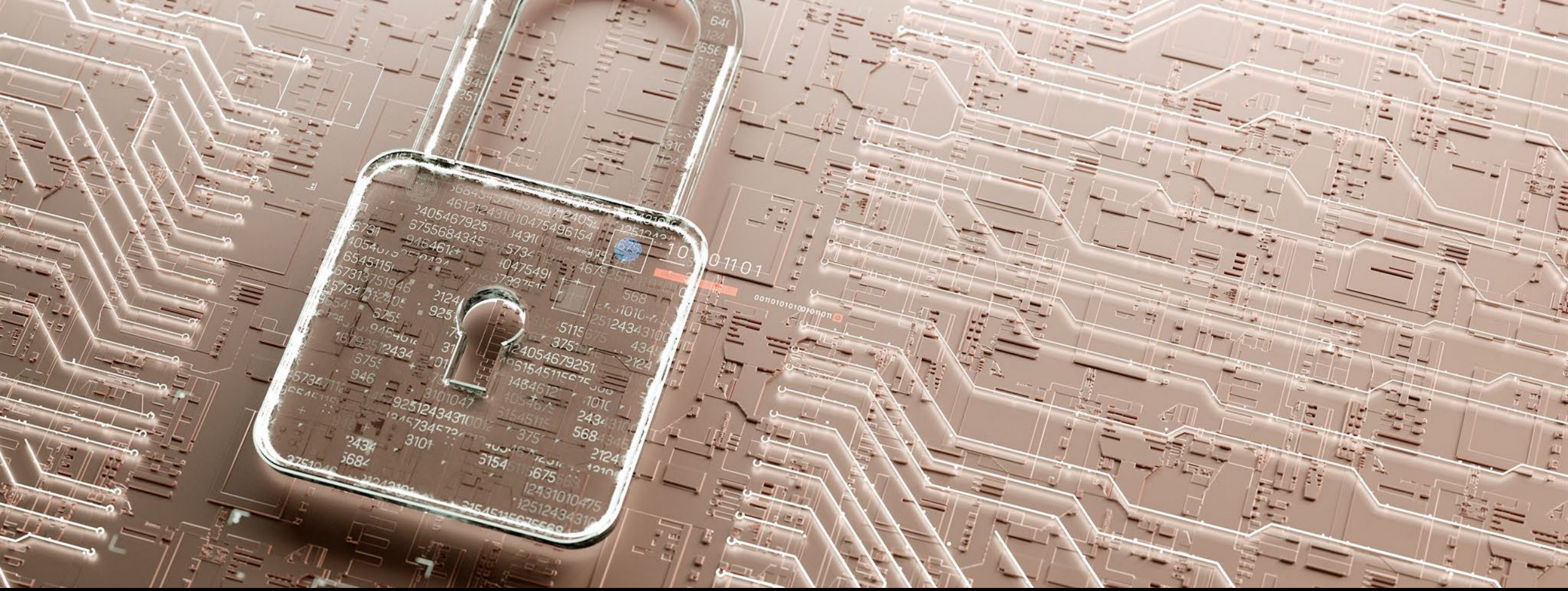


TRUST GATEWAY BANKA 2026+: NEXT-GEN ONBOARDING I STEP-UP BEZBEDNOST

NAPREDNE TEHNOLOGIJE ZA SIGURNOST I KORISNIČKO ISKUSTVO

UVOD I KONTEKST DIGITALNE TRANSFORMACIJE BANKARSTVA

Izazovi digitalnog bankarstva 2026+

Izazovi digitalne transformacije

Bankarski sektor se suočava sa pritiskom da ubrza usluge i ispuni regulativne zahteve za digitalno poverenje i autentikaciju.

