



# Całościowe zarządzanie tożsamością i dostępem do aplikacji i systemów – od A do Z

Tomasz Surmacz

Sales Manager

[Tomasz.Surmacz@microfocus.com](mailto:Tomasz.Surmacz@microfocus.com)

# Micro Focus Identity & Access Management

– kompletny stos rozwiązań



**Zarządzanie tożsamością,  
uprawnieniami,  
przebiegami i audyty**



Access Request



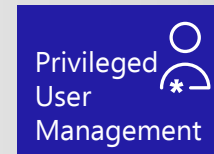
Access Certification



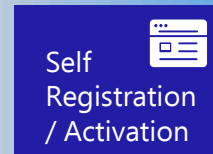
Workflow Orchestration



Business Policy Management



Privileged User Management



Self Registration / Activation



Intelligent Decision Support



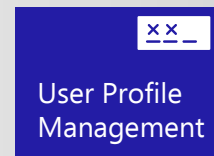
Identity Life cycle



Collection & Fulfillment



Role Mining & Management



User Profile Management



Evidence & Compliance

REST APIs  
Common UI



**Kontrola dostępu,  
uwierzytelnianie**



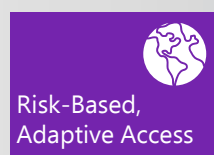
Access Enforcement



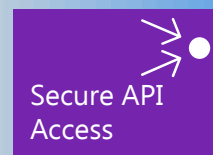
Multi Factor Authentication



Mobile Access



Risk-Based, Adaptive Access



Secure API Access



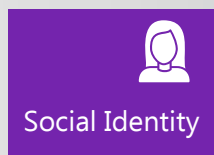
Reporting



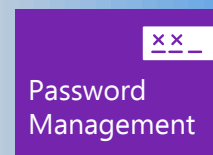
Single Sign-On



Federation



Social Identity



Password Management



**Zarządzanie i monitorowanie  
dostępu uprzywilejowanego**



Privileged Access Management



User Activity Monitoring



Group Policy Management



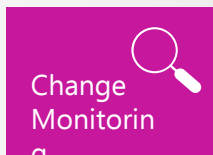
Secure API Access



File Integrity Monitoring



Analytics



Change Monitoring



Delegated Administration



Audit & Compliance



Admin Session Recording



Activity Monitoring

**Kontrola dostępu –  
wydawałoby się, że  
jest...**



PASSWORD

\* \* \* \* \*

Hasła nie zapewniają już bezpieczeństwa,  
jak więc wzmocnić kontrolę dostępu?

# Istotne elementy procesu uwierzytelniania

## 1. Coś co wiesz:

- Hasła
- Kody PIN
- Pytanie + znana Ci odpowiedź

Jacek01

12345678

1234

3004

080808

Qwertyui

Haslo123

@#%~&\*()

Gdzie się urodziłam?

Name of your first pet?

## 2. Coś co masz przy sobie

- Karty bezdotykowe
- Karty inteligentne
- Smartfony (SMS/tekst, głos)
- FIDO U2F, tokeny USB
- Tokeny OTP, tokeny HW
- Smartfon wraz z **apką dla mobilnych urządzeń**



## 3. Coś Twojego (biologicznie)

- Odcisk palca
- Głos
- Tęczówka oka
- Kształt twarzy
- Podpis





# Micro Focus NetIQ Advanced Authentication

Nie musisz traktować wszystkich użytkowników w ten sam sposób!



- Centralnie określasz, jakie metody mogą lub muszą być zastosowane w organizacji
  - Ty decydujesz, dla jakich systemów i kiedy będzie wymagane wieloskładnikowe uwierzytelnianie
  - Obsługujesz całe środowisko w firmie oraz dostępy do usług u operatorów w chmurze
  - Możesz łatwo dodać 2FA do istniejącej infrastruktury dostępu z zewnątrz przez VPA
- Środki bezpieczeństwa, takie jak uwierzytelnianie 2FA czy MFA, są skuteczne tylko wtedy, gdy są łatwe do zaakceptowania przez użytkowników

# NetIQ Advanced Authentication

*Aplikacje na smartfony (Android, iOS)*

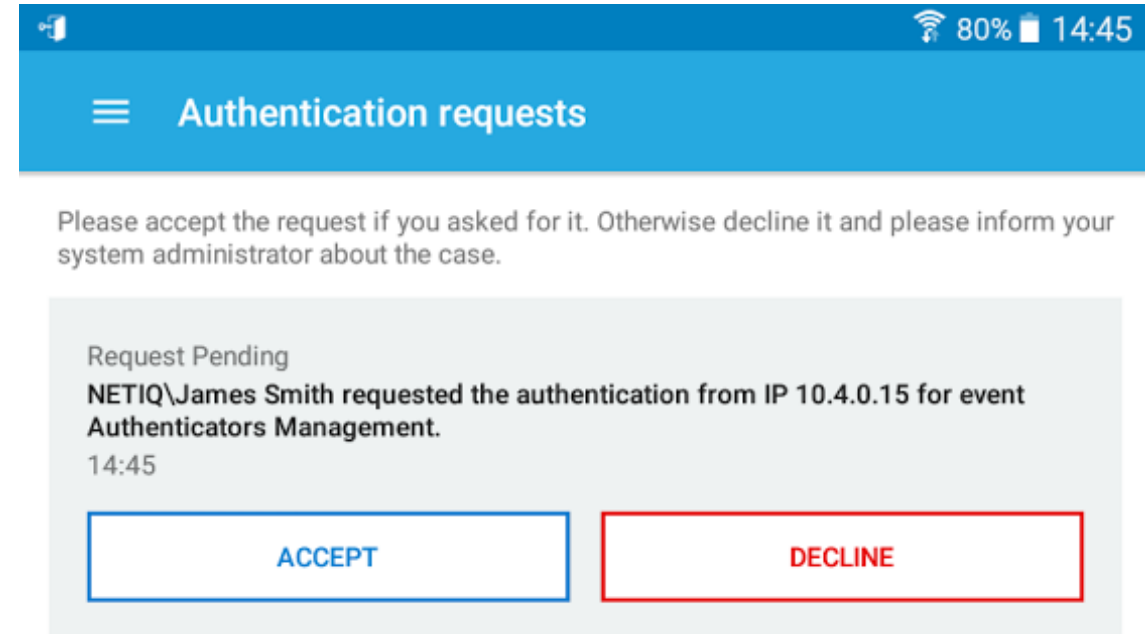
Prosta w użyciu aplikacja

Tylko dwa przyciski:

AKCEPTUJ lub ODRZUĆ

Uwierzytelnianie przygotowane dla użytkowników biznesowych

Hasło jednorazowe w przypadku braku połączenia



# Wsparcie dla FIDO i FIDO2

## Universal Second Factor (U2F)

- **ŁATWE W UŻYCIU I SZYBKIE** (szyfrowanie w urządzeniu)
- **Bezpieczeństwo:** odporność na phishing, ataki podsłuchowe man-in-the-middle
- **Pragmatyczne podejście:** już teraz przystępna cena, spadające koszty sprzętu
- **Szybkość dla użytkownika:** szybkie szyfrowanie w urządzeniu (krzywa eliptyczna)
- **Pomyśl tak:** „To karta inteligentna opracowana ponownie pod kątem nowych potrzeb użytkowników sieci”





# NetIQ Advanced Authentication i karty zbliżeniowe

- Użytkownik może korzystać z kart zbliżeniowych z czytnikiem USB
- Wygoda, łatwość użycia
- Karta zabezpieczona kodem PIN
- Tap-N-Go
- Możliwość buforowania hasła domeny MS
- Użytkownik może używać tylko karty + PIN do logowania się do komputera



# Współpraca z Office 365 i chmurą Azure



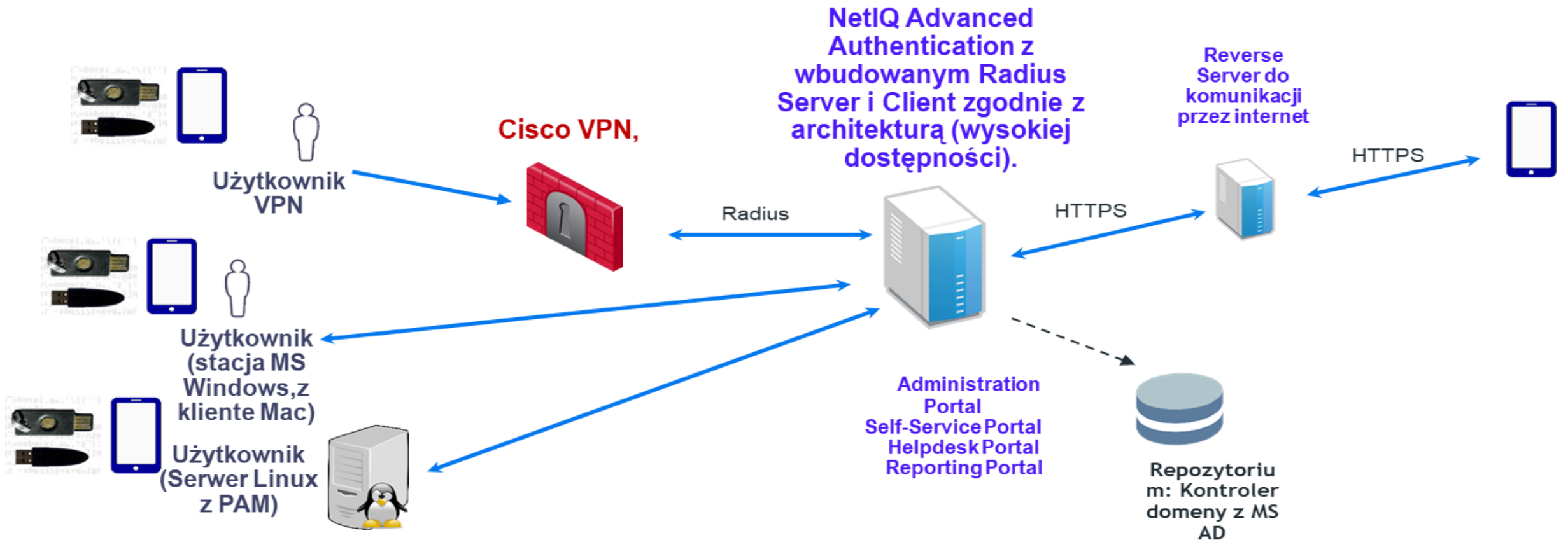
- NetIQ Advanced Authentication współpracuje z SAML i ADFS
- Wszystkie metody są wspierane w celu integracji z Office 365

## Chmura Azure

- Łatwość integracji z Azure
- Wsparcie dla OpenID Connect w celu konfiguracji w Azure
- To samo dla innych serwisów (Google, Facebook...)

