia poprzez przycisk „uruchom jako administrator”.

B. Konfiguruj zestawy uprawnień dla różnych grup użytkowników

Wiele organizacji potrzebuje różnych polityk dostępu dla konkretnych działów. Admin By Request daje możliwość tworzenia ustawień podrzędnych, które mogą zastępować powszechne konfiguracje uprawnień.

Narzędzie umożliwia także zdefiniowanie pracowników, którzy nie mogą wnieść o podniesienie uprawnień lub zdefiniować grupę osób, które mogą to zrobić. Praktyczne zastosowanie powyższej funkcjonalności jest następujące:

- **Białe listy definiowane w ramach programu Admin By Request umożliwiają różnym grupom użytkowników dostęp do określonych aplikacji**
- **Grupa użytkowników może prosić o podwyższenie uprawnień do wykonania danej czynności**
- **Grupa (np. dział IT) ma prawo wnioskować o dostęp do pełnej sesji administracyjnej z podwyższonymi uprawnieniami**
- **Jest to możliwe dzięki funkcji określania zakresu globalnego dostępu i ustawień podrzędnych.**

C. Zezwól na rozpoczęcie sesji administracyjnej

Admin By Request daje możliwość zezwolenia użytkownikowi na rozpoczęcie sesji z uprawnieniami lokalnego administratora. Dostęp udzielany jest na określony czas, podczas którego pracownik może wykonywać swoje obowiązki zawodowe. Jest to funkcja, z której korzystają m.in. przedstawiciele działów IT oraz helpdesków. W ten sposób osoby, chcące przeprowadzić szereg czynności mogą realizować je w pełnym komforcie, bez konieczności kilkakrotnego wnoszenia o wyższe uprzywilejowanie.

D. Twórz białe listy

Poprzez Admin By Request można skonfigurować listę aplikacji, których używanie nie wymaga wyższych uprawnień. Dział IT może definiować i tworzyć listy programów, do których użytkownicy mają dostęp na prawach lokalnego administratora. Jest to wygodny sposób na zmniejszenie listy zapytań. Dodanie do białej listy dobrze znanych aplikacji oraz oprogramowania, z którego użytkownicy korzystają na co dzień pozwala podnieść komfort i płynność pracy.

E. Wykrywaj złośliwe oprogramowanie w czasie rzeczywistym

Gdy użytkownik zażąda uprawnień administratora, w celu przeprowadzenia instalacji programu lub uruchomienia aplikacji, agent Admin By Request wywołuje poprzez API skanowanie otwieranego pliku.

Ponad 30 silników antywirusowych dokonuje sprawdzenia aplikacji w czasie rzeczywistym, co pozwala ograniczyć niebezpieczeństwo zainfekowania środowiska pracy przez złośliwe oprogramowanie.
Rozwiązanie zaimplementowane w Admin By Request nie koliduje z programem antywirusowym zainstalowanym na komputerze użytkownika końcowego. Jest to możliwe dzięki przeniesieniu procesu wykrywania złośliwego oprogramowania do chmury.

F. Korzystaj z Admin By Request bez dostępu do Internetu

Oprogramowanie działa bez względu na to, czy komputer jest podłączony do sieci, czy działa w trybie offline. Istnieje możliwość podniesienia uprawnień poprzez kod PIN wygenerowany przez administratora. Użytkownik końcowy wpisuje kod, który pozwala mu na dostęp do zasobów wymagających wyższego uprzywilejowania.

