BLITZ IDENTITY PROVIDER

Authentication server for your organization
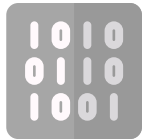
REAK SOFT, LLC

🌐 identityblitz.ru

TYPICAL ISSUES

Proprietary application login mechanisms are not always secure

Disparate logging of security events complicates access auditing

Users have trouble remembering multiple logins and passwords

Password authentication is not enough to effectively protect company applications
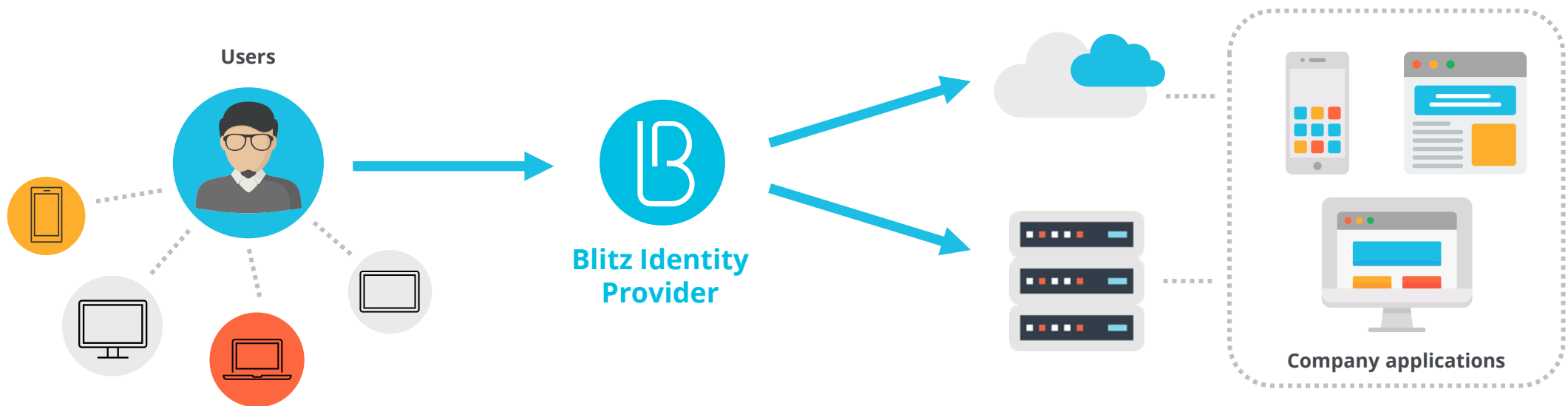
When employees work remotely, the risk of account hacking increases

Employee access to cloud services is inconvenient or insecure

SOLUTION

Create a Single Sign-On service for user to access company applications

BLITZ IDENTITY PROVIDER

Software product deployed on company servers. Solves identification, authentication, authorization and audit tasks

- Single Sign-On (SSO)
- Multi-factor authentication (MFA)
- support for various authentication methods
- suitable for different users: employees, customers, counterparties

- suitable for websites, mobile applications, and smart devices
- web applications and company services protection (Access Management, API Security)
- access to infrastructure services (SSH, RDP, VPN)
- security event logging and accountability of user actions

SINGLE SIGN-ON

Allows users to log in to their account once and gain access to all company applications with one simple step

improves user experience

enhances security

saves time and investments

VARIOUS AUTHENTICATION METHODS

Built-in support for multiple authentication and login confirmation methods. Flexibility to integrate the company's own internal login methods

login and password, built-in brute force protection

smart cards, USB tokens for digital signature, FIDO2 and U2F security keys

push-authentication, QR-code authentication

various external identity providers

hardware and software generators, HOTP and TOTP

Passkey and WebAuthn, biometric authentication via Face ID and Touch ID

one-time confirmation codes via SMS or email, Flash Call

proprietary authentication methods

FLEXIBLE AUTHENTICATION FLOWS

Authentication server considers the needs of different user groups for secure and efficient management of identification, authentication, and access

Employee — secure and convenient access to corporate resources using Single Sign-On (SSO), Multi-Factor Authentication (MFA), and access control policies