# Dostęp przez VPN z wykorzystaniem NetIQ Advanced Authentication

Wspierane są metody Remote Access



# Współpraca NetIQ Advanced Authentication z serwerem Microsoft IIS

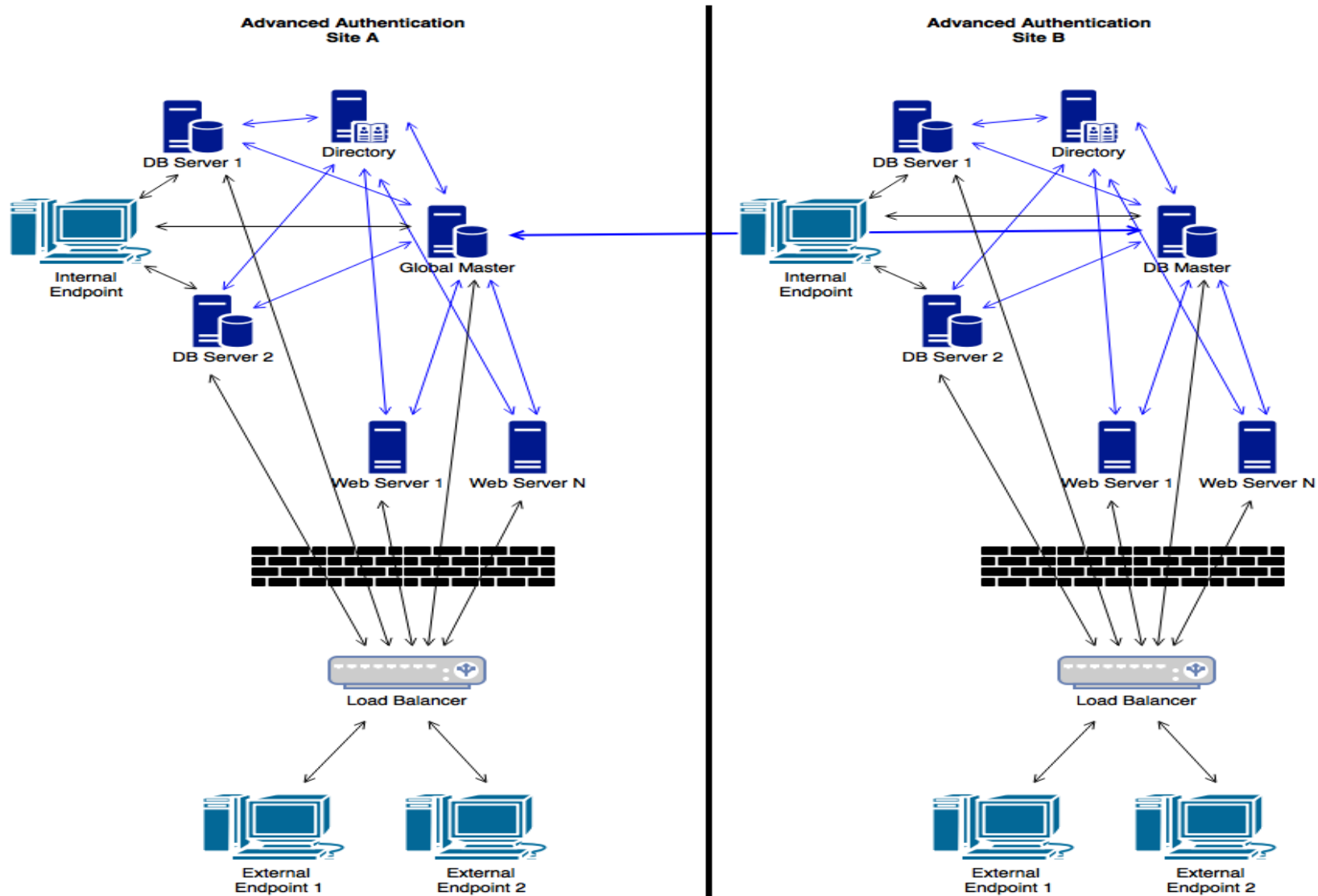
- Gotowa wtyczka dla serwera Microsoft IIS
- Użytkownicy, którzy chcą uzyskać dostęp do stron internetowych, muszą przeprowadzić uwierzytelnianie wieloczynnikowe na serwerze
- Przykład wykorzystania:
  - Zabezpieczenie dostępu do Outlook Web Access (OWA)
  - Zabezpieczenie dostępu do aplikacji udostępnianych przez Remote Desktop Web (RDWeb)

# Obsługa bardzo wielu metod uwierzytelniania

Metody				Kluczowe funkcje			Kluczowe funkcje		
Smartphone Out-Of-Band push to iOS, Android or Windows Phones	Geo-Fencing Smartphone Based GPS Location validation	FIDO U2F "Fast Identity Online" for Chrome / API	Bluetooth Device-in-Range login and lock for Windows	Windows Hello Support Win10 Hello Methods (Win)	Multi-Tenant - Support Multi Divisions or Clients	AWS / Azure Public Cloud Deployment options	ADFS ADFS Plug-in Integration	Windows CP Credential Provider Win 7, 8 and 10	Citrix Devices Citrix Device Redirection Support
Out-of-Band Agent Out-of-Band	Google Auth. External Google Authenticator OTP	Microsoft Live External Microsoft Live OATH / OTP	Voice OTP Voice-call delivered OTP	SMS OTP ADFS Short Message Service delivered OTP	SAML Connect application via SAML2	RADIUS Internal RADIUS Server and RADIUS Client	REST Light Weight Programming Interface	Mac OSX OS X Authentication Plug-in	Citrix SSO Facilitate user authentication to Citrix App/Session
Face Face Biometrics on Windows 8/10	Soft Token Application OATH Based TOTP / HOTP	Hard Token Device OATH Based TOTP / HOTP	PKI-PKCS7 Smartcard (or other) w/Certificate Validation (Win, Lin, Mac)	PKI-PKCS11 Smartcard (or other) w/Certificate Validation (Win, Lin, Mac)	OAuth2 Connect applications via Open Authorization Token / Open ID	FIPS 140-2 "FIPS Inside" via OpenSSL FIPS Module	Caching Second Factor Skipping for admin specified window of time	Linux PAM RPM and DEB modules	Card Tool Identity found cards with a tap
NFC 13,56 MHz Cards, Tokens, etc. (Win, Lin, Mac)	RFID 125 kHz Proximity Cards, Tokens, etc. (Win, Lin, Mac)	Emergency PW Helpdesk Assisted Password	Email OTP Email Delivered OTP	Swisscom External Swisscom Smartphone PKI Authentication	Impersonation Linked Account Authenticator	HTTP Proxy Secure AA Behind Network with Proxy	Dashboard Customizable Administration Console	RDP / Term Svcs Card and PKI Redirection	Off-Line Workstation Login (Win, Mac, Linux)
RADIUS Client Interface with existing RADIUS solutions	Voice Call Voice Call with Prompt for User PIN validation	Challenge User Enrolled Challenge/Response	PIN Code User enrolled PIN Code as a Factor	BankID Swedish BankID (PKI) support	Incorporate Mobile SDK to integrate with any App	App. Policy Mobile App Policy Enforcement	Localization User facing interface strings all localized	Tap-N-Go Windows Login / Logout with card tap (and PIN Caching)	BYOD Non-domain Workstation Support
Fingerprint Windows Biometric Framework	Fingerprint Support MS Modern Keyboard with Biometrics	Fingerprint Lumidigm / MD Direct API Integration	Fingerprint Digital Persona Driver Based Integration	Fingerprint NEXT Biometrics Direct API Integration	Kerberos SSO with Kerberos ticket Systems To Consoles	ReCaptcha Force Google ReCaptcha for Web based events	Token Standalone Token administration	NIST Use NIST Biometric Image Software	
SAML SAML Federated validation	OAuth2 OpenID Connect validation	TouchID Mac OSX TouchID Fingerprint	Fingerprint Mobile device fingerprint verification		AAaaS MFA Available as-a-Service	ConnectWise Partner Dashboard Integration for NMM-to-MSP's	Migration Export / Import configuration		

