Enabling a seamless customer identity experience

accenture security

Consumer expectations around identity are increasing

Macro trends

Omni channel experience

Organizations are building next generation experiences, leveraging their digital identities across mobile, web, IVR, chat, and other channels.

Digital identity can bring improved user experience, increased security, reduced fraud, and reduced cost to all channels.

Convergence of identity & risk

Identity systems are becoming orchestrators, gathering the entire context of transaction risk, and tailoring authentication.

Organizations are leveraging identity systems to prevent fraud, increase confidence, and apply appropriate friction.

Elastic infrastructure

Authentication in a state of rapid evolution. Being able to flex infrastructure and environments is an enabler for development and deployment of new features, as well as adapting to changing demands.

Self managed identity

Consumers are demanding more control over their identity data. Organizations are implementing new privacy preserving features via distributed identity, and preference & consent management.

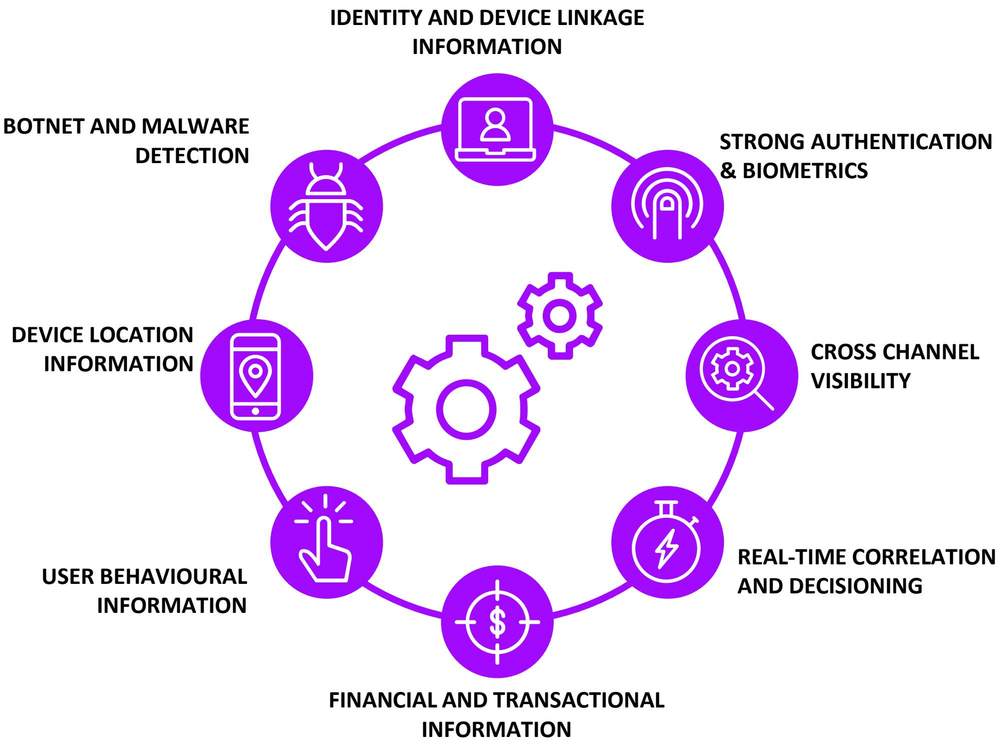
Next-gen authentication

Passwords have long been recognized as the most significant security weakness. They are cumbersome and expensive to use. Customers hate them. There is a convergence of technology and consumer expectations that is allowing organizations to reduce dependency on passwords.