Client — sign in using banking credentials, social media accounts, or registration through a web form can be used to enhance the customer experience
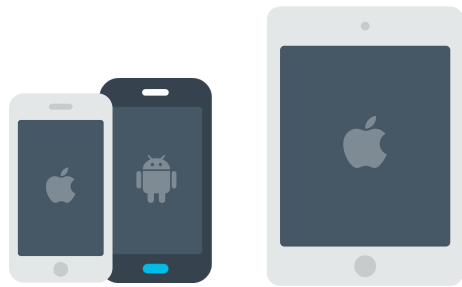
Affiliate — remote access management for business affiliates and contractors without compromising the company's internal security policies

SMART DEVICES SUPPORT

Our product takes into account the specifics of access and security scenarios when using various devices

**Smartphones and tablets**   **Personal computers**   **Smart devices**

WEB APPLICATIONS AND COMPANY SERVICES PROTECTION

Ability to centralize configuration of the authorization logic for user access to web applications and company services

✓ API Security Gateway as part of an authentication server for securing web services

✓ Access rights can be based on, for example, user attributes and context parameters

✓ Access policies may differ for different applications, organizations and user groups
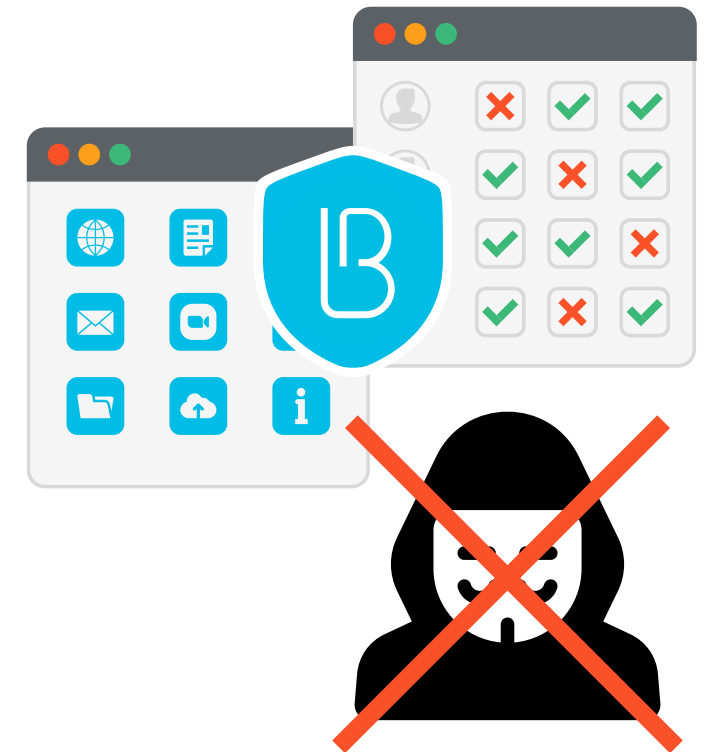
AUDIT AND ACCOUNTABILITY

Authentication server records user logins and accesses to the company's applications and services

Continuous monitoring allows timely detection and response to attacks

Export security events to an external security analysis system (SIEM)

