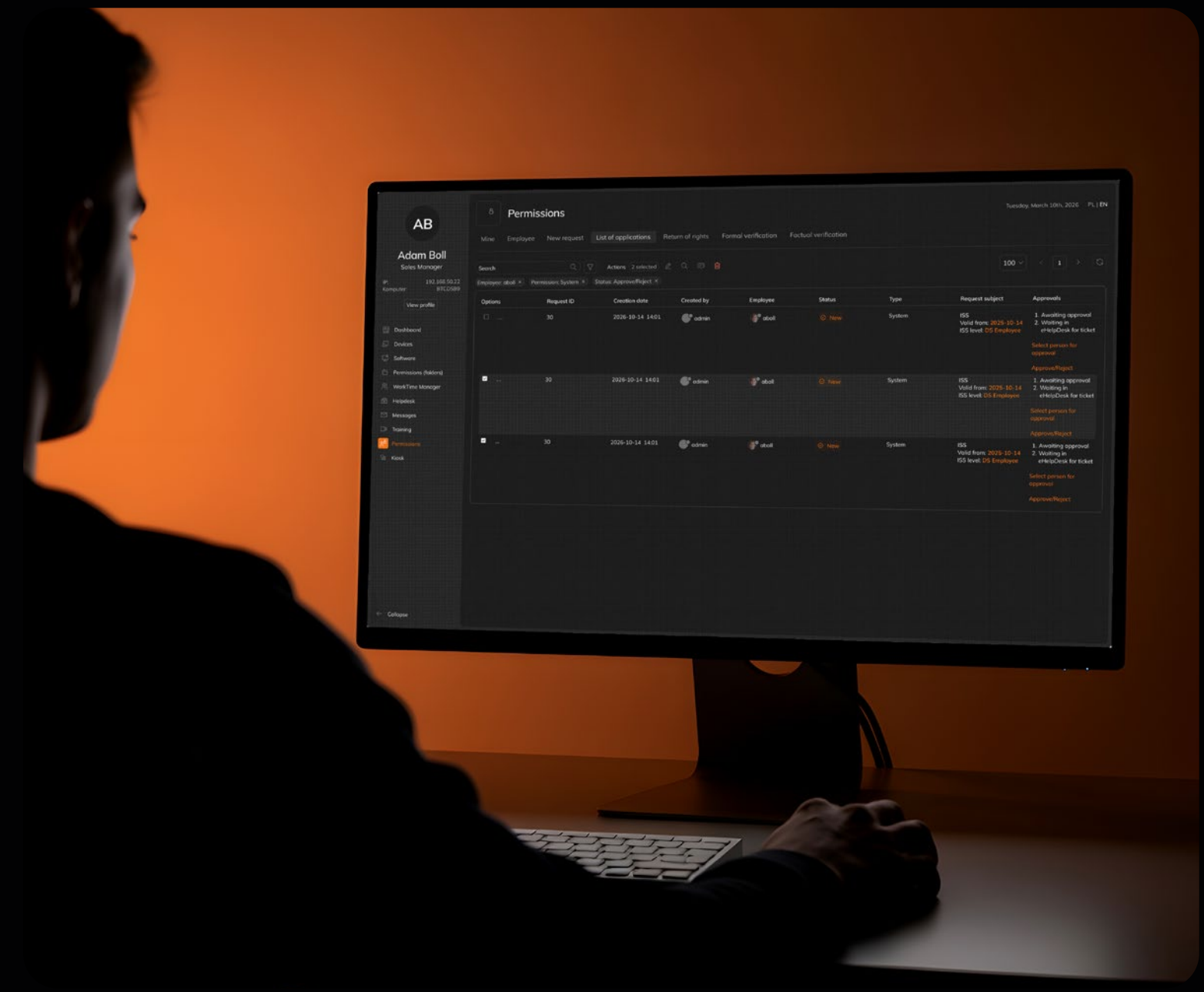


eAuditor IAM

System zarządzania tożsamością i dostępem do zasobów IT

eAuditor IAM przejmuje pełen cykl życia uprawnień pracownika: od pierwszego konta i przypisania profilu, przez czasowe rozszerzenia ról, aż po automatyczny zwrot dostępów przy odejściu z firmy. Wszystko w jednym miejscu, w pełni audytowalnie, z minimalnym obciążeniem działu IT.

WNIOSKUJ • AKCEPTUJ • AUDYTUJ • ODBIERAJ

Korzyści z wdrożenia

Zgodność z regulacjami
UKSC2 / NIS2 / ISO 27001 / DORA / KRI

System wprost odpowiada wymogom art. 8 UKSC2 (kontrola dostępu, MFA), NIS2, ISO 27001, DORA i Krajowych Ram Interoperacyjności: zasada least privilege, recertyfikacja, cykl życia tożsamości (JML), 2FA, kompletny ślad audytowy.