Authenticating in the new

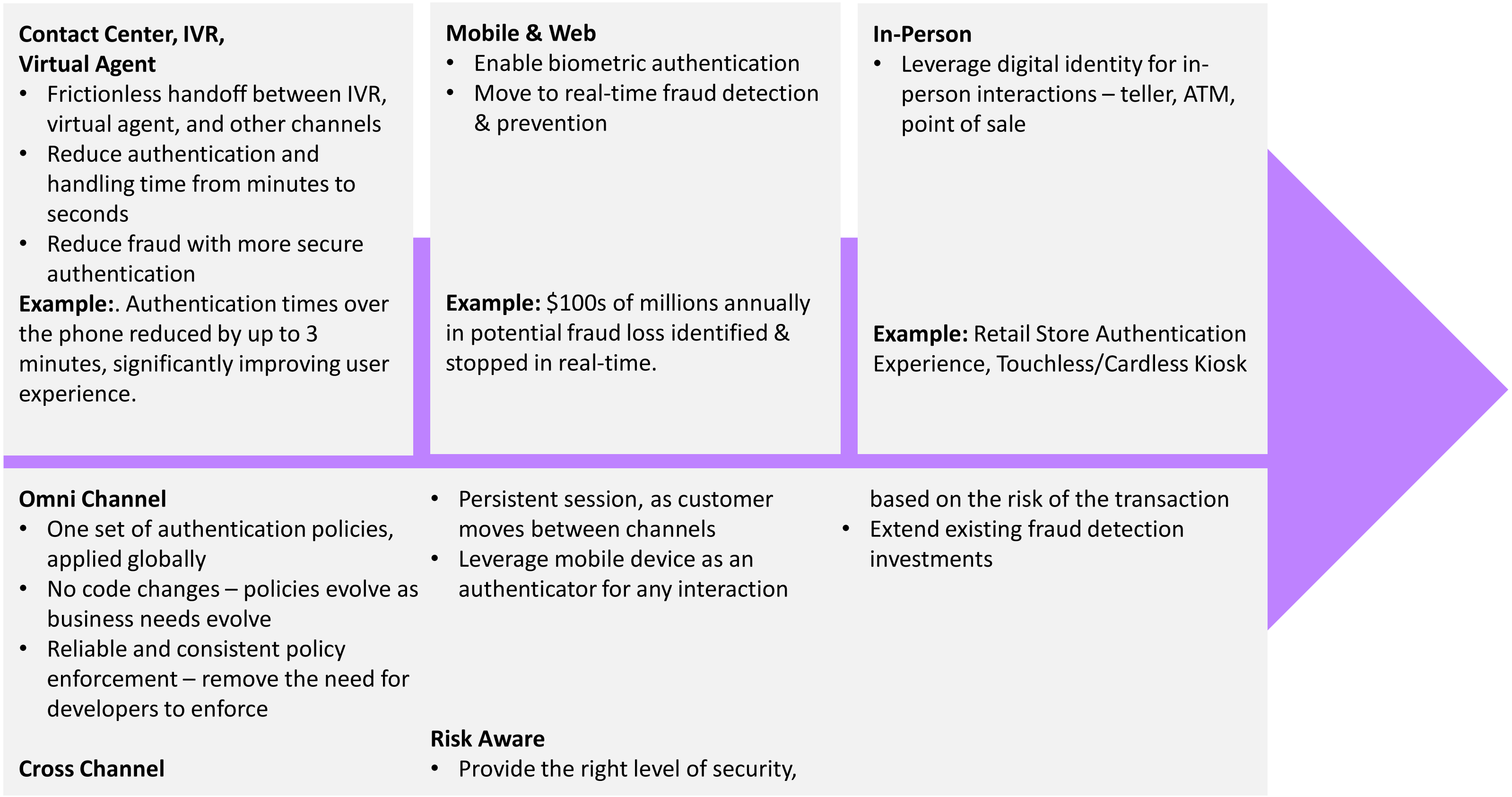
Moving to a risk-based approach allows organizations to apply the appropriate amount of friction when authenticating customers.

An omnichannel, real-time fraud detection and prevention capability adds context and actionable intelligence to your authentication decisions


IDENTITY AND DEVICE LINKAGE INFORMATION
STRONG AUTHENTICATION & BIOMETRICS
CROSS CHANNEL VISIBILITY
REAL-TIME CORRELATION AND DECISIONING
FINANCIAL AND TRANSACTIONAL INFORMATION
USER BEHAVIOURAL INFORMATION
DEVICE LOCATION INFORMATION
BOTNET AND MALWARE DETECTION

Unlocking the value of CIAM

Moving to a risk-based omni-channel authentication approach improves customer experience while reducing risk.



Contact Center, IVR, Virtual Agent

- Frictionless handoff between IVR, virtual agent, and other channels
- Reduce authentication and handling time from minutes to seconds
- Reduce fraud with more secure authentication

Example:. Authentication times over the phone reduced by up to 3 minutes, significantly improving user experience.