EU identitetski okvir

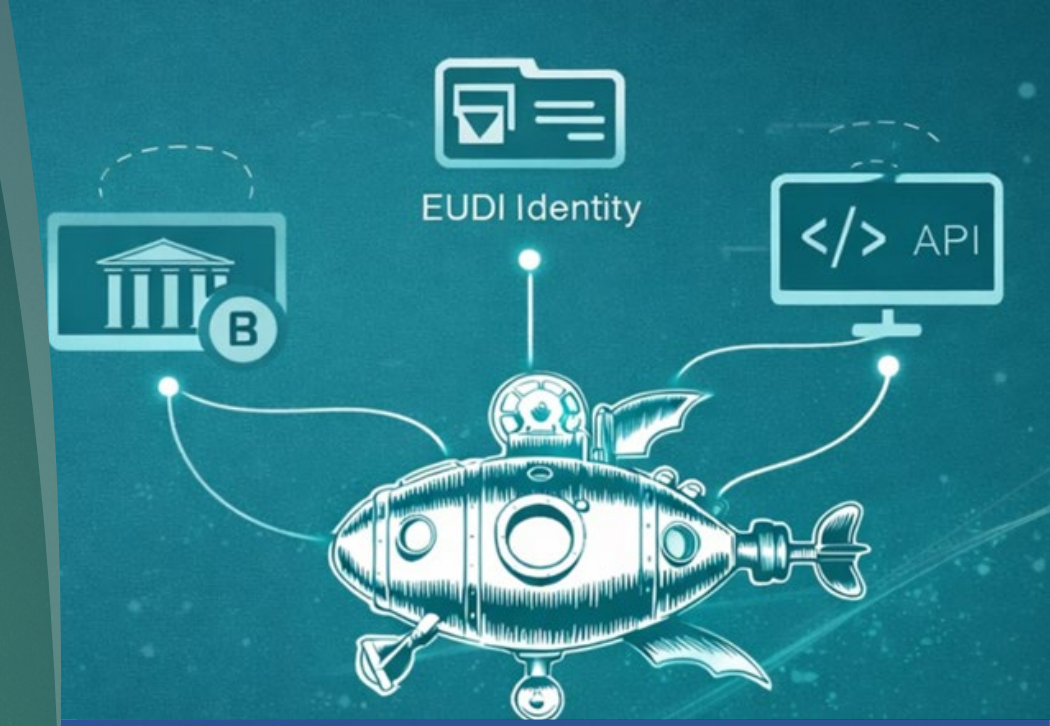
eIDAS 2.0 i EUDI Wallet uvode nove digitalne identitete koje banke moraju integrisati za pristup i autorizaciju usluga.

Tehnički izazovi integracije

Integracija novih identitetskih tokova u postojeće bankarske sisteme je kompleksna zbog rigidnosti i bezbednosnih rizika.

Rešenje: Trust Gateway

Trust Gateway omogućava postepenu evoluciju bankarskih sistema slojevito, bez ometanja stabilnosti core komponenata dodajući orkestracioni sloj između dogitalnih kanala i core sistema.



Zašto Trust Gateway sada postaje prioritet

Potreba za Trust Gateway-om

Banke moraju balansirati regulatorne zahteve, tehnološka ograničenja i korisnička očekivanja od 2026. godine nadalje.

Rastući digitalni rizici

Napredni bot napadi, credential stuffing i manipulacije API tokenima povećavaju finansijske pretnje u digitalnim kanalima.

Funkcionalnosti Trust Gateway-a

Omogućava step-up autentikaciju, API token validation i policy enforcement, centralizovani nadzor i izolovane trust zone bez remonta sistema.

Evolutivni pristup implementaciji

Modularni pristup omogućava postepeno uvođenje slojeva bez zastoja, izbegavajući velike migracije sistema.