# Zaawansowana architektura NetIQ AA

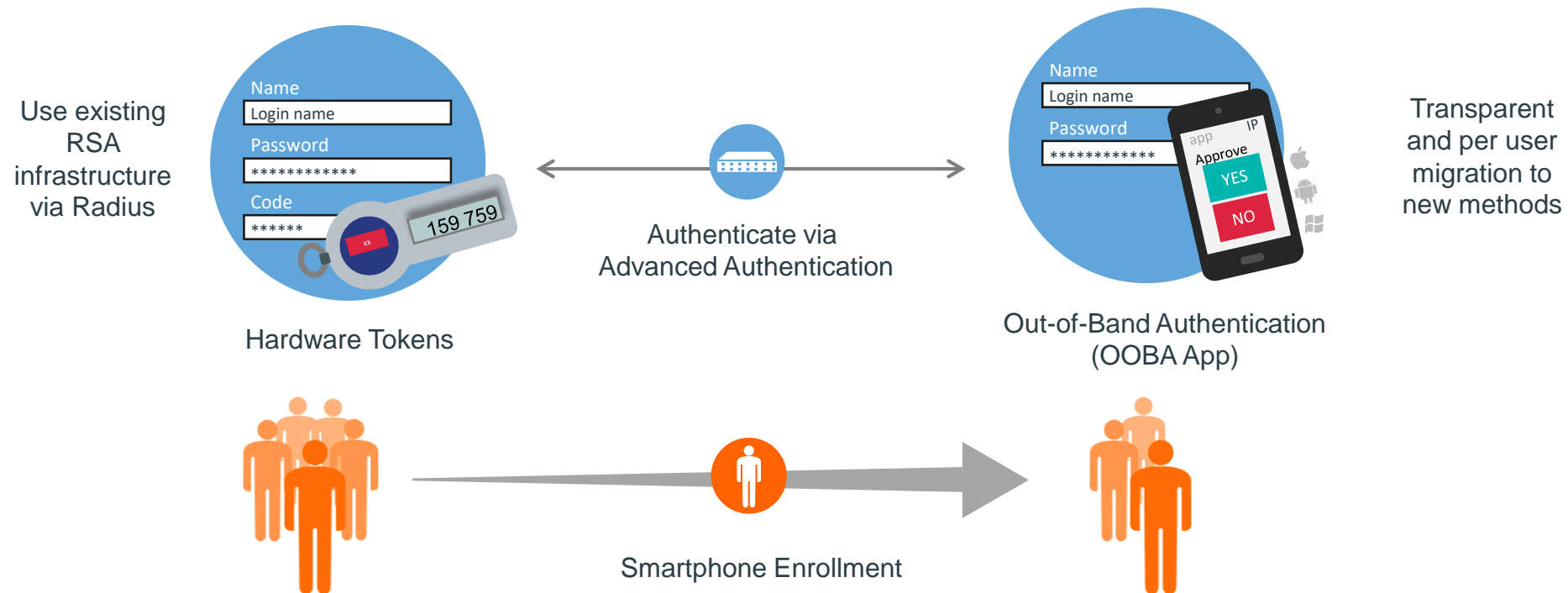
*Równoważenie obciążenia i obsługa wielu oddziałów (replikacja)*





# Przykład koegzystencji i migracji z RSA (tokeny sprzętowe) do NetIQ AA z uwierzytelnianiem przez smartfon

Płynne przejście oraz duża redukcja kosztów



## **Kolejne scenariusze dodania 2FA: mamy aplikacje i systemy, które nie można zintegrować za pomocą standardowych interfejsów**

Do dyspozycji pozostaje nam dostępny nadal wraz z NetIQ AA interfejs REST API

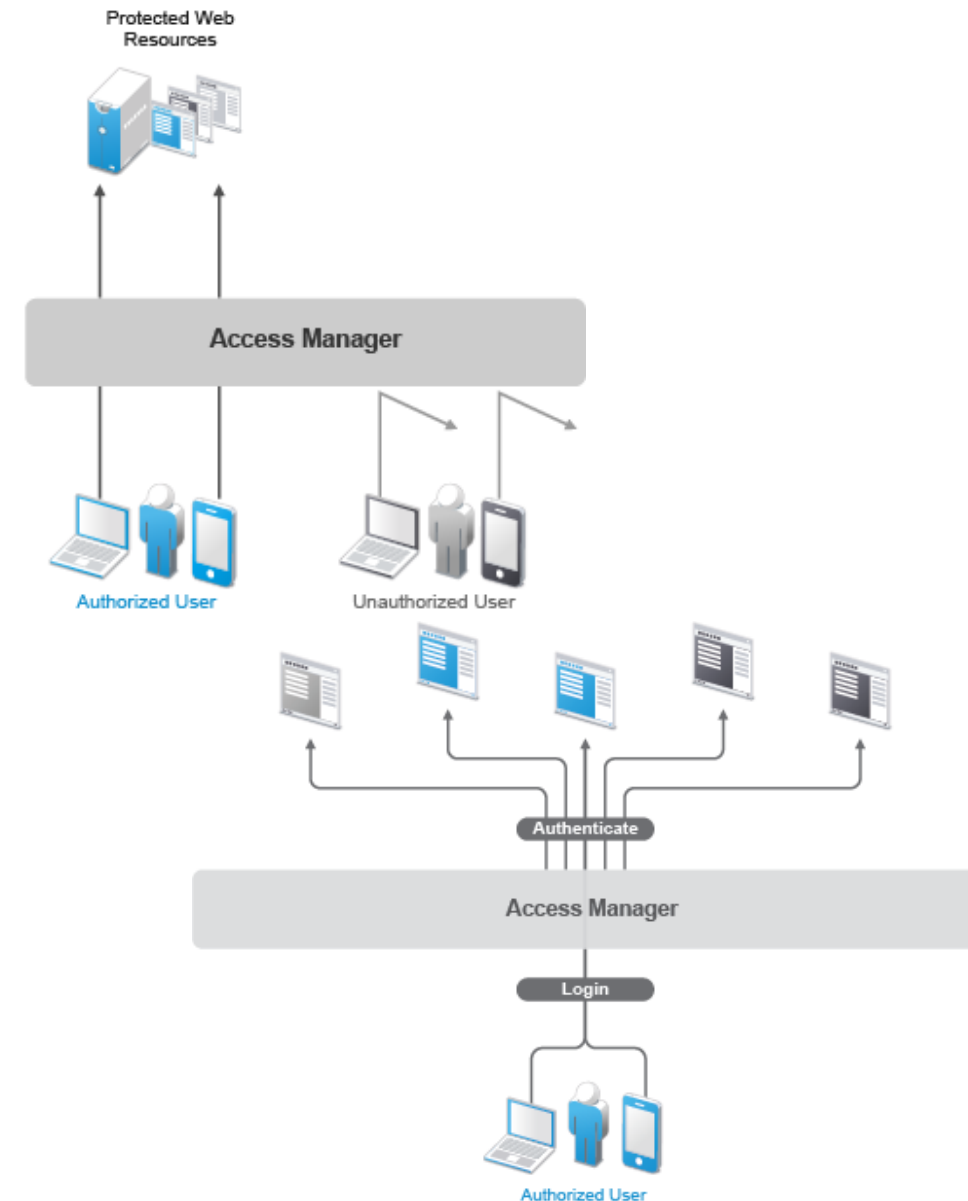
*lub*

Jeszcze prostszy sposób, nie wymagający programowania i ingerencji w kod aplikacji:

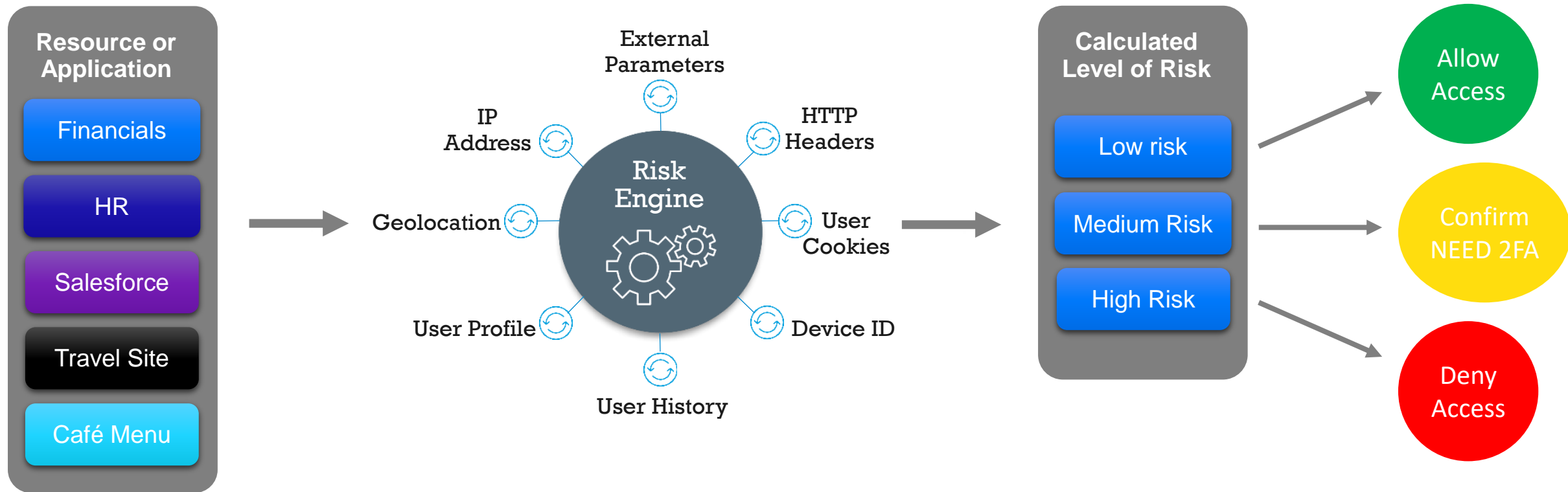
- Wykorzystanie Micro Focus NetIQ Access Manager dla dowolnych aplikacji webowych
- Wykorzystanie Micro Focus SecureLogin (SSO) dla dowolnych aplikacji z grubym klientem, dostępem przez emulator terminala lub webowych

# Potrzeby, które zaspokaja NetIQ Access Manager

- Kontrola dostępu do aplikacji i serwisów www wewnątrz firmy oraz w chmurze dla użytkowników wewnętrznych i zewnętrznych
- Single Sign-on dla aplikacji webowych, wewnątrz firmy oraz w chmurze
- Obsługa relacji B2C
- Zwiększenie bezpieczeństwa: **Risk Based Authentication** – nałożenie wymagań dodatkowego uwierzytelniania przy logowaniu się do aplikacji webowych