Mniej pracy operacyjnej w IT

Wniosek trafia do właściwej osoby automatycznie. Akceptacja, realizacja w Active Directory, powiadomienia mailowe – bez ręcznego procesowania zgłoszeń przez administratorów.

Audyt zawsze gotowy

Każda zmiana uprawnień jest rejestrowana. Cykliczne przypomnienia o weryfikacji nadanych dostępów. Raporty operacyjne i strategiczne wygenerujesz w kilka kliknięć – gotowe dla audytora i regulatora.

Mniej nadmiarowych dostępów

Dwuetapowa weryfikacja, uprawnienia czasowe i samodzielny zwrot uprawnień przez pracownika ograniczają zjawisko privilege creep i konta-sieroty.

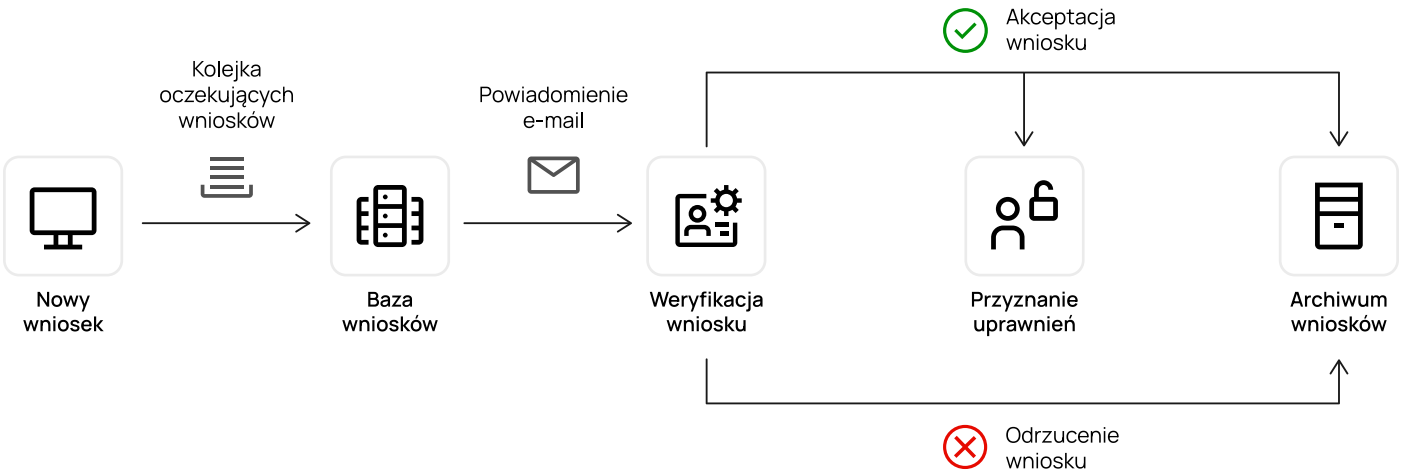
Ciągłość mimo nieobecności

Urlopy, zwolnienia, delegacje – system automatycznie wyznacza zastępcę i przekierowuje do niego wnioski oraz akceptacje. Proces nigdy nie czeka na powrót decydenta.

Elastyczność systemu

Pełna konfigurowalność na etapie wdrożenia – kartoteki, definicje uprawnień i ścieżki akceptacji tworzysz bez programisty. System obsługuje dostęp nie tylko do aplikacji IT, ale też do maszyn produkcyjnych, pomieszczeń czy sprzętu.

Funkcje systemu



Zarządzanie uprawnieniami

Wniosek o uprawnienia

Formularz z polami dynamicznymi, wybór pojedynczych aplikacji lub profili (grup uprawnień), data ważności OD i DO, historia statusów. Akceptacja w panelu lub bezpośrednio z poziomu e-maila.

Szablony zatwierdzeń

Definiowalne ścieżki akceptacji oparte na danych z Active Directory (login, stanowisko, dział). Jeden szablon obsługuje wiele definicji uprawnień, jednoznacznie wskazując decydenta dla każdego typu wniosku.

Audyt bilansu otwarcia

Import istniejących uprawnień z systemów źródłowych i Active Directory, dwuetapowa weryfikacja (formalna przez przełożonego, faktyczna przez IT).

Cykliczna recertyfikacja

Harmonogram automatycznych przeglądów uprawnień. System przypomina przełożonym o weryfikacji aktualnych dostępów ich zespołów. Każdy cykl kończy się raportem.