TRUST GATEWAY ARHITEKTURA I NJENI MODULI

The Digital Trust Gap in Modern Banking

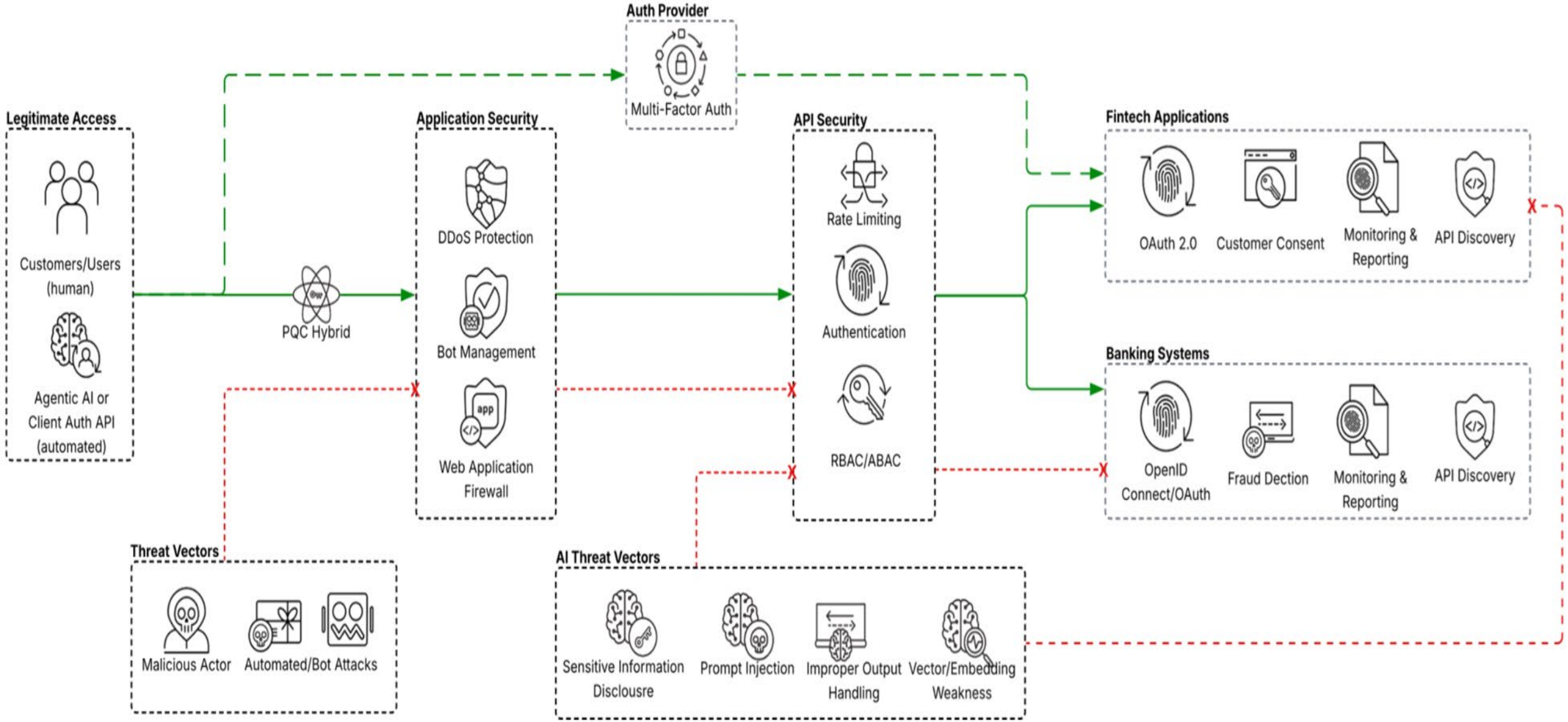
ALEF Trust Hub

Existing Security Components

- IAM Platforms
- MFA Authentication
- Fraud Detection
- API Gateway & WAF
- SIEM / SOC Operations

ALEF Trust Gateway Architecture

ALEF integrates existing security components into a **unified** Trust Gateway architecture that orchestrates identity, transaction and API


Auth Provider
Multi-Factor Auth
Legitimate Access
Customers/Users (human)
Agentic AI or Client Auth API (automated)
PQC Hybrid
Application Security
DDoS Protection
Bot Management
Web Application Firewall
API Security
Rate Limiting
Authentication
RBAC/ABAC
Fintech Applications
OAuth 2.0
Customer Consent
Monitoring & Reporting
API Discovery
Banking Systems
OpenID Connect/OAuth
Fraud Dection
Monitoring & Reporting
API Discovery
Threat Vectors
Malicious Actor
Automated/Bot Attacks
AI Threat Vectors
Sensitive Information Disclousre
Prompt Injection
Improper Output Handling
Vector/Embedding Weakness

Identity Enforcement sloj

Adaptivna autentikacija

Adaptive MFA automatski prilagođava nivo autentikacije prema riziku transakcije i ponašanju korisnika.

Obogaćivanje postojećih identiteta

Gateway obogaćuje postojeće identitete dodatnim signalima rizika i atributima iz više izvora, uključujući EUDI Wallet.

Federation bridge funkcionalnosti

Povezivanje različitih identitetskih sistema omogućava jedinstven front-door bez menjanja aplikacija.

Centralizovano upravljanje pravilima

Centralno upravljanje policy pravilima olakšava kreiranje trust i step-up mehanizama za sigurnost.

API Trust Layer i digitalni kanali

Konsistentna kontrola kanala

API Trust Layer obezbeđuje doslednu kontrolu nad svim digitalnim kanalima kao što su mobilne aplikacije i web portali.