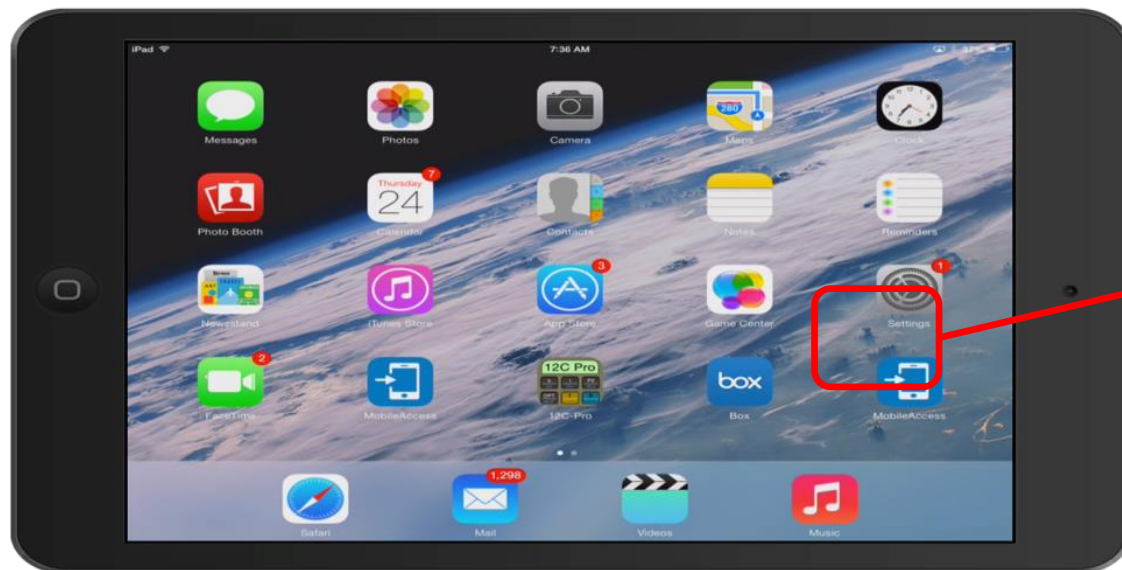


# Uwierzytelnianie oparte na szacowaniu ryzyka za pomocą NetIQ Access Manager



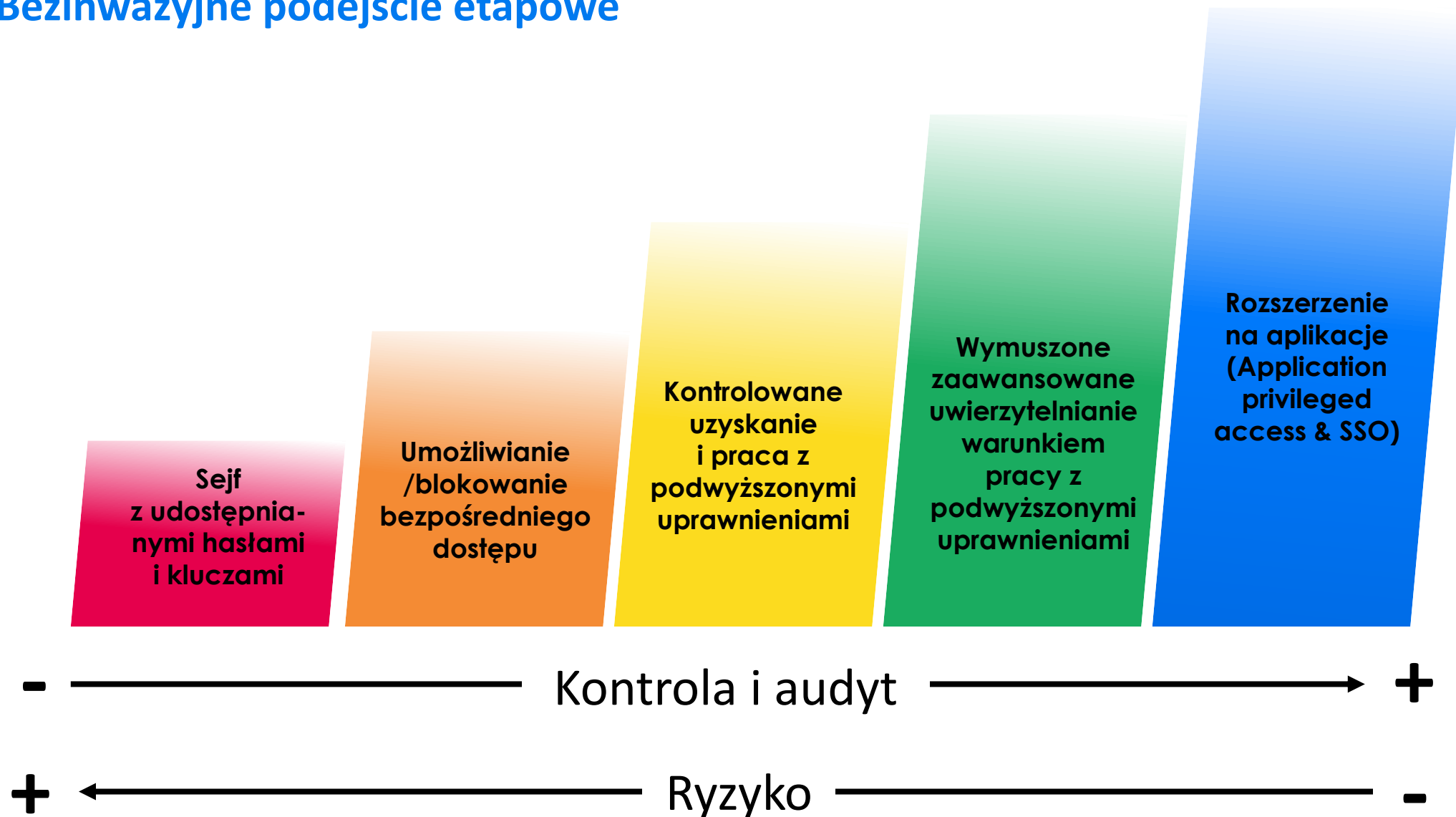
# Access Manager i dostęp z urządzeń mobilnych

- Dostarczany jako apka na urządzenia mobilne
- Kontrola, które z korporacyjnych aplikacji i zasobów webowych będą dostępne dla użytkowników z poziomu urządzeń mobilnych



# Micro Focus Privileged Access Management

Bezinwazyjne podejście etapowe





# Lista kont uprzywilejowanych

## – wsparcie ich wykrywania i tworzenia listy

### Privileged Account Auto Discovery

- Nie wymaga instalacji oprogramowania na przeszukiwanych systemach
- Windows/Unix/Linux

NetIQ Privileged Account Discovery

### Enter Range Details

Range Details

Windows  SSH

IP Range:

Windows Credentials:

User Name:

Password:

SSH Credentials:

User Name:

Password:

Add

NetIQ Privileged Account Discovery

NetIQ Privileged Account Discovery tool helps to discover and generate a detailed report of the privileged accounts in the systems and domain

Click to configure the respective system details

- Range of IP Addresses
- Windows
- UNIX/LINUX
- Domain
- Directory
- Import Configuration

NetIQ Privileged Account Discovery

### Customize Reports

Filter Discovery Details Based On:

