Key Tenets of CIAM Solution

Empower

consumers, CSRs & administrators...

Scale

to millions of entities, cloud based service...

Security

should be in-grained...

Why is Identity Governance & Assurance critical for CIAM?

Let's review some of the use cases

1 Frictionless Onboarding

at the same time, provide assurance and manage risk…

- Enable customers and business partners with self-service account management tools

- Ensure they are who they 'claim' to be

- Manage user groups and associated access across multiple identity stores

Registration

Level of Assurance

ID Proofing

1 Orchestrate customer journeys securely

with tiered ID proofing and based on a risk framework

- Based on the channel (Mobile, Social etc.)

- Risk-level of the entity or service that user is planning to consume

- Risk at user and session level, constantly evaluate the user activity and behavior

- Integration with case management tools

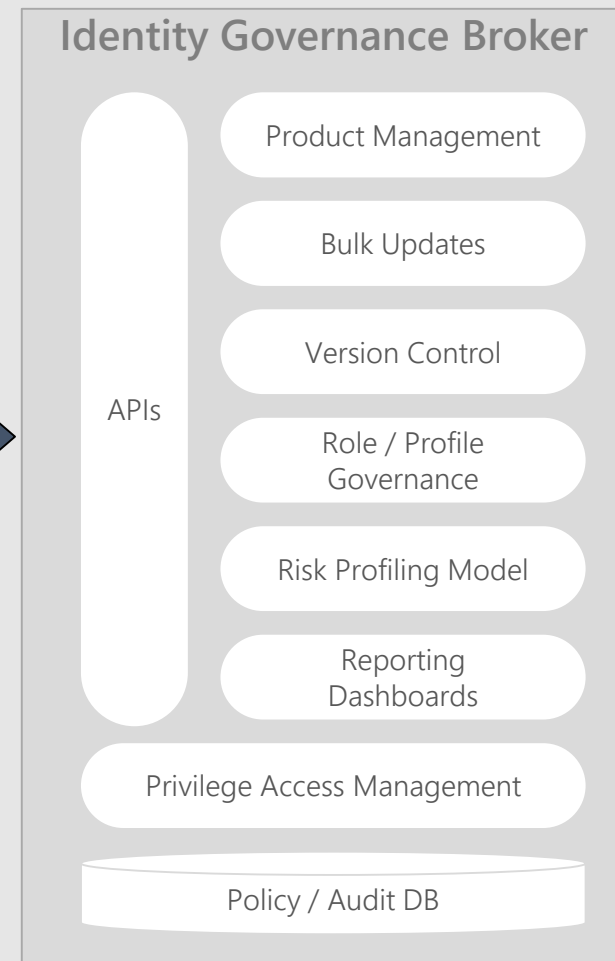- Account linking based on risk associated with both user and the entity (e.g. insurance policy)

Consumer

Registered Customer

▼ RISK   ▲ TRUST

Trusted user

User
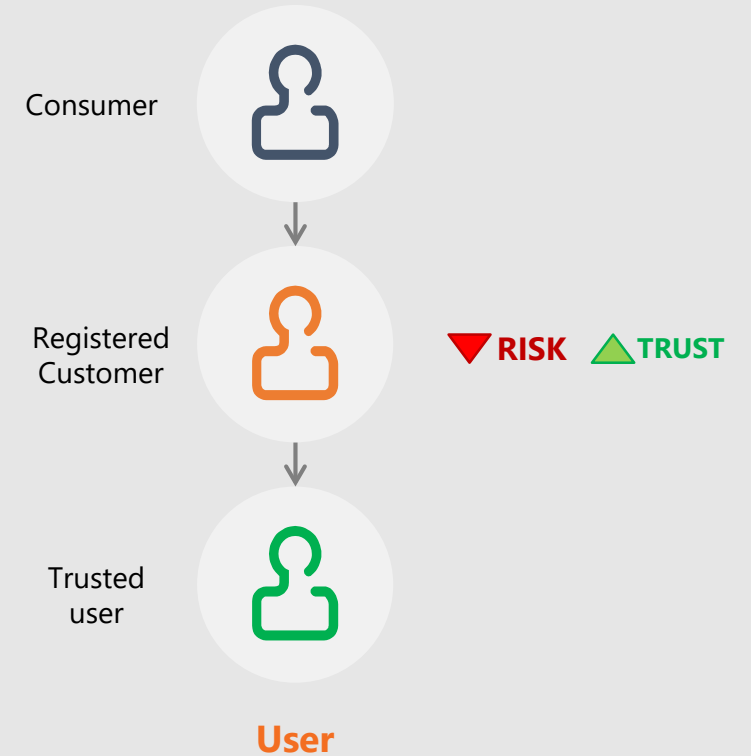
Ability to select ID proofing providers based on the risk framework

- ANOMALI
- experian.
- IDOLOGY
- JUMIO
- LexisNexis
- neustar.
- SECURONIX
- SOCURE
- CMDB,...

2 Access Control & Policy Management

simplify access model across multiple portals/applications

- Enforce visibility rules for attribute management, trigger approval workflows upon state change

- Perform provisioning actions upon state change across multiple repositories

Product Owners

Customer Support

IDM Management

Identity Governance Broker

APIs

Product Management

Bulk Updates

Version Control

Role / Profile Governance

Risk Profiling Model

Reporting Dashboards

Privilege Access Management

Policy / Audit DB

3 Privileged Access Management

for consumer facing applications...

- Manage product and service catalogs

- Support granular delegated administration of users / organizations with integrated audit and traceability

- Organize access and subscription bulk changes to user communities, manage attribute inheritance model

- Continuous governance of access, policies

Context aware

Delegated Administration

Risk modeling

4 Self-Service Capabilities

enabling customized experience

- Visibility into their personal information

- Consent management (GDPR, PSD2 compliance)

- Subscription management

- Password management

Privacy / Consent Management

Profile Management

Password Management

5 Risk aggregation & distribution

to continuously monitor user and entity behavior

- Integration with UEBA / Threat Management tools for additional threat intelligence feeds

- Propagate risk to authentication providers as well as downstream applications

Behavior Analytics

Preventive Controls

Compliance Management

So, how does the end-state CIAM architecture look like?

IT Security Audit / Compliance

Employees

Customers, Partner Admins

Customer Support

Portal / App Owners

CONSUMER APPS / PORTAL SERVICES

Micro-services abstraction layer

IDENTITY MGMT. & GOVERNANCE

Manage Account (Self-service / delegated)	Account Validation / Linking	Subscription / Profile Management	Privacy / Consent Management	Forgotten ID / Password Management
Portal Entitlement Management	Privilege Access Management	Product / Service Catalog Management	Case Management Support	Just-in-time Provisioning

Tiered Identity Proofing	Risk Profiling / Management	Delegated User Administration	Access Review
Role / Policy / Group Management	Workflow	Provisioning	Reports, Controls, Dashboards

ACCESS MGMT.

Federation / Single Sign-On	Multi-factor Authentication	Adaptive Authentication	Session Management
Access Policy Management	Web Services Security	Security Token Service	Audit, Reports

3rd Party / Internal Risk Providers	Customer Identity Stores, AuthN / AuthZ stores, Legacy Platforms	User & Entity Behavior Analytics	Customer Master Data Management

Questions?

www.saviynt.com

yash.prakash@saviynt.com