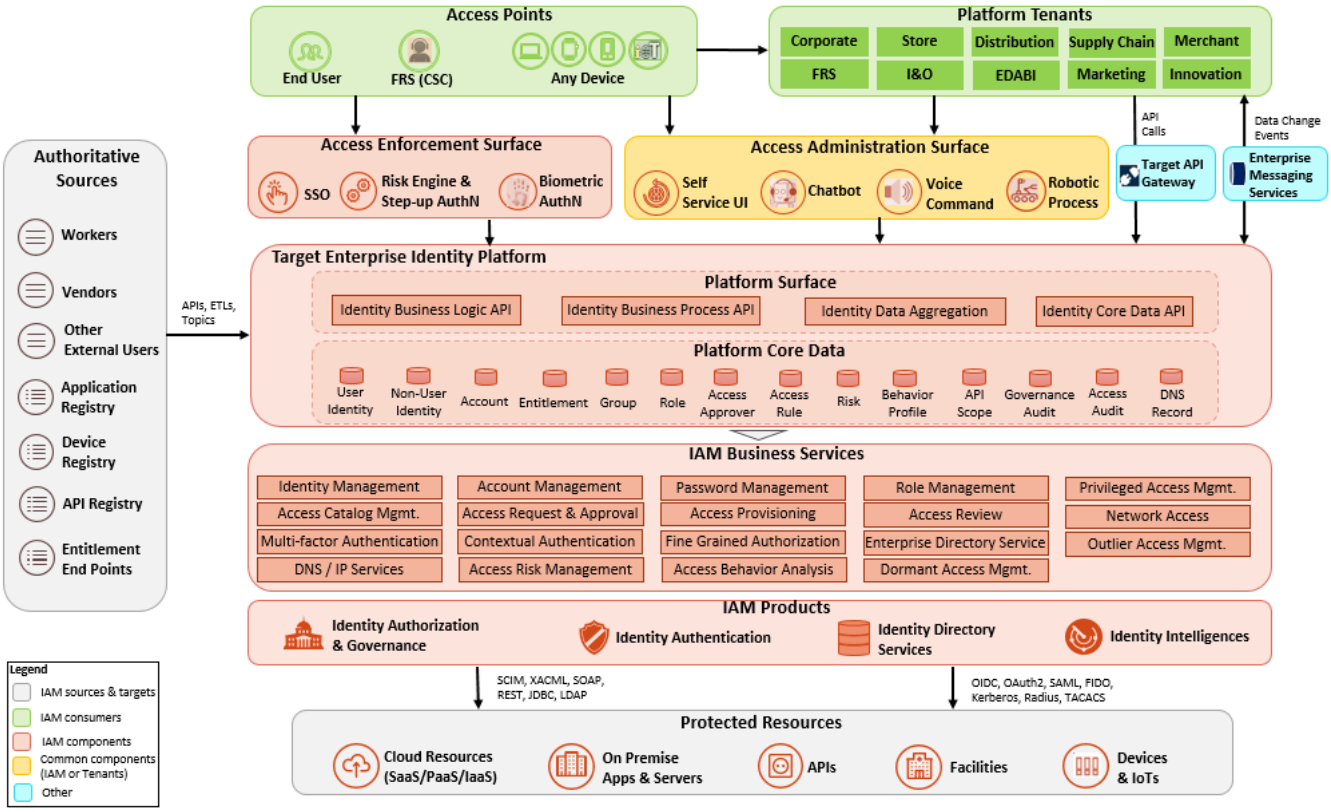
IAM Reference Architecture

IAM Architectural Diagram & Illustration



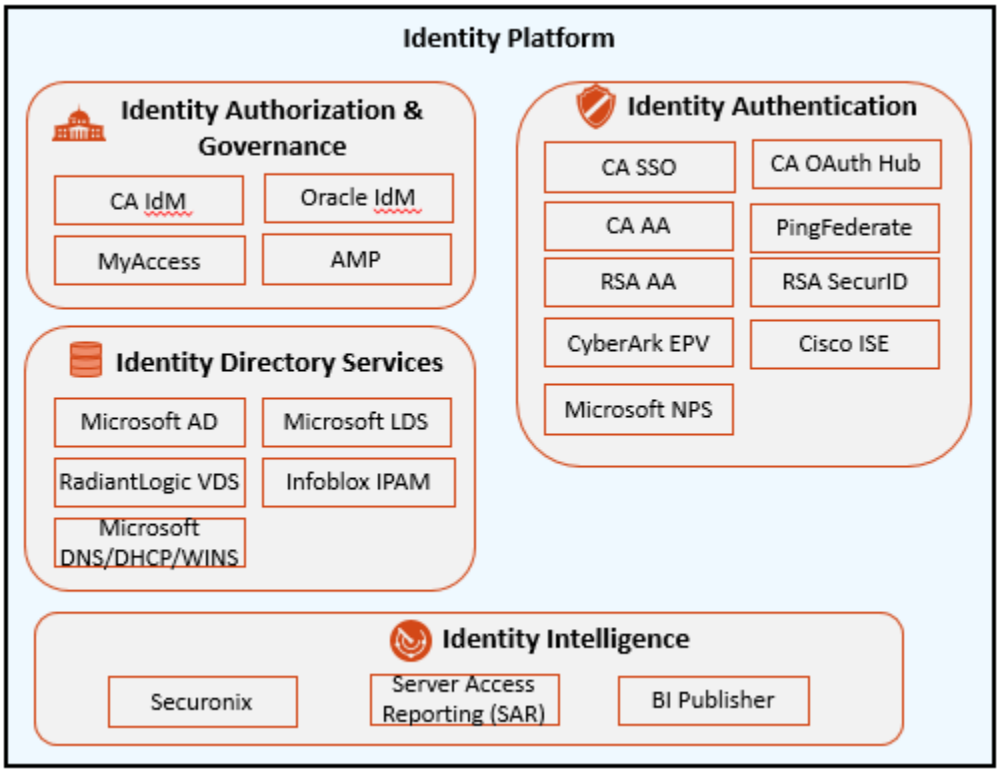
- **Authoritative Sources:** A set of authoritative sources supplying change events and profile data for user and non-user, and information about the protected resources via API calls (REST / SOAP), message queues or ETL processes. Worker platform (Workday, Beeline), vendor platform (VMM) are the sources for team members, contractors, and external vendors, respectively. Application registry (e.g. Tulip) and device registry (e. g. Northstar) provides profile data for non-user (i.e. app and device, respectively). API registry (e.g. Target API gateway / Consul) and various entitlement end points provides information about APIs and end points (e.g. applications, servers) that needs to be protected. As business evolves, other types of external users (e.g. external developers, marketing partners) may be identified and served by IAM.
- **Access Points:** Any users (e.g. team members, contractors, vendors) may access protected resources via any device (e.g. laptop, workstation, smart phone, wearable, IoT). End users may also get assistant from FRS Client Support Center (CSC) for identity needs (e.g. password reset, access fulfillment). Tenant app or device (non-User) may also need to access protected resources either by itself or on behalf of a user. Each user and non-user requires own unique identity for access mananagement. Any users (e.g. team members, contractors, vendors) may access protected resources via any device (e.g. laptop, workstation, smart phone, wearable, IoT). End users may also get assistant from FRS Client Support Center (CSC) for identity needs (e.g. password reset, access fulfillment). Tenant app or device (non-User) may also need to access protected resources either by itself or on behalf of a user. Each user and non-user requires own unique identity for access management.