Hosts Locked Accounts

Password Disabled Accounts

Expired All

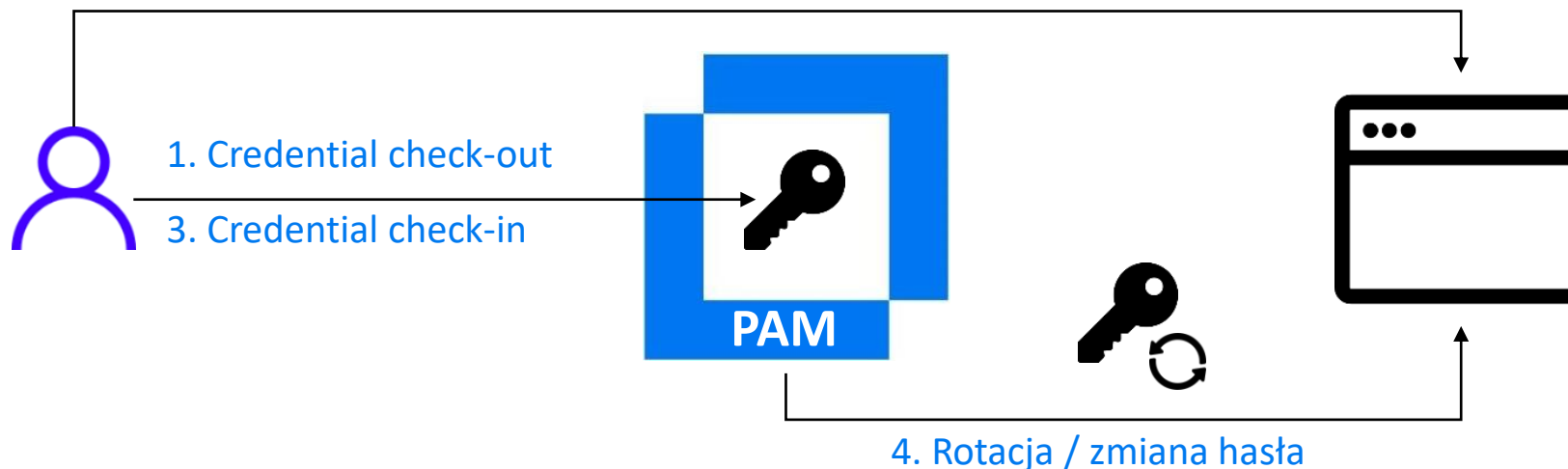
Back

# Sejf – Credential Vault

## Kontrola dostępu do haseł i kluczy

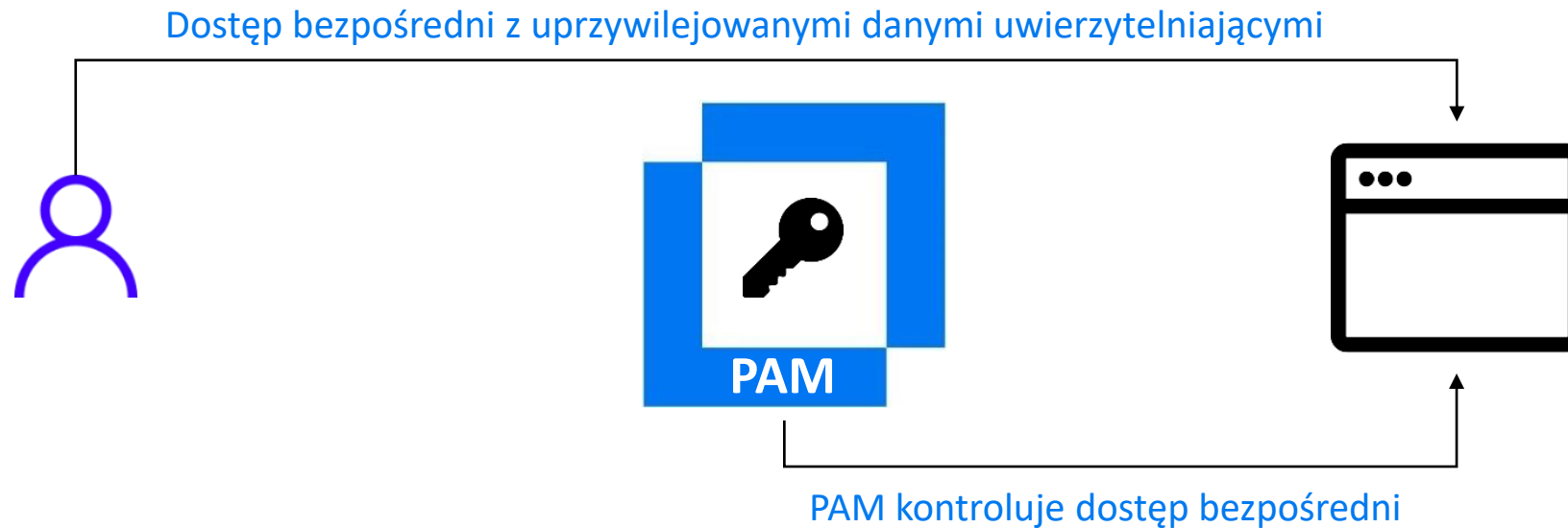
- Scentralizowany dostęp i zarządzanie uprzywilejowanymi poświadczeniami
- Rotacja haseł prowadzona przez PAM
- W pudełku: AD, LDAP, AWS, OpenStack, Windows, Linux / Unix, VMware ESXi, SAP
- Można dodać inne skrypty
- Integracja z NetIQ Identity Manager, który następnie może zmieniać hasła w innych systemach
- Aplikacje mogą żądać poświadczeń za pomocą PAM REST API

### 2. Bezpośredni dostęp z udostępnionymi danymi uwierzytelniającymi



# Kontrola bezpośredniego dostępu

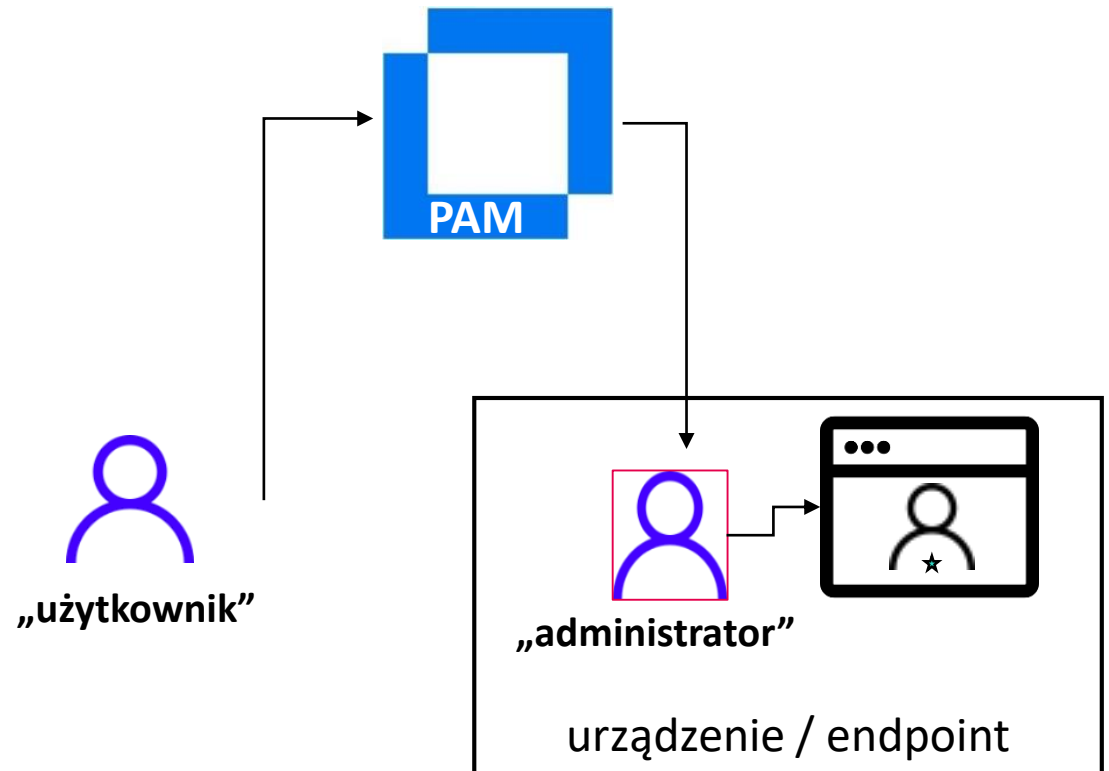
## Direct Access Control



- Użytkownik korzysta z istniejącego konta uprzywilejowanego w systemie docelowym na urządzeniu końcowym (SSH, Linux/Unix, Windows, RDP)
- W PAM definiujemy zasady dla użytkowników dotyczące bezpośredniego dostępu do zdefiniowanych systemów, nagrywania sesji i audytu
- PAM kontroluje, czy użytkownik może uzyskać dostęp i zalogować się bezpośrednio do system (SSH, Linux/Unix, Windows, RDP)

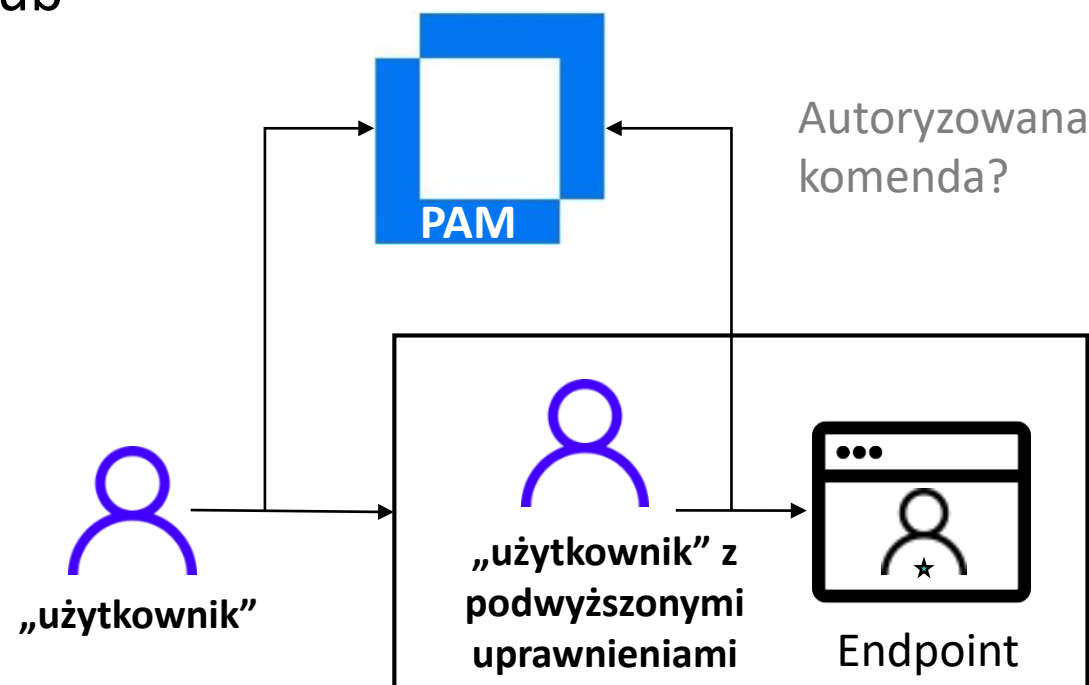
# Eskalacja uprawnień

- PAM podczas sesji uprzywilejowanej podaje dane uwierzytelniające
- Użytkownik nie zna tych danych
- Użytkownik musi się zalogować do PAM
- PAM może kontrolować dostęp do systemu, zapisywać i rejestrować sesje
- Opcjonalne żądanie dostępu awaryjnego



# Uprzywilejowane wykonywanie poleceń / komend

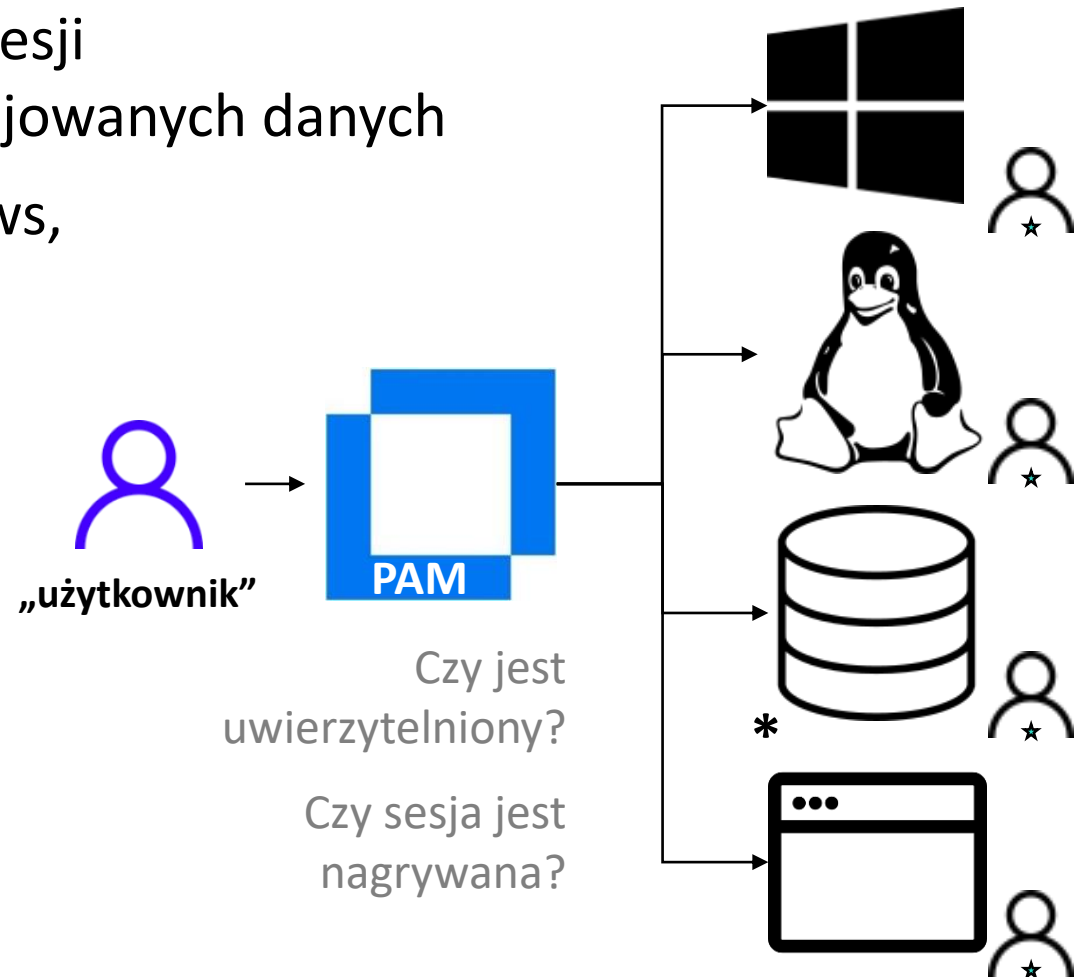
- Użytkownik uwierzytelnia się w systemie operacyjnym za pomocą **swojego konta** i dzięki PAM może uruchamiać aplikacje lub polecenia wymagające wysokich uprawnień
- PAM może kontrolować i ograniczać związane z tym zadania, takie jak zarządzanie usługami Windows, wykonywanie komend w systemie Linux
- PAM używa lokalnego agenta do autoryzacji dostępu, nagrywania sesji i uruchamiania aplikacji lub wykonywania komend uprzywilejowanych