Validacija tokena

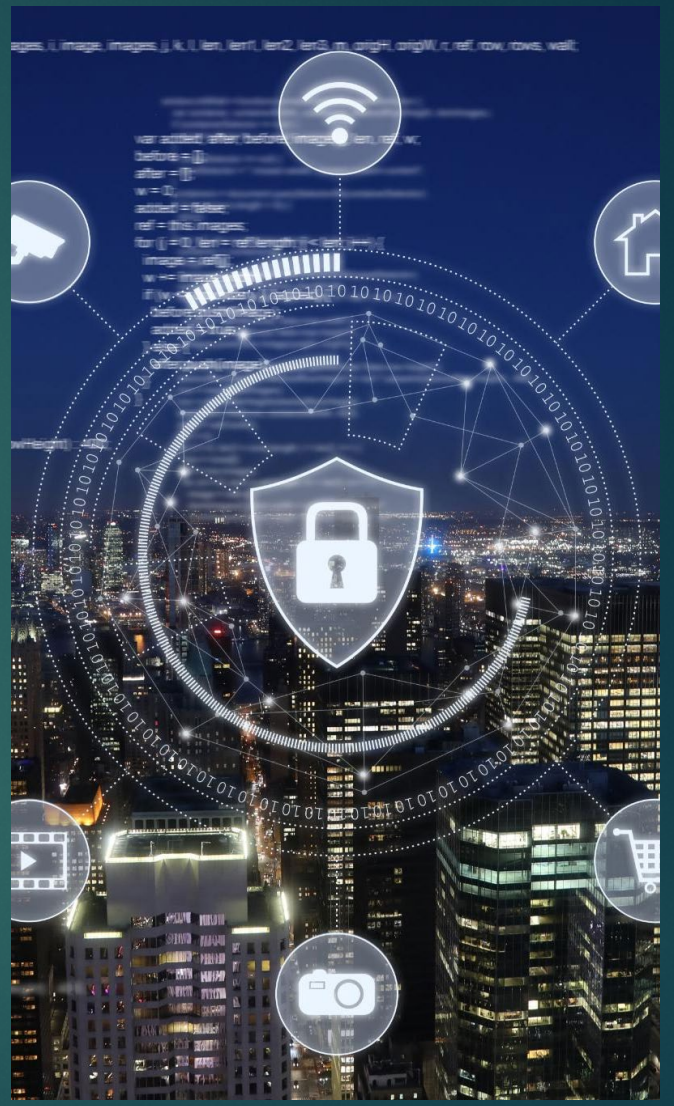
Token enforcement aktivno proverava i primenjuje pravila nad API tokenima kako bi se sprečile zloupotrebe i napadi.

Zaštita od pretnji

Napredna zaštita od botova i DDoS napada prepoznaje i blokira sofisticirane automatizovane pretnje u realnom vremenu.

Dinamička bezbednosna pravila

API Gateway omogućava dinamičko prilagođavanje sigurnosnih politika na osnovu ponašanja aplikacija ili korisnika.



Operational Trust i izolovana trust zona

Kontrola privilegovanih pristupa

Operational Trust sloj obuhvata privileged access management, secrets management, exposure management, SIEM monitoring i audit.