- **Platform Tenants:** Tenant applications are owned by various product teams or business units, e.g. corporate systems, supply chain, etc. Platform tenants can leverage Target Enterprise Identity Platform (TEIP) APIs or events to consume IAM business services for administrating and controlling user and non-user access to their applications. Tenant applications are owned by various product teams or business units, e.g. corporate systems, supply chain, etc. Platform tenants can leverage Target Enterprise Identity Platform (TEIP) APIs or events to consume IAM business services for administrating and controlling user and non-user access to their applications.
- **Access Administration Surface:** Self-service UI can be used for administrating and governing user access (e.g. access request, approval, provisioning and review), configuring own authenticators, setting up authentication client, and so on. Chatbots and voice commands makes access management more convenient for users. Robotic processes leverage Robotic Process Automation (RPA) technologies to replace repeatable manual access administrative tasks performed by users where automated access management is not feasible. If needed, platform tenants can also build own access administration surface leveraging TEIP APIs instead of having their users interact with the surface provided by IAM.
- **Access Enforcement Surface:** Single Sign On (SSO) provides one login experience to users for accessing protected resources. Biometric authentication (e.g. fingerprint, voice, facial recognizance) provides more convenient and secure way for user access based on who the user is, as oppose to what user knows (e.g. password) or possesses (e.g. secure token). Risk engine plays a key role in authentication by analyzing access behaviors and contextual information (e.g. geolocation, browser, device) to detect abnormal access, determine its risk level, and trigger additional / stronger authentication mechanism before access is allowed. Single Sign On (SSO) provides one login experience to users for

accessing protected resources. Biometric authentication (e.g. fingerprint, voice, facial recognition) provides more convenient and secure way for user access based on who the user is, as oppose to what user knows (e.g. password) or possesses (e.g. secure token). Risk engine plays a key role in authentication by analyzing access behaviors and contextual information (e.g. geolocation, browser, device) to detect abnormal access, determine its risk level, and trigger additional / stronger authentication mechanism before access is allowed.