# Zastosowanie PAM dla dostępu do aplikacji

## Sesja uprzywilejowana i SSO

- Działając jako przekaźnik, PAM uwierzytelnia i autoryzuje użytkownika oraz przyznaje mu dostęp do sesji uprzywilejowanej bez ujawniania uprzywilejowanych danych
- PAM dostarcza SSO dla aplikacji MS Windows, emulatorów terminali, aplikacji web
- Uprzywilejowane dane uwierzytelniające mogą być planowo zmieniane i wykorzystywane do powiązanych zadań jak zarządzanie usługami Windows czy innymi zadaniami związanymi z aplikacjami



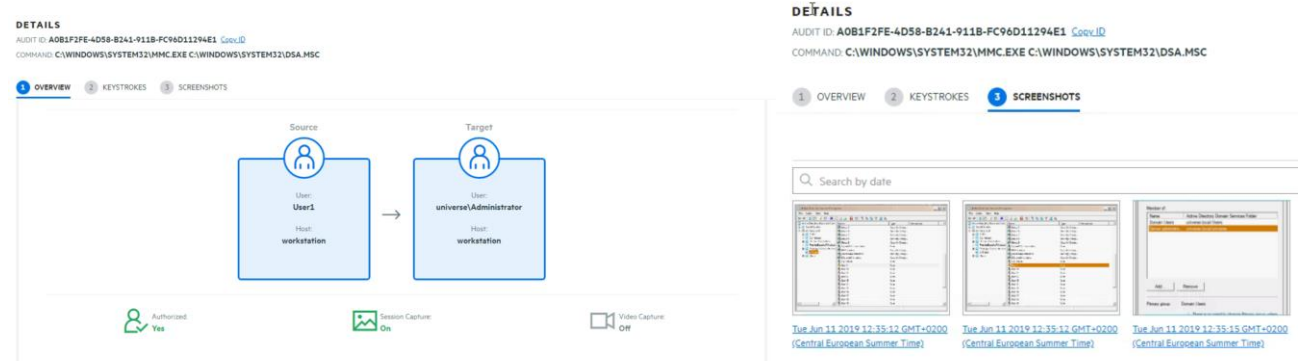


# Ścieżka audytowania

## Raporty, zdarzenia, ryzyko

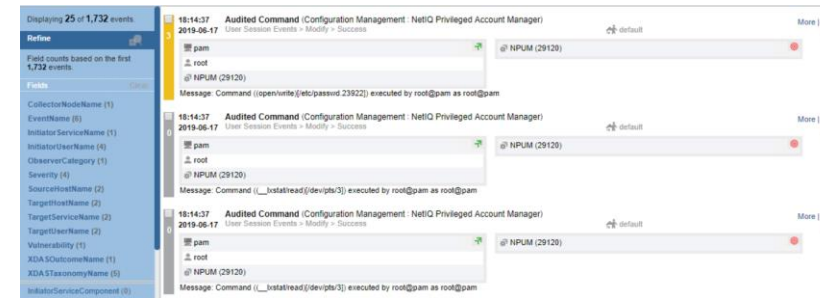
### Raporty

Przechowuje szczegółowe informacje o aktywności użytkownika, ma możliwość eksportowania rekordów i zapisywania sesji



### Zdarzenia

Wysyła całą sekwencję działań do platformy SIEM poprzez syslog, w celu połączenia tych danych z innymi informacjami dot. bezpieczeństwa



### Ryzyko

Klasyfikuje aktywność użytkownika i klasyfikuje poziom ryzyka w celu nadawania priorytetów w razie konieczności reakcji na zdarzenia

UTC Time	Standard Input
Tue Jun 18 12:20:39 2019	whoami[CR]
Tue Jun 18 12:20:46 2019	ssh linuxserver1[CR]
Tue Jun 18 12:21:00 2019	ls[CR]
Tue Jun 18 12:21:02 2019	yas[CR]
Tue Jun 18 12:21:12 2019	cd [NAK]ls[CR]
Tue Jun 18 12:21:34 2019	userd mod -s /fmp/maliciu ioush. r

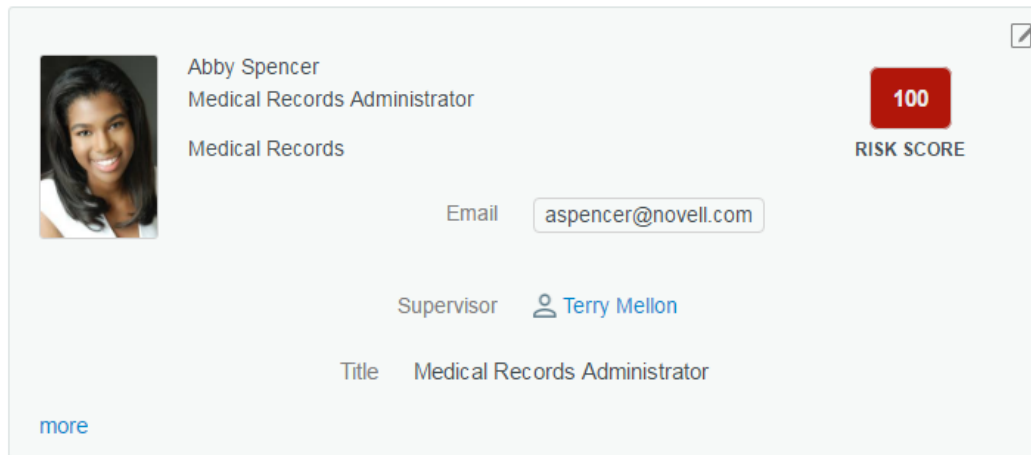


**Procesy zarządzania tożsamością,  
przeglądem informacji o uprawnieniach  
użytkowników, certyfikacja dostępu –  
NetIQ Identity Management &  
Governance**

# Od czego można zacząć

## Stan bieżący dla użytkowników i ich uprawnień

Abby Spencer



Abby Spencer  
Medical Records Administrator  
Medical Records

RISK SCORE  
**100**

Email: aspencer@novell.com

Supervisor: Terry Mellon

Title: Medical Records Administrator

[more](#)

Groups 1 | **Permissions 11** | Accounts 1 | Roles 1 | Business Roles 2

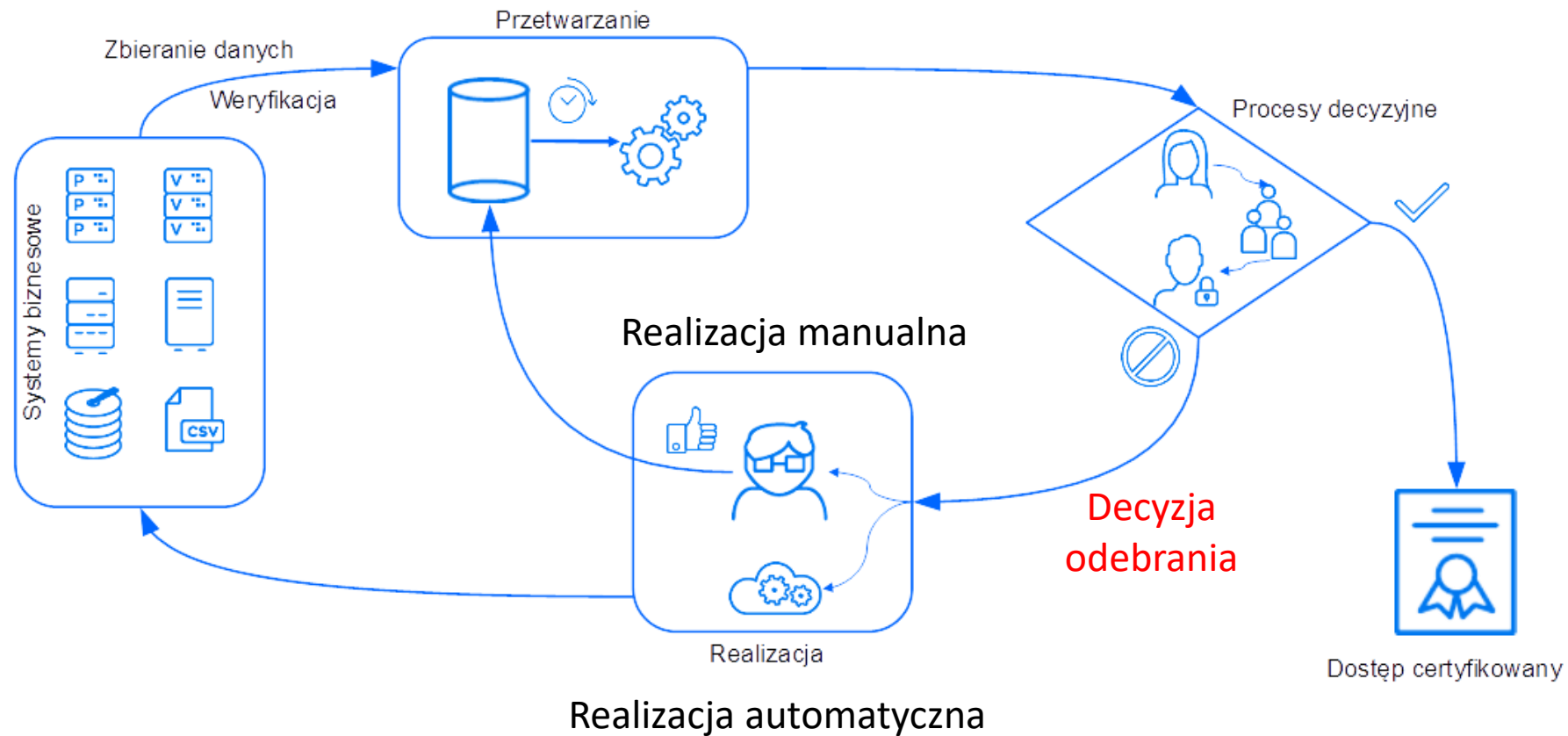
Search for permissions of Ab...

