

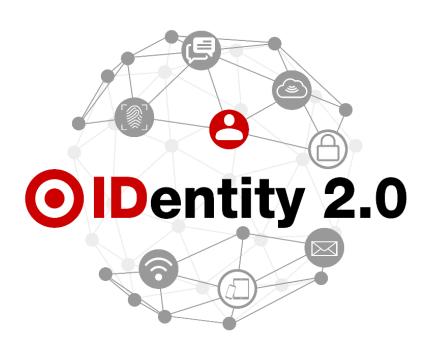
Identity 2.0

Simple. Seamless. Secure





- Executive summary
- What is Identity @Target
- Our Identity journey
- Guiding principles of ID2.0
- Key ID2.0 milestones



ID2.0 – Executive Summary





Consolidate multiple authentication and identity management platforms (13 \rightarrow 5) Leverage open standards, DevOps & CI/CD, and increased automation



Passwordless authentication for low risk transactions

Reduced effort to request and maintain access

Reduced friction for Target engineers to consume IAM services



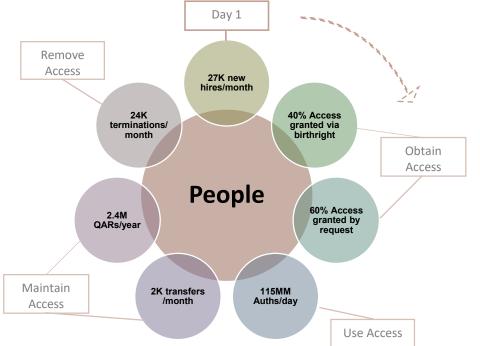


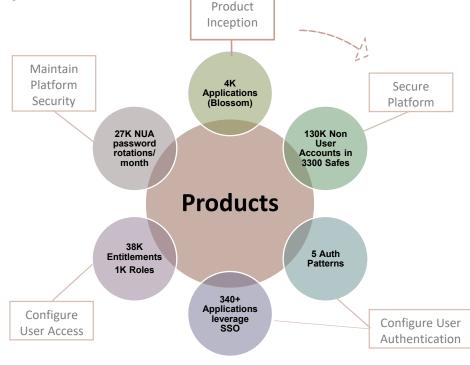
Reduced identity attack surface

Contextual authentication experiences based on risk

Continued focus on compliance and risk reduction









Identity Journey at Target



Program ripe for improvement:

- Few IAM SMEs; heavy dependence on CTs (70%)
- \$25M/yr IAM program
- · Lack of top-down strategic vision for IAM
- Lack of accountability/governance in IAM team
- Slow and inconsistent user user experience -Access request & reviews
- Complex IAM products landscape (13) with overlapping functionality
- No SDLC followed for development work
- · Lack of true single sign on
- Poor catalog health due to lack of governance
- Significant SOx deficiency
- Overall low customer satisfaction

Build team:

- ~10 external IAM hires across IAM (Engs/Ldrs)
- Transition out high cost contractors (40% CTs)

Simplify access and platform

- Stabilize Platform (Incident Tickets Reduction)
- SAP Role Redesign, Rogue Access & SoD Mgmt

Drive efficiency for customers

- 80% catalog health
- Reduce NUID provisioning time (10d to 1h)
- Automate RACF provisioning

Security & Compliance rigor

- 100% healthy SOX entitlements
- Implemented 2FA for all 3rd party vendors
- 0 SOx deficiencies
- Functional Monitoring launched

Build team:

- ~10 external IAM hires across IAM
- Continue CT elimination (30% CTs)
- Launched Product model; adopted Agile

Simplify

- \$19.2M IAM program
- Application centric onboarding
- ID2.0 program launch; ↑ platform automation

Enhance User Experience

- One login experience & next-gen UI launched
- Unified interface for Access/QAR review
- Access review recommendations
- Self-service & API access to IAM services
- 40% RBAC coverage

Compliance and Risk Reduction

- Quality Program launched
- Reduced Privileged Access attack surface
- Establish CAPA process for the IAM program
- 0 SOx deficiencies

2018:

- 80:20 TM:CT mix
- \$17.6M IAM program

Simple:

4 IAM platforms sunset

Seamless:

- 80% RBAC coverage
- IAG Recommendation Engine launch
- Self-service & API (12 new) access to IAM

Secure:

- Contextual authentication launch (340)
- Reduce Identity attack surface

2019+: IAM solution maturity

- IAM platform entitlement (5 distinct capabilities)
- API-everything through TEIP
- Identity Analytics drive IAM decisions
- IDaaS for Partners
- True SSO fewer logins & single global identity
- · Just-in-time access provisioning
- Role lifecycle management self-service
- Risk-based network and device access model
- Device / IoT identity management

2010-15

IAM Assessment:

IAM Assessment:

E∲ 1 Assessment: Level: 2.5 IAM Assessment: Level 3 2018+

2018 IAM Assessment:

Level 3.5

To be achieved

70:30 TMs:CTs \$19M/yr IAM program

2017

80:20 TMs:CTs \$18M/yr IAM program

Guiding principles of Identity 2.0

Identity 2.0 will...



- Consolidate 13 IAM platforms to 5, simplifying maintenance efforts and providing cycles to devote to business
- Standards-based architecture provides flexibility to growth with market & technology landscape
- Target Enterprise Identity Platform for Product teams to consume IAM
- DevOps & CI/CD patterns to manage infra and app stacks



- Rule- and Role-based access model simplifies access request processes and reduces QARs
- Mobile, intuitive UI available wherever, whenever, & on whatever device needed
- Identity Analytics driving decisions e.g. Access Recommendation Engine, outlier access, customized risk scoring - enhance user experiences (UX) and increase security
- Less reliance on Passwords and launch of new authenticators enhance UX and increase security



- Contextual risk experiences drive customized UX across apps, data & business processes
- Privileged Access reduction increases security
- Strong authentication across apps and infrastructure protects Target
- Just-in-Time access assignment reduces privileged attack surface & reduces QARs

Key ID2.0 Milestones