Users can manage their account security settings in Profile

Built-in system for user notification about important account security events

KEY FEATURES

Authentication & SSO

- ✓ 20+ authentication methods
- ✓ MFA and adaptive access control
- ✓ Brute force protection
- ✓ SSO based on OpenID Connect & SAML
- ✓ Flexible and customizable authentication flows
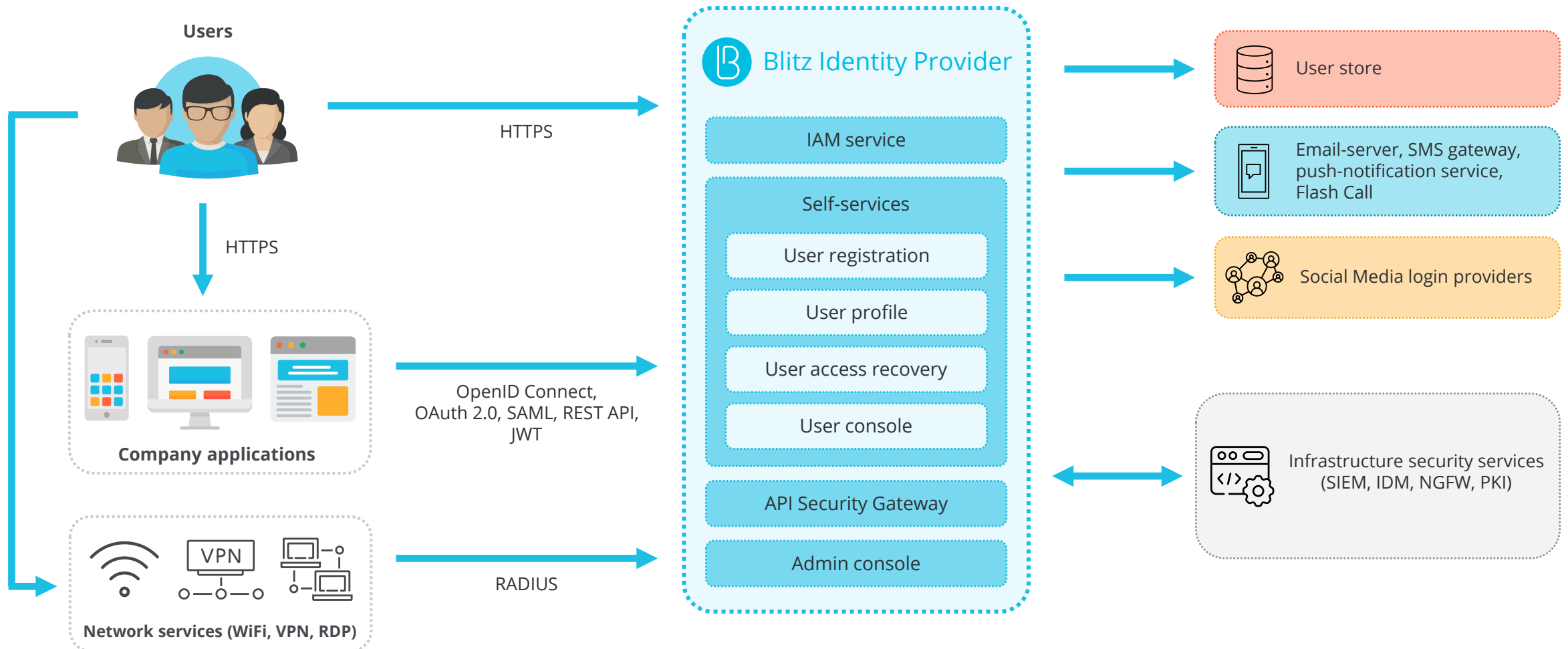- ✓ Seamless and safe account linking