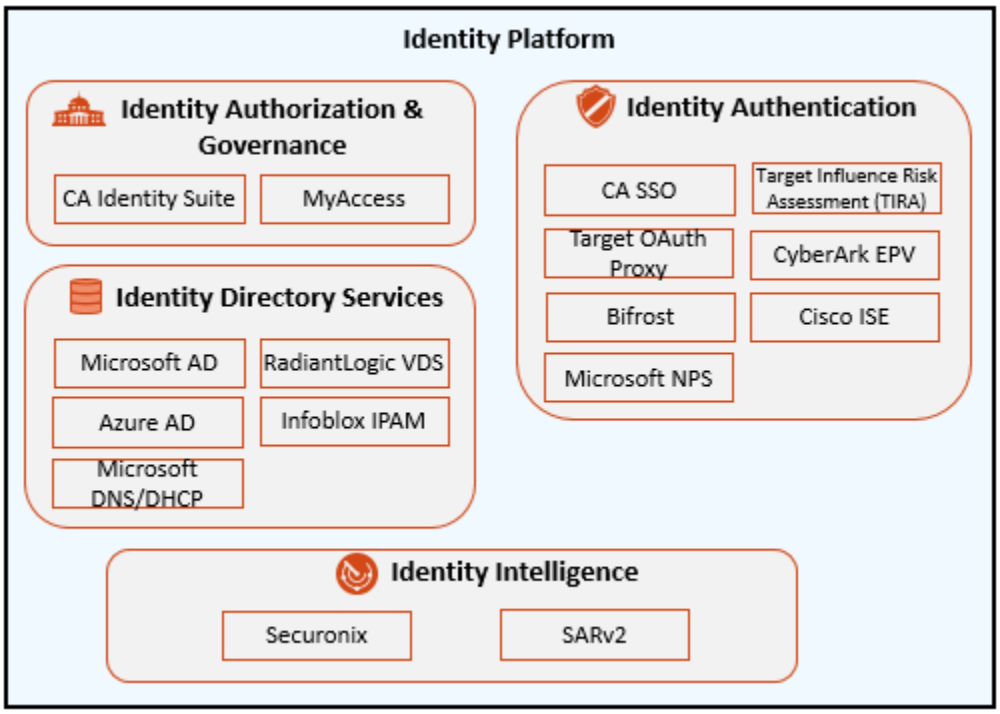
- **Target Enterprise Identity Platform:** TEIP enables tenant applications to directly consume IAM services via API calls or data change events to provide more tailored and intuitive IAM experience serving own users and business needs. TEIP also provides backbone functions / services for central IAM services exposed to users and other non-users. Read TEIP Whitepaper for more information.
- **IAM Products and Services:** A wide range of IAM services provided by IAM products
    - Identity Authorization & Governance (IAG) product focuses on providing services for user and non-user identity management, access administration, access review and identity data governance. Just-in-time and just-enough access shall be provided to users, adhering to Least Privilege and Need to Know security principles. Role-based / attribute-based / rule-based automatic access grant / revocation is more preferable than explicit access request & approval. Risk-based and event-driven access reviews are more efficient than periodically scheduled reviews to meet compliance requirements.
    - Identity Authentication (IA) product focuses on providing services for run time access control (authentication and authorization) in heterogeneous environments, such as web singled sign on (SSO) for web apps, federated SSO for external partner / SaaS apps, adaptive access for internet facing / high risk apps, multi-factor authentication for remote network access, central authentication (AD bridge) for Unix/Linux servers, password vault for privileged access, secrets management for developers and applications, jump host for accessing Cloud infrastructure, and so on. Authentication becomes more dynamic in modern digital world, driven by contextual information and identity relationships as oppose to traditional access control list or static access rules. Variety of authentication methods shall be provided to reduce dependency on password and to provide better user experience and security, e.g. authenticator based on what you know (other than password), who you are (biometrics), what you have (device, token, etc.) and what you do (behavior patterns). Authorization becomes more granular and needs to be supported down to data elements and transaction level.
    - Identity Directory Service (IDS) product manages enterprise directory (user and non-user stores) serving identity, authentication and authorization needs. It also provides DNS / IP services to engineering and infrastructure teams.
    - Identity Intelligence (II) product focuses on gathering and analyzing access granted to the user and access used by the user to provide actionable insights for continuous improvement of access governance and access control to reduce risk and meet security and compliance requirements.
- **Protected Resources:** A wide range of resources need to be protected from unauthorized use, including SaaS apps, Cloud platforms and infrastructures, on-premise apps and servers, API operations used for app-to-app or machine-to-machine interactions, restricted facilities (e.g. badge access), devices and Internet of Things (IoTs). All protected resources should have risk levels determined by sensitivity of data and operations, compliance requirements, business criticality and so on. Identity level of assurance (LOA) and authentication LOA must be appriopriate to the risk level of protected resources being accessed. Standard protocols should be followed for provisioning access (e.g. SCIM, JDBC, LDAP) and controlling access (e.g. OIDC, OAuth2, Kerberos) to the protected resources.

Technology Evolvement

As-Is Technology Landscape (2018-2019)



To-be Technology Landscape (2019-2020)


Identity Platform
Identity Authorization & Governance
CA Identity Suite
MyAccess
Identity Directory Services
Microsoft AD
RadiantLogic VDS
Azure AD
Infoblox IPAM
Microsoft DNS/DHCP
Identity Authentication
CA SSO
Target Influence Risk Assessment (TIRA)
Target OAuth Proxy
CyberArk EPV
Bifrost
Cisco ISE
Microsoft NPS
Identity Intelligence
Securonix
SARv2