Exposure Management za rizike

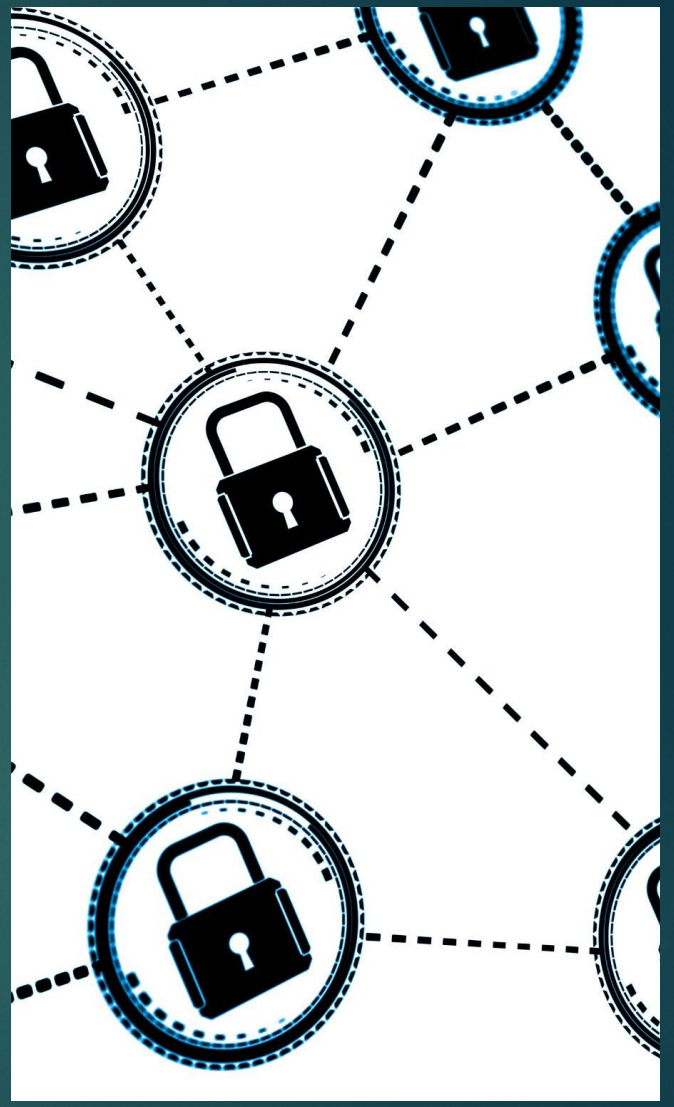
Exposure Management pruža ažurne informacije o ranjivostima i neusklađenim konfiguracijama unutar bankarske infrastrukture.

Izolovana zona za trust servise

Izolovana trust zona na hyperconverged infrastrukturi omogućava sigurno izvršavanje kritičnih trust servisa - token validacija, policy enforcement, audit - nezavisno od glavne mreže.

Bezbedan Trust Gateway

Trust Gateway se postavlja bez rizika iznad postojećeg core sistema, pružajući snažan bezbednosni sloj bez promena arhitekture.



USE-CASE I PRIMENA U REALNOM BANKARSKOM OKRUŽENJU

High-Risk Step-Up scenario

Procena rizika transakcije

Sistem automatski analizira rizik koristeći podatke o transakciji, uređaju, lokaciji i prethodnom ponašanju klijenta.

Adaptive višefaktorska autentikacija

Adaptive MFA bira najoptimalniji metod autentikacije u realnom vremenu, smanjujući neprijatnosti za korisnika.

Token enforcement i audit zapisi

API Trust Layer primenjuje token enforcement, a audit zapisi se prosleđuju SIEM/SOC sistemima radi sigurnosti i usklađenosti.

ROADMAP I EVOLUCIONA IMPLEMENTACIJA

PoC pristup i fazna implementacija

Analiza trenutnog stanja

Proces započinje dvonedeljnom analizom, identifikujući ključne trust scenarije i rizike za unapređenje bez velikih ulaganja.

PoC faza implementacije

PoC traje 4 do 6 nedelja i uključuje autentikaciju, token enforcement i integraciju sa SIEM/SOC sistemima.

Operativni trust sloj i dalje faze

Nakon PoC-a uvode se PAM, ZTNA i izolovane trust zone za sigurnu i neprekidnu digitalnu transformaciju.

Prilagodljiv i siguran rast

Fazni pristup omogućava transformaciju sa jasnim povratom ulaganja i bez prekida poslovanja.

ZAKLJUČAK I STRATEŠKI ZNAČAJ

Ključne koristi Trust Gateway pristupa

Unapređenje sigurnosti i usklađenosti

Trust Gateway omogućava bankama da poboljšaju sigurnost i regulatornu usklađenost bez menjanja osnovnih sistema.

Brži onboarding i smanjenje rizika

Ovaj pristup ubrzava onboarding korisnika i smanjuje rizike u digitalnim kanalima zahvaljujući adaptivnoj autentikaciji i API zaštiti.

Centralizovana vizuelizacija rizika i trust odluka

Trust Gateway omogućava bankama centralizovan pregled rizika i trust signala kroz sve digitalne kanale, što povećava otpornost sistema i daje jasnu sliku bezbednosnih odluka kao deo digitalne strategije banke.

Integracija i evolucija sistema

ALEF pruža bankama brz, evolutivan i bezbedan put ka digitalnoj izvrsnosti kroz duboko poznavanje enterprise okruženja.