Authorization & Audit

- ✓ API protection, OAuth 2.0
- ✓ Flexible authorization policies (RBAC, GBAC, ABAC)
- ✓ Tracking used devices, browsers, locations
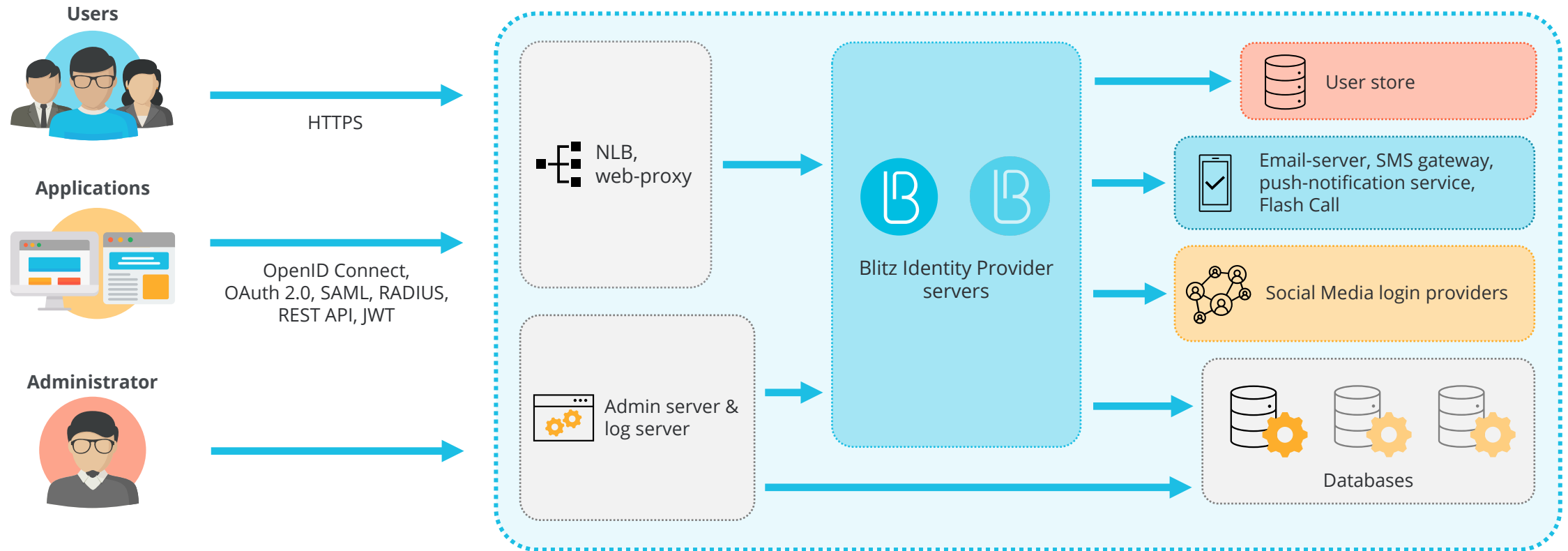- ✓ Security events logging & exporting to DB, files and MQ

Self-Services

- ✓ Account registration
- ✓ Profile management
- ✓ Access recovery
- ✓ Application panel
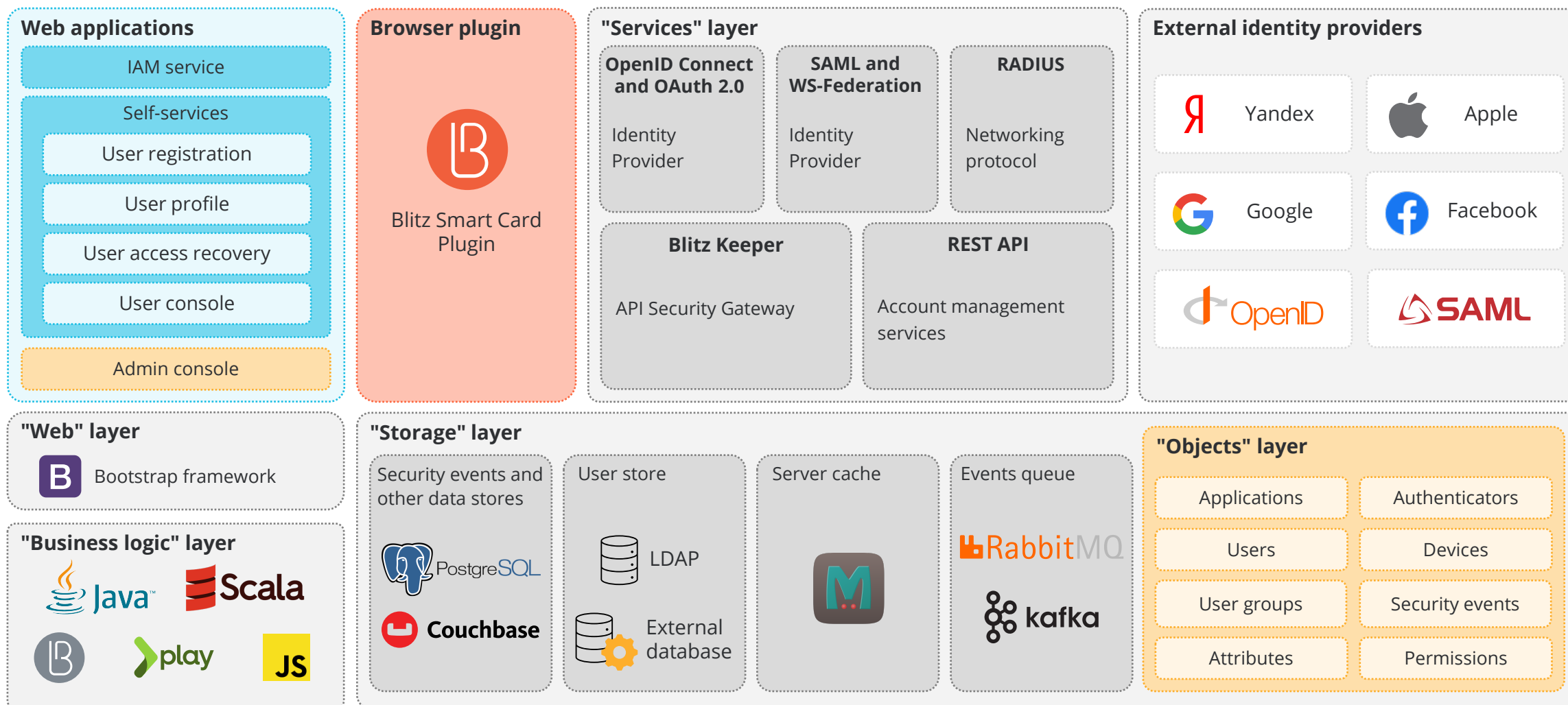- ✓ User actions for onboarding, MFA setup, contacts actualization