Mobile & Web

- Enable biometric authentication
- Move to real-time fraud detection & prevention

Example: $100s of millions annually in potential fraud loss identified & stopped in real-time.

In-Person

- Leverage digital identity for in-person interactions – teller, ATM, point of sale

Example: Retail Store Authentication Experience, Touchless/Cardless Kiosk

Omni Channel

- One set of authentication policies, applied globally
- No code changes – policies evolve as business needs evolve
- Reliable and consistent policy enforcement – remove the need for developers to enforce

Cross Channel

- Persistent session, as customer moves between channels
- Leverage mobile device as an authenticator for any interaction

Risk Aware

- Provide the right level of security, based on the risk of the transaction
- Extend existing fraud detection investments

- **Improved customer experience**
- **Reduced fraud**
- **Reduced cost**
- **Higher digital channel adoption**
- **Improved speed to market**
- **Visibility of customer interactions across channels**

Omni-channel best practices

Moving to an omni-channel experience requires careful thought about authenticators and risk, to preserve security and customer experience.

What's my login & password?

Whose name is on the account?

What's the PIN?

I was just talking to someone about this

I just want to pay my bill, why do you need this information?

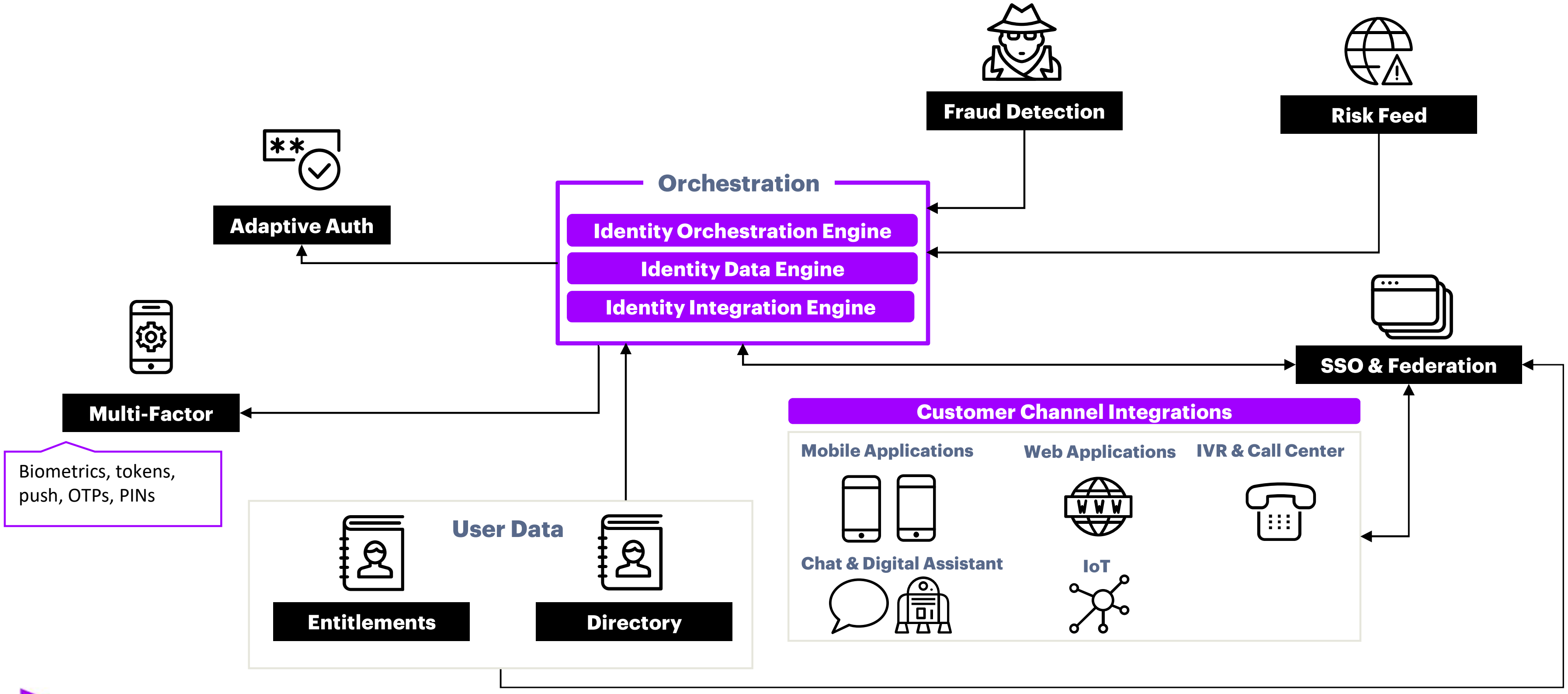
WEAK AUTHENTICATORS

LACK OF CONTEXT & RISK

- **Easy to use, strong authenticators** – passwords are cumbersome and weak. Consider biometric and other passwordless options.
- **Authenticator choice** – not all authenticators work for all customers. PINs, passwords, and other knowledge-based authenticators are difficult to remember. Biometrics vary in effectiveness. Give users a choice.
- **Risk-based decisions** – balance risk and user experience. Avoid making authentication a barrier to adoption.

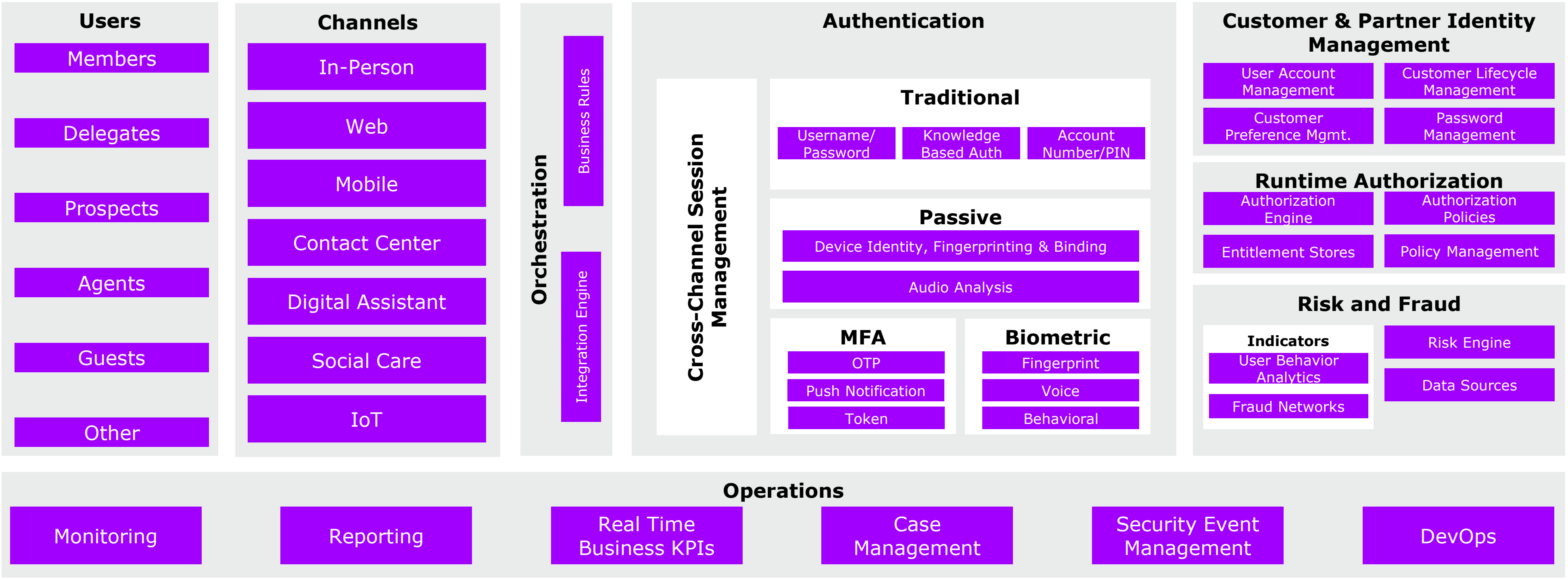
Omni channel conceptual architecture

Adopting an omni channel authentication platform allows organization to apply consistent authentication policies across channels, as well as improve customer experience.



Typical CIAM platform capabilities

The below framework illustrates typical capabilities underpinning an omni channel authentication platform.