Name	Description	Authorized By
Patient Management System	Identity Manager Permissions	
Can Edit Patient Medical Records	Users with this level of access can edit patient medical records.	Medical Records Administrator
Can Release Patient Medical Records	Users with this level of access can release patient medical records.	Medical Records Administrator

Zebrana i skorelowana informacja o osobie i jej kontaktach, rolach i uprawnieniach w różnych systemach

Dostarcza szczegółowe informacje pomocne w podejmowaniu decyzji

# Przegląd i recertyfikacja



Proces zebrania i przeglądu uprawnień powinien obejmować systemy, które podlegają automatyzacji a prowizacji dostępu jak i systemy, które nadal są manualnie obsługiwane od strony zakładania kont i uprawnień

# Definiujemy przeglądy i recertyfikacje uprawnień użytkowników, ich kont, dostępów do plików i danych

Przegląd Żądanie dostępu **Przeglądy** Katalog Założenia 67 Realizacja 2 Źródła danych Administrowanie danymi ⚠ Konfiguracja

Definicje przeglądu

Przegląd działu sprzedaży



Definicja przeglądu

Typ przeglądu

Nazwa  ✓

Opis

Instrukcje dotyczące przeglądu

Elementy przeglądu dostępu użytkowników ✓

Wyszukaj użytkowników



oraz użytkownicy, którzy spełniają  spośród następujących kryteriów wyboru: +

X  
Znajdź wartość atrybutu katalogu lub podaj swój

# Przeglądy mogą być generowane na podstawie np. wykrytych incydentów z systemów SIEM

The screenshot displays the 'Identity Governance' interface. The main content area shows a configuration for a 'User Access Review' triggered by a 'Security Event Triggered' event. The review is active from 09/07/2017 2:59 PM to the present. The configuration includes the following details:

- Review type:** User Access Review
- Name:** Security Event Triggered
- Description:** This access review was triggered due to a security event being detected by the SIEM solution.
- User Access Review:** Select accounts that match any of the following selection criteria: `sec_violation_flag` Yes
- Review Options:** Allow review owner to override decisions
- Reviewer:** Review by Mary Markum
- Review owner:** Aaron Corry
- Review period:** 2 Week(s)
- Expiration policy:** Complete review
- Partial approval policy:** Allow partial approvals on demand
- Notifications:** Review start notice Notification sent to review owner that the review has started
- Validity Period:** 2 Month(s)

At the bottom of the configuration window, there are links for 'Review definition', 'View run history', and 'Monitor running review'. Below the configuration window, another review configuration is partially visible: 'Unused Accounts', 'Account Review', 'Aaron Corry', 'Terminated', '3 months', and 'Start Review'.

“ It was very important to complete the deployment quickly, because all the company’s other IT projects depended on having a working identity management architecture in place. The out-of-the-box capabilities of the NetIQ solutions were a big advantage in helping us deliver this quickly.

”

—Per, Pulsen  
(speaking about deployment at large automobile manufacturer)

# Wykrywamy i rozstrzygamy naruszenia założeń rozdziału obowiązków

Naruszenia założeń rozdziału obowiązków

ŁĄCZNIE	NIE OCENIONE	ZATWIERDZONE	ZATWIERDZENIE WYGASŁO	ROZSTRZYGANIE	ZAMKNIĘTE	WSTRZYMANE
69	68	1	0	0	0	0

Linux

Nazwa	Tytuł	Typ sprawcy naruszenia	Zasada SoD	Numer sprawy	Status przypadku
Adam Nowy	Marketing Assistant	Użytkownik	Administrator systemu rozliczeniowego i Administrator Linux	SOD-0045	Nie ocenione

**Adam Nowy**  
Marketing Assistant  
International Marketing

Poczta elektroniczna:

Ryzyko użytkownika: 0

**Administrator systemu rozliczeniowego i Administrator Linux**

Rozstrzygnij  
Stan: Aktywne  
Właściciele: [UserApp Administrator](#)

Adam Nowy narusza założenia SoD Administrator systemu rozliczeniowego i Administrator Linux, ponieważ:

Adam Nowy ma wszystkie spośród następujących:

- [Linux Administrator, Linux](#)

AND

Adam Nowy ma wszystkie spośród następujących:

- [Billing Administrator, IDM AE](#)

Przypadek: SOD-0045  
Początkowy czas wykrycia: 14.10.2019 13:40  
Ostatnie wykrycie: 14.10.2019 13:40  
Liczba wykrytych przypadków: 1  
Stan: **Nie ocenione**  
Liczba działań: 0

# Automatyzacja odbierania dostępu po recertyfikacji

NetIQ Identity Manager & Governance zapewnia możliwość **w pełni zautomatyzowanego odbierania uprawnień dostępu**, co dla biznesu oznacza **ograniczenie zagrożeń płynących z wewnątrz organizacji**

Do automatyzacji można wykorzystać:

- Konektory do podłączonych systemów
- Integrację z systemami Service Desk
- Procesy manualne: e-mail z powiadomieniem odpowiedniego administratora, który zrealizuje czynności. System przy kolejnym pobraniu danych źródłowych będzie miał automatycznie informacje o realizacji przez administratora odebrania dostępu