Automatyzacja i integracja

Automatyczne nadawanie uprawnień

Po akceptacji wniosku silnik PowerShell wykonuje skrypt: konto w domenie, hasło, dostęp do folderów współdzielonych, skrzynka e-mail — co tylko zdefiniujesz. Lista możliwości jest praktycznie nieograniczona.

Dwa narzędzia w jednym — IAM i eHelpDesk

Panel Pracownika oparty jest na rozwiązaniu eHelpDesk. Po akceptacji wniosku system automatycznie generuje zgłoszenie realizacyjne do właściwej grupy wsparcia — bez kopiowania danych między systemami. Pracownik z jednego miejsca składa wnioski o uprawnienia i zgłoszenia serwisowe; administrator IT widzi pełną historię obu w jednym narzędziu.

Dostęp i ciągłość

Panel Pracownika

Webowa aplikacja dostępna z pulpitu komputera — bez konieczności ponownego logowania. SSO domenowe rozpoznaje zalogowanego użytkownika. Pracownik widzi swoje uprawnienia, składa wnioski, śledzi ich status.

Moduł nieobecności i zastępstw

Kalendarz nieobecności, automatyczne wyznaczanie zastępcy, integracja z procesem akceptacji wniosków. Dla pracowników zatrudnionych na czas określony — blokada wniosków na okres dłuższy niż czas zatrudnienia.

Jak wygląda wdrożenie?

1

Poznajemy organizację

Spotykamy się i ustalamy, jakie systemy mają zostać objęte obiegiem uprawnień, kto akceptuje wnioski oraz jak wyglądają ścieżki decyzyjne w organizacji. Efektem jest mapa procesów przygotowana na miarę potrzeb.

2

Wdrażamy system w środowisku

Instalację przeprowadzamy zdalnie, w infrastrukturze (on-premise). Konfigurujemy kartoteki, definicje uprawnień oraz procesy.

3

Przeprowadzamy „pierwszy spis" — bilans otwarcia

Pobieramy aktualne uprawnienia z systemów źródłowych oraz Active Directory i poddajemy je dwuetapowej weryfikacji.
Po tym etapie po raz pierwszy w organizacji wiadomo dokładnie, kto i jakie uprawnienia posiada — oraz czy rzeczywiście powinien je posiadać.

4

Towarzyszymy po starcie. Wsparcie w standardzie SLA

W kolejnych miesiącach od uruchomienia produkcyjnego świadczymy usługę wsparcia obejmującą: bieżący monitoring pracy systemu, obsługę zgłoszeń serwisowych, korekty konfiguracji oraz dostrojenie procesów do realiów organizacji. Celem tego etapu jest pełna stabilizacja wdrożenia.

Integracje

- Microsoft Active Directory — struktura organizacyjna, użytkownicy, uwierzytelnianie domenowe (SSO).
- LDAP, CAS — uwierzytelnianie zewnętrzne.
- Uwierzytelnianie dwuskładnikowe (2FA) oraz weryfikacja dwuetapowa e-mail.
- eHelpDesk — kierowanie wniosków do grup wsparcia oraz wspólny Panel Pracownika.
- Bazy danych: MS SQL, MySQL, PostgreSQL, Oracle — import danych pracowników i uprawnień.
- Pliki źródłowe: CSV, Excel, XML, TXT — także przez ODBC.

Wymagania techniczne

- Model wdrożenia: on-premises — instalacja w infrastrukturze klienta.
- System operacyjny serwera: Ubuntu / Debian / RHEL / CentOS / Windows Server.
- Środowisko: JDK 8 (OpenJDK), Apache Tomcat 10.x.
- Baza danych: PostgreSQL 16.x.
- Sprzęt (minimum): 4-rdzeniowy CPU, 8 GB RAM, 20 GB przestrzeni dyskowej.
- Klient: dowolna nowoczesna przeglądarka (Chrome, Firefox, Edge) — bez instalacji oprogramowania na stacjach.

Model licencjonowania

System oferowany w modelu licencji wieczystej. Cena zależna od liczby administratorów systemu (kont uprawnionych do administrowania) oraz liczby użytkowników występujących w procesach (zwykle = liczbie kont w MS Active Directory).

Zapraszamy do kontaktu!

Skontaktuj się z naszymi Managerami Sprzedaży IAM, aby umówić bezpłatną prezentację lub otrzymać ofertę dopasowaną do Twojej organizacji.

Wojciech Jakubowski
Manager Sprzedaży IAM

wjakubowski@btc.com.pl
tel.: 91 481 72 26
kom.: 500 114 607

Daria Lorek
Manager Sprzedaży IAM

dlorek@btc.com.pl
tel.: 91 481 72 21
kom.: 797 440 524

Dowiedz się więcej

www.eauditor.eu/IAM