Users

- Members
- Delegates
- Prospects
- Agents
- Guests
- Other

Channels

- In-Person
- Web
- Mobile
- Contact Center
- Digital Assistant
- Social Care
- IoT

Orchestration

- Business Rules
- Integration Engine

Authentication

Cross-Channel Session Management

Traditional

- Username/ Password
- Knowledge Based Auth
- Account Number/PIN

Passive

- Device Identity, Fingerprinting & Binding
- Audio Analysis

MFA

- OTP
- Push Notification
- Token

Biometric

- Fingerprint
- Voice
- Behavioral

Customer & Partner Identity Management

- User Account Management
- Customer Lifecycle Management
- Customer Preference Mgmt.
- Password Management

Runtime Authorization

- Authorization Engine
- Authorization Policies
- Entitlement Stores
- Policy Management

Risk and Fraud

Indicators

- User Behavior Analytics
- Fraud Networks

- Risk Engine
- Data Sources

Operations

- Monitoring
- Reporting
- Real Time Business KPIs
- Case Management
- Security Event Management
- DevOps

Cyber-Fraud Attacks Take Many Forms

FRAUDSTERS DEPLOY A BROAD RANGE OF METHODS TO GAIN ACCESS TO ACCOUNTS, AND EXPLOIT THE DISCONNECT BETWEEN SECURITY AND FRAUD CONTROLS

AS ORGANIZATIONS INCREASE THEIR DIGITAL FOOTPRINT, A HOLISTIC APPROACH TO SECURITY AND FRAUD PREVENTION CAN MITIGATE RISK AND ENHANCE CUSTOMER EXPERIENCE

Credential stuffing attacks lead to compromised accounts

Automated account opening facilitates future fraudulent activity

Phishing and malware harvest credentials and device fingerprints

Skimming collects payment details for fraudulent use

Data breaches exacerbate identity theft and new-account fraud

Synthetic identities enable mule accounts and deposit fraud

SIM swapping circumvents authentication controls

Social engineering exploits weaknesses in the call center

The current state of call center authentication

AS ORGANIZATIONS HAVE STRENGTHENED DIGITAL AUTHENTICATION, THE CONTACT CENTER HAS BECOME ACHILLES HEEL, DUE TO LEGACY AND SILOED AUTHENTICATION PROCESSES AND TECHNOLOGY

THESE LEGACY TOOLS AND SILOED AUTHENTICATION PROCESSES HOLD ORGANIZATIONS BACK FROM DIGITAL TRANSFORMATION AND OPEN THE DOOR FOR FRAUD.

Legacy IVR Technology still in place from the 80s/90s/2000s

Security controls easily guessed or reverse engineered data (e.g. PINs)

Controls easily by-passed using exception processes (e.g. failed IVR authentication)

Lack of strong second factors for authentication

Disjointed authentication processes based on publicly available information

Humans susceptible to social engineering

Lack of integration with fraud detection and prevention processes

Lack of Intelligence about the context of the customer and devices used during call center interaction

Call center fraud

CALL CENTERS HAVE WEAK AUTHENTICATION PROCCESSES AND LEGACY TECHNOLOGY THAT PROVIDES AN EASY TARGET FOR FRAUDSTERS. THE SCOPE OF CALL CENTER FRAUD HAS INCREASED DRAMATICALLY.

Call Center Fraud By the Numbers

- Call center fraud rate went up by 113% between 2015 and 2016
- An increase in fraudulent calls from 1 in every 2000 calls to 1 in 937 calls
- Call center losses per call $0.58
- Mobile account takeovers have doubled over the last 4 years [2]

> "The call center is the softest target for fraud in virtually every organization [1]"

What are they trying to get?

- Reconnaissance for account takeover
- Use as a beachhead to land and expand exploiting the organization
- Card not present and other fraud

> "Criminals make an average of 5 CALLS before completing a transaction[1]"

Common Fraud Tactics

- Caller ID spoofing
- Social engineering - calling in numerous times to get information from a willing representative

Implementing strong omni channel authentication improves user-experience and reduces cost to identify and authenticate per call

1. 2017 Call Center Fraud Report – Pindrop
2. Call center fraud prevention – Experian

10