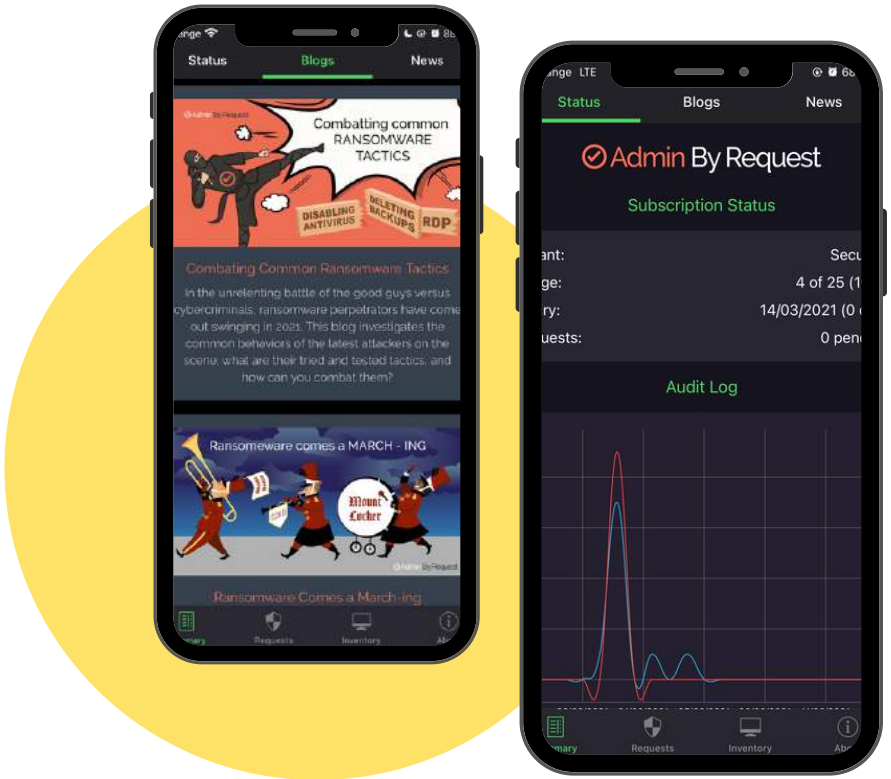
7. Aplikacja mobilna

Zarządzanie dostępem uprzywilejowanym może odbywać się z poziomu smartfona.
Wersja mobilna to pełna funkcjonalność., możesz za jej pomocą zobaczyć dane sesji administratora na klientach, co pozwala zidentyfikować nadużycia nawet bez dostępu do komputera. Kolejnym usprawnieniem są oczekujące, zatwierdzone i odrzucone żądania, które są widoczne w menu „Request". Pogląd żądań użytkowników końcowych możliwy jest do czasu wygaśnięcia wniosku lub rozpoczęcia sesji uprzywilejowanej.

Aplikacja dostępna jest w

Google Play

App Store



Z poziomu telefonu możesz zatwierdzić lub odrzucić prośbę. Użytkownicy wersji mobilnej dostają powiadomienia push, które informują ich o pojawiających się requestach. Z poziomu aplikacji można też konfigurować role użytkowników końcowych. Superużytkownik może zdecydować, kto ma wgląd w sesje oraz jakie osoby są uprawnione do zatwierdzania próśb.

8. Rozwijaj swój biznes wykorzystując najlepsze praktyki bezpieczeństwa IT

Admin By Request pozwala zrobić łatwy krok na drodze do zredukowania przestrzeni podatnej na zagrożenia wewnętrzne. Intuicyjne narzędzie umożliwia zadbanie o zarządzanie uprawnieniami lokalnego administratora bez konieczności przeprowadzania skomplikowanych wdrożeń i drogich audytów.

BEZPŁATNA LICENCJA DLA 25 STANOWISK
to możliwość przetestowania funkcji Admin By Request i przekonania się, że bezpieczeństwo Twojej firmy to temat, o który możesz zadbać bez działu IT.

CHCĘ ZAŁOŻYĆ DARMOWE KONTO

Skontaktuj się z naszym zespołem, aby uzyskać pełne wsparcie w obszarze dobierania odpowiednich programów do Twojego biznesu oraz kompleksowego wdrażania innowacyjnych rozwiązań, które pomogą chronić Twoją organizację przed nadużyciami.

Skontaktuj się z nami

+48 722 158 258

biuro@securivy.com

Poznaj więcej szczegółów o Admin By Request