GENERAL WORKFLOW

TYPICAL DEPLOYMENT

BLITZ IDENTITY PROVIDER CORE

Web applications

IAM service

Self-services

User registration

User profile

User access recovery

User console

Admin console

Browser plugin

Blitz Smart Card Plugin

"Services" layer

OpenID Connect and OAuth 2.0

Identity Provider

SAML and WS-Federation

Identity Provider

RADIUS

Networking protocol

Blitz Keeper

API Security Gateway

REST API

Account management services

External identity providers

Yandex

Apple

Google

Facebook

OpenID

SAML

"Web" layer

Bootstrap framework

"Business logic" layer

Java

Scala

play

JS

"Storage" layer

Security events and other data stores

PostgreSQL

Couchbase

User store

LDAP

External database

Server cache

Events queue

RabbitMQ

kafka

"Objects" layer

Applications

Authenticators

Users

Devices

User groups

Security events

Attributes

Permissions

BENEFITS OF SINGLE SIGN-ON

For employees

- ✓ Simpler access to company's applications and resources
- ✓ Speeding up the procedure for gaining access
- ✓ Eliminating "password chaos"

For IT department

- ✓ Reduction of administration costs
- ✓ Reducing the number of access requests from users
- ✓ Simplification of external access granting procedure

For IS department

- ✓ Reducing risks of an unauthorized access
- ✓ Increasing security through multifactor authentication
- ✓ Unification of authentication policies

PROJECT PORTFOLIO

mos.ru	Moscow E-Government Public Services	Blitz Identity Provider Blitz Smart Card Plugin	15M city residents 100K employees
INGOSSTRAKH	Ingosstrakh Insurance Company	Blitz Identity Provider	3M customers 4K employees 20K contractors
NLMK	Novolipetsk Steel (NLMK)	Blitz Identity Provider	30K employees 50K workers 60 companies
Bank of Russia	The Bank of Russia	Blitz Identity Provider	50K employees

MOSCOW E-GOVERNMENT PUBLIC SERVICES AUTHENTICATION

mos.ru

8 months

15M city residents
100K employees

TASK:

- Provide an access control system to digital public services of Moscow E-Government Public Services

RESULTS:

✓ Software has been unified, various software products solving the problem of user of identification, authentication, and access have been replaced by a single solution

✓ Improved performance and reliability of the system, increased performance reserve with reduced hardware resources

✓ Connection of new applications to the system is simplified, as the platform complies with standard protocols and specifications

✓ Core functionality improved, security of user accounts was enhanced

✓ Improved usability for system administrators and users

AUTHENTICATION SYSTEM FOR INGOSSTRAKH INSURANCE COMPANY

INGOSSTRAKH

TASKS:

• Provide a unified solution for identifying employees, contractors and customers

• Ensure operation of different authentication modes

6 months
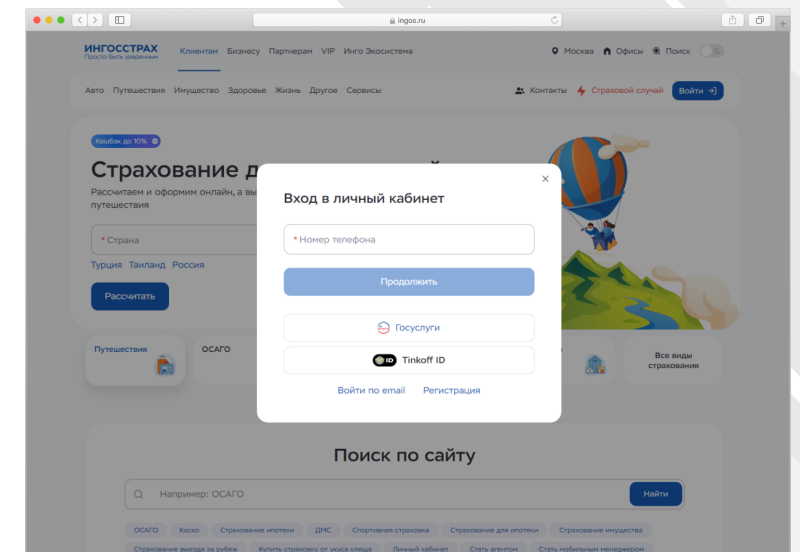
3M customers
4K employees
20K contractors

RESULTS:

✓ A unified authentication system for identifying users and providing access to the company's applications was created

✓ Integration with AD, Kerberos for domain user authentication for company employees was implemented

✓ Two-factor authentication for company's contractors was enabled

✓ Provided a single point of access control: different categories of employees are given access to different applications

AUTHENTICATION SYSTEM FOR NOVOLIPETSK STEEL (NLMK)

TASKS:

- Ensure registration and reliable identification of NLMK employee accounts

- Provide a single login to NLMK's HR and training applications for office employees

RESULTS:

- ✓ Provided independent user registration as well as registration through human resources department. During the registration process, the data is reconciled with the HR system

- ✓ Two user account stores are enabled simultaneously – the office employee's account store and the external employee's account store – which does not require access to internal IT resources

- ✓ Multilanguage interface support: English, French, Danish and Italian

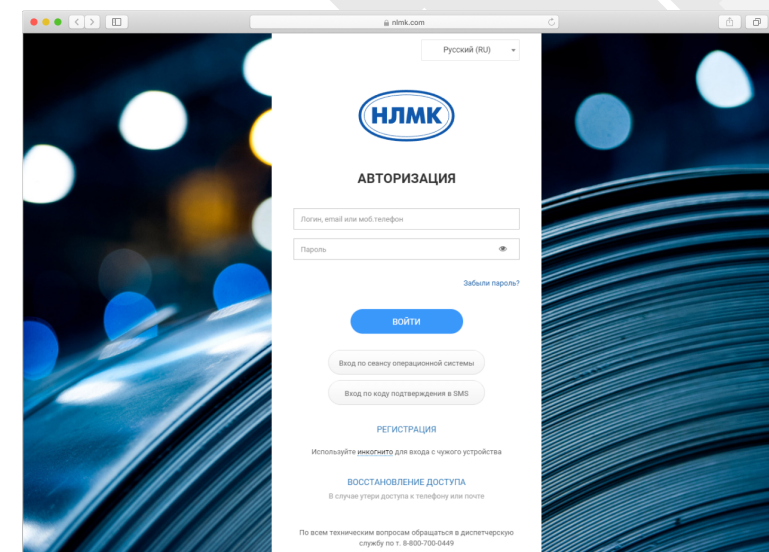- ✓ Provided SSO to the corporate portal, mobile application, web application and cloud services of the company
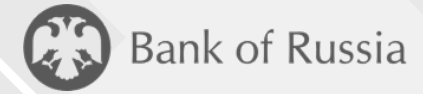
3 months