# Pełna automatyzacja obsługi zarządzania tożsamością w Micro Focus Identity Manager & Governance



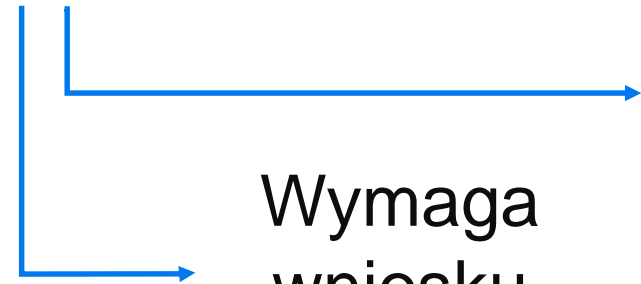
# Ulepszamy zarządzanie – reguły i role



Functioncode uit PZ = 5400



Rola biznesowa



Wymaga  
wniosku  
i zatwierdzenia

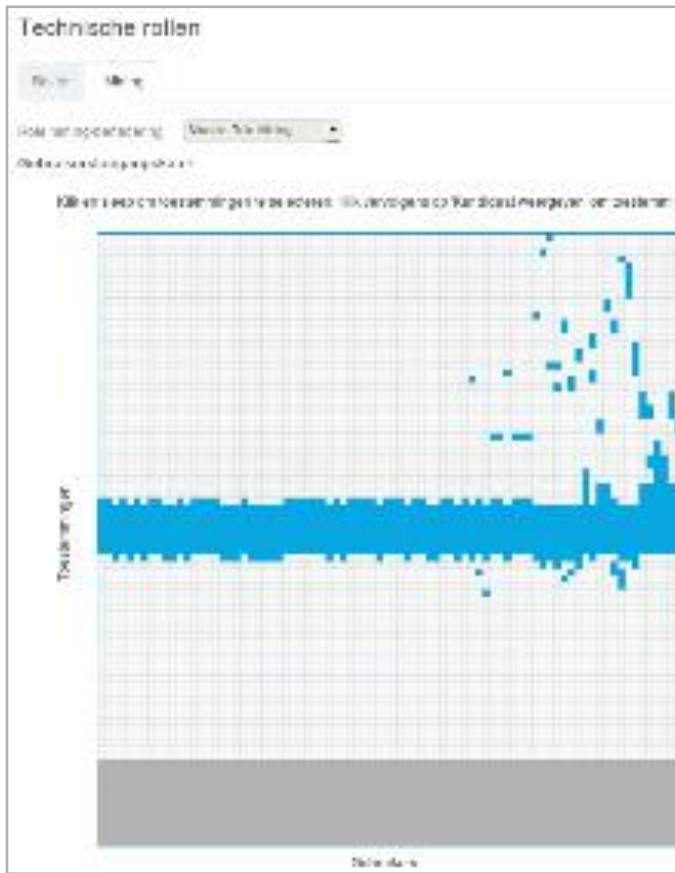


Reguły organizacyjne i biznesowe

Żądania dostępu, zatwierdzenia, przeglądy, SoD

# Ułatwiamy analizę i budowę zastawów ról

## Role mining



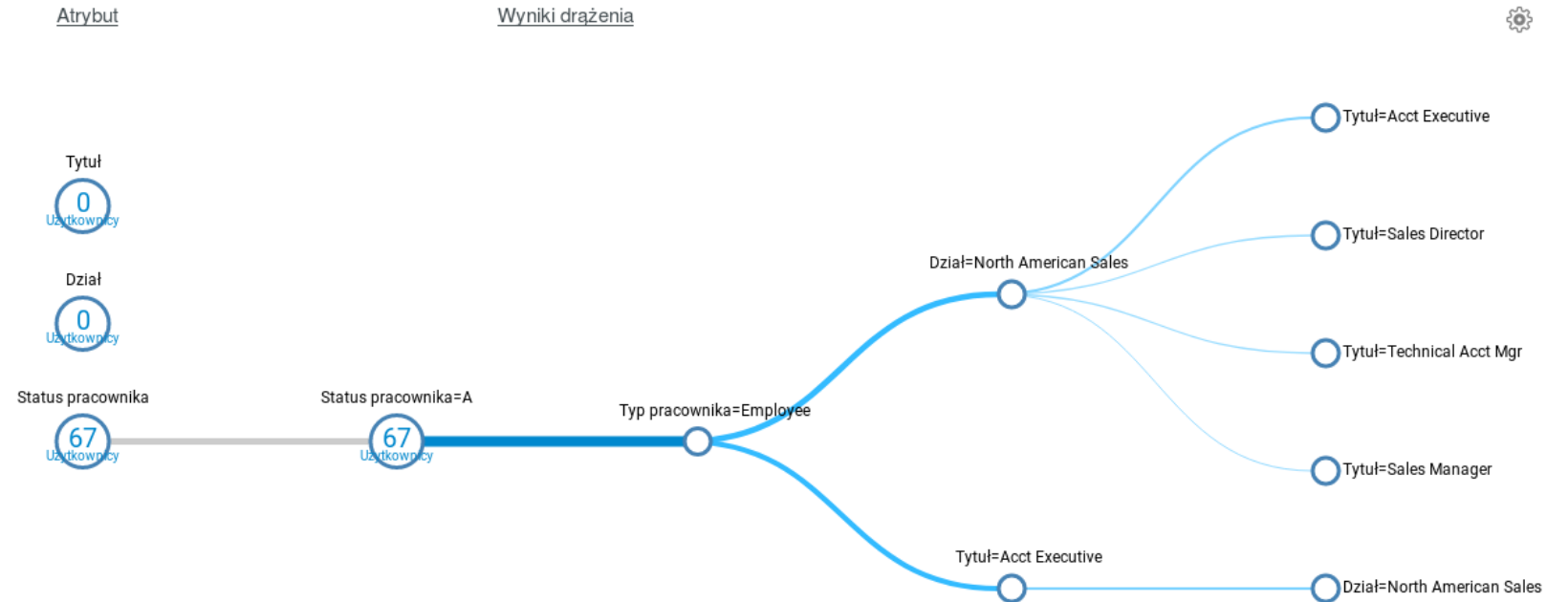
Przegląd Żądanie dostępu Przeglądy Katalog Założenia Realizacja 2 Źródła danych Administrowanie danymi Konfiguracja

Role Założenia zatwierdzania **Drażenie** Analiza Manage Auto Requests Business Role Detections

Metoda drażenia ról Wizualne drażenie ról

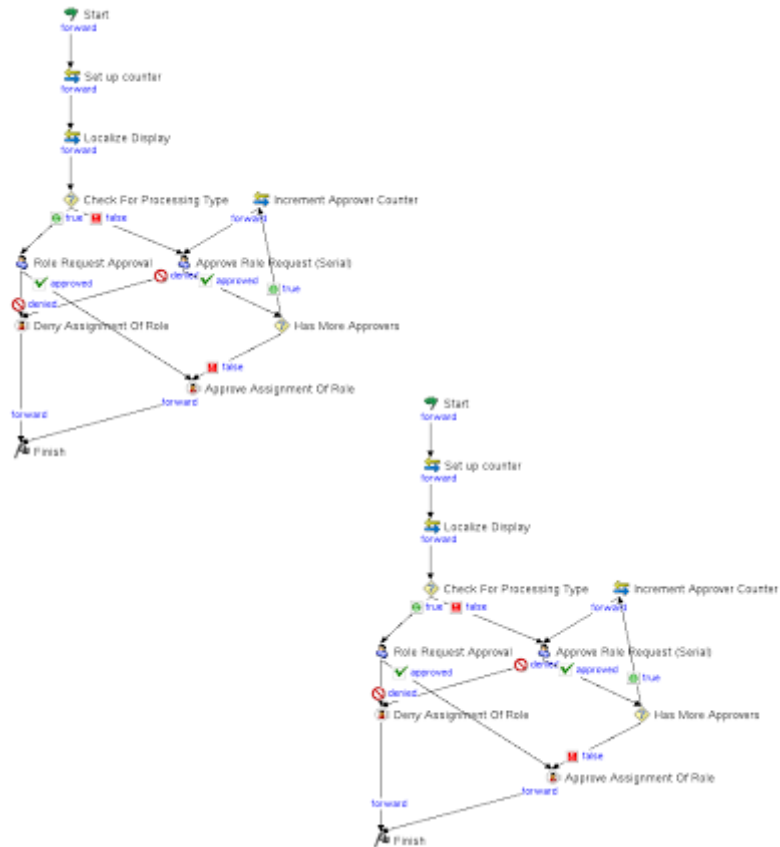
Zalecane kryteria Wyniki drażenia 0

Następujące rekomendacje zostały wygenerowane na podstawie danych użytkowników przeanalizowanych w dniu 09.10.2019 o 14:45. Średnica atrybutu wskazuje moc rekomendacji, a szerokość i natężenie linii wyniku drażenia wskazują podobieństwo wyników. Wybierz wyniki drażenia, aby dodać je jako kandydatury na role.



Ilustracja i podpowiedzi dla grupowania uprawnień w role

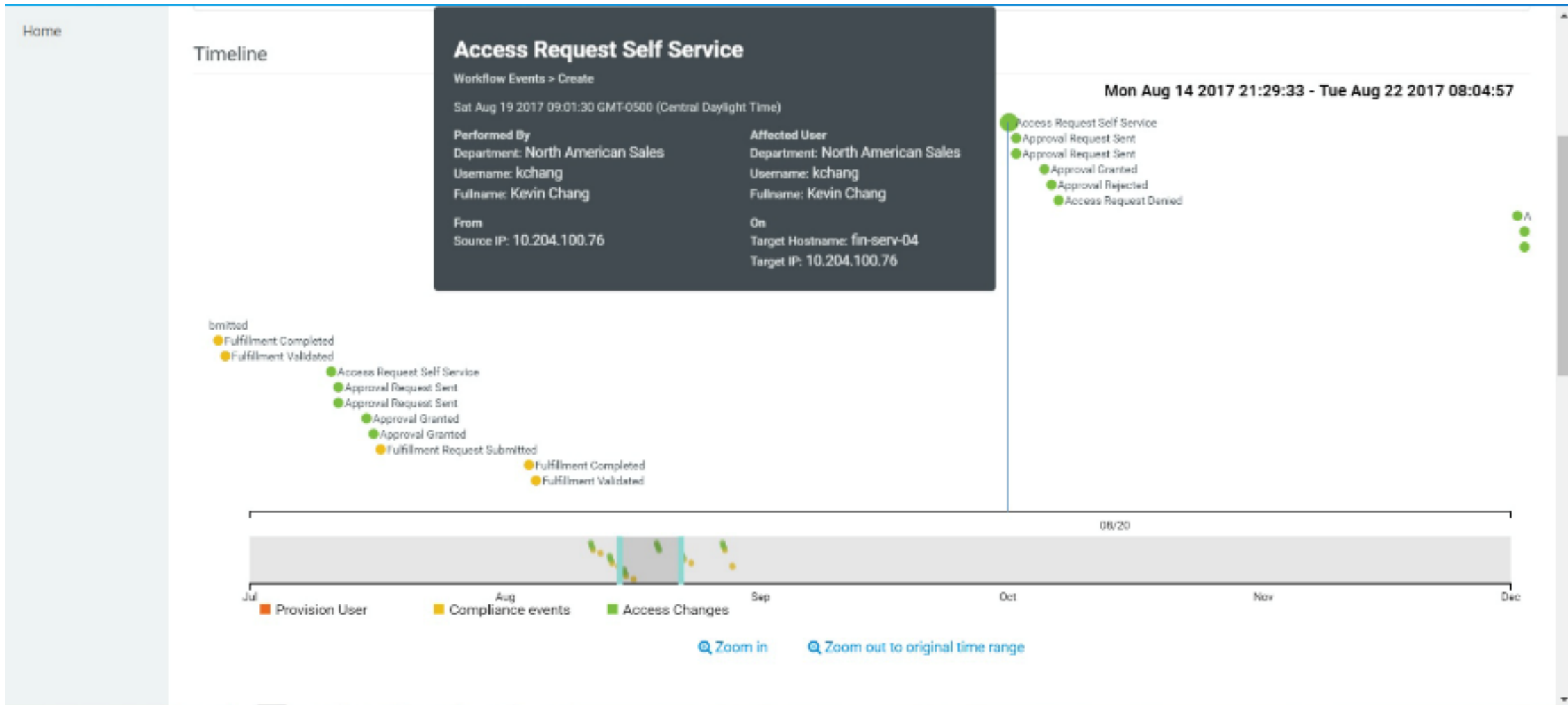
# Dostarczamy zaawansowany system workflow do obsługi wnioskowania



- Konfigurowane procesy *workflow* i ustawione reguły decydują o tym, kto powinien widzieć i zaakceptować te wnioski. SLA dla akceptacji, eskalacja.
- Manager /użytkownik widzi wnioski, które może inicjować, jak i wnioski, które trafiły do akceptacji. Można zaakceptować, odmówić, przekazać innej osobie, wpisać uzasadnienia. Możliwa jest akceptacja wielostopniowa, wielowątkowa, wymaganie akceptacji przez *quorum*, akceptacja jednej osoby z grona (np. pierwsza, która podejmie wnioski).
- Można pracować w imieniu lub ustanowić pełnomocnika w wypadku choroby czy nieobecności.

# Nowa wersja Micro Focus NetIQ Identity Manager jeszcze w tym roku!

Nowe narzędzie do budowy formularzy, analityka z Micro Focus Veritica





# Dziękuję za uwagę!

Zapraszam do kontaktu z nami:

[Tomasz.Surmacz@microfocus.com](mailto:Tomasz.Surmacz@microfocus.com)

+48 22 537 5000