30K employees
50K workers
60 companies

DOMAIN AUTHENTICATION FOR THE BANK OF RUSSIA

Bank of Russia

TASK:

• Provide an end-to-end domain user authentication (login using OS session) to the company's applications

RESULTS:

✓ Provided an end-to-end domain user authentication for employees to access company's applications (AD, Kerberos)

✓ Web Single Sign-On technology is implemented

✓ Ease of integration as standard application connectivity was provided via SAML, OpenID Connect, and web-proxy

✓ Smart-card, USB-token and digital signature authentication was implemented

✓ Admin console for user administration was connected

3 months

50K employees
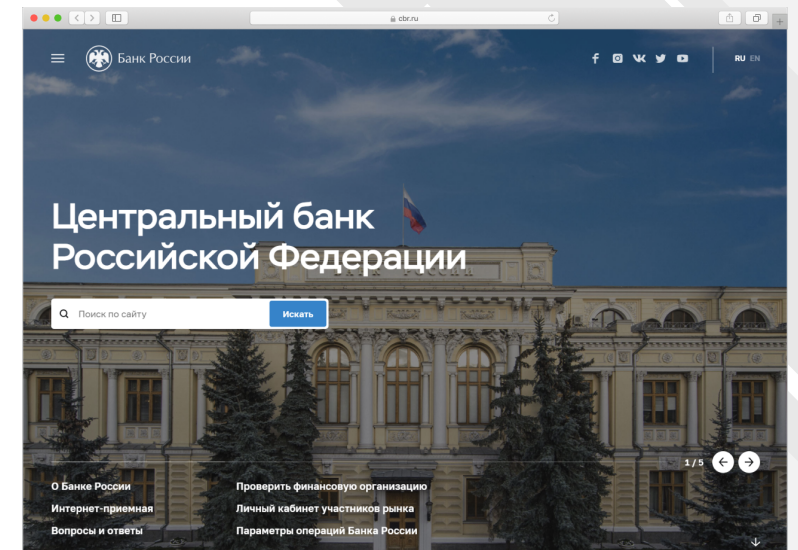
OUR COMPANY

IDENTITY BLITZ is a leading Russian software development company, providing state-of-the-art solutions for identification, authentication, and user access management for corporate applications. Since its inception in 2014, the company has been a dynamic player on the cybersecurity market

IDENTITY BLITZ designs software solutions that empower businesses to manage and control user access to corporate resources

OVER **10 years**
ON THE MARKET

OVER **50 projects**
IN PORTFOLIO

OVER **100M**
ACTIVE USERS

OUR ADVANTAGES

IAM EXPERTISE

A team of highly qualified experts can provide assistance to partners and customers throughout the presale, architecture design, deployment, and tech support phases

FLEXIBLE PRICING & SERVICES

Customers pay only for the services they require. Choose the license type that best aligns with your needs

EXTENSIVE PRODUCT CUSTOMIZATION

All services and features are readily available out of the box. Customize with zero-coding, eliminating the necessity of hiring developers for adapting software to the customer's environment

CLIENT-DRIVEN DEVELOPMENT

Our software can be swiftly tailored to meet our customers' specific requests and requirements

EXCEPTIONAL EFFICIENCY

Achieve superior performance with minimal system requirements. Our solution is easy to scale and cluster

OUR MANAGEMENT

Mikhail Vanin
Chief Executive Officer (CEO)

Responsible for setting the strategic direction of the company, establishing long-term goals, and policies

Professor at Bauman Moscow State Technical University, Department of Information Security

mvanin@idblitz.com

Kirill Gavrilov
Chief Operations Officer (COO)

Responsible for implementation of the company's strategic objectives and development of the company's products

PhD, Assistant Professor at the Analysis of Social Institutions Department, National Research University Higher School of Economics (HSE)

kgavrilov@idblitz.com

CONTACTS

73, Pyatnitskaya st., Moscow,
115054, Russian Federation

+7 (499) 322-14-04

info@idblitz.com

t.me/identityblitz

identityblitz.com