



Zero Trust Converged IAM

Secure user access, privileges, identities,
devices across your extended enterprise

Identity and Access Management Solution
with an IGA Suite that helps growing
enterprises be IT Compliant in real-time
with a frictionless user experience.

Security & Governance just got friendly!

- Identity Store, RBAC, Connectors to help scale up and manage user access to critical applications
- User Self Services that provides managers with greater flexibility and control over cloud application/systems
- Access Management and Governance on a single platform, ensuring effective risk and compliance management

Modules

IDENTITY MANAGEMENT



Manage User
Lifecycle



Visualise &
Approve Identities



Create
Identity Store



Connect
applications

User Lifecycle management

- **Create users** and manage their identity lifecycle with **custom attributes** across auditable workflows and life-cycle events
- Manage Entitlement through auto-provisioning and **Cymmetri Workflow Engine**
- **Synchronize & Reconcile** between source and target systems
- Automate controls based on **Hooks & Scripts**
- Hassle free process with no backend implementation.

Role Management

- **Define, Discover and Manage** the organization's business roles across applications, assigning entitlements and authentication policy
- Enable **RBAC/ABAC** provisioning and sync with the managed system for any role creation and modification activities
- **Visualise and Analyse** the entitlements available to a single user as well as to digital resources
- Business centric **Segregation of Duties** to simplify access request and certification

Identity Store & Connectors and Applications

- Connect various Identity Sources into a **Single Source of truth**.
- **Out-of-box configurations** for cloud and enterprise applications for authentication with minimal settings
- Controls for AWS, Azure and other Cloud Platforms with SCIM
- User **Just-in-time provisioning** when authenticating with source system (AD or HRMS)

IM Policy and Rule Engine

- Master rule engine to manage an organization's **security policies** for Identity management

IDENTITY GOVERNANCE



Access
Re-certification



Audit and
reports



Alerts and
Notifications



SoD and Risk
Profiling

ACCESS MANAGEMENT



Streamline
with SSO



Secure with
MFA



Privileged
Access Mgmt



User Self
Service

SSO and Federated Identity

- Secured **Single Sign-On (SSO)** with One-click access to all apps – from any location and any device
- Trusted framework to Integrate on-premise & cloud applications for seamless authentication of users (**Passwordless Access**)
- Integrate all target systems like **AD & LDAP** with any Authentication provider [SAML, OpenID connect/Oauth, Custom API-based token exchange & Reverse Proxy]
- *Reduce exposure and handle security risks with Privileged Access Mgmt*

Multi Factor Authentication & Rule Engine

- Enable different Multi-Factor Authentication methods for a smart and secure system
- **Cymmetri and Google Authenticator** (mobile apps) with **ToTP, Consent based authentication, SMS Authentication, Secret Question & Answers, Biometric methods (coming soon)**
- Intelligent **Contextual Access** management with adaptive rules and policy engine to authenticate users on basis of their - *Network reputation, geographic locations, devices, time anomalies and more*

Access Delegation

- Allow **user to delegate their access** to others within the organization when on leave or travelling

User Self Service

- Empower users and managers with **Self Service Capabilities** - *Managing Sessions, Password Reset, Profile Management, Trusted Device Management, Account History, Authorised Apps, Privacy & Consent*

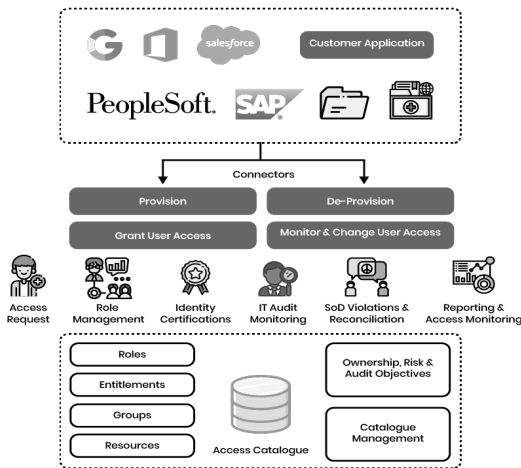
Privileged Access Management

- Password Vault, PAM Policy Management, Session Management & Recording, Session Review

- **IGA Suite** to ensure compliance and protect systems from cyberattacks and breaches
- Schedule **Audit Campaigns & Access Re-Certification**
- Generate a **Corporate Risk Profile** for the organization.

Key Workflows

- Auto Provisioning & Deprovisioning workflows based on Roles and Entitlements
- Design your user joiner, mover and leaver process workflows with SSO
- Alerts, notification and escalation workflows with custom communication designer
- Governance workflows using a Rules and Policy Library
- Configure and Schedule Audit Campaigns for security policies
- Validate IT Security Compliance Checks.
- Approvals and Access Management workflow managed without IT Admin support



Technical Specifications

- n-tier organizational structure
- LDAP and Active Directory synchronization and reconciliation
- Single Sign On using SAML, OpenID/Oauth, API/Token and Reverse Proxy
- Multifactor Authentication through Time-based OTP, SMS OTP, Email OTP and Push Notifications (Mobile Application)
- Social sign-in with 20+ social identity providers including Facebook, Google, Github etc.
- Cloud SaaS, on-premise & hybrid product architecture
- Micro services based architecture
- Multi-tenancy enabled
- Scalable Document DB (based on industry first NoSQL approach)

Feature Table

Identity Management	
Automated Provisioning and De-provisioning	✓
Reconciliation and Synchronization	✓
Hooks and Scripts	✓
Role Management	↻
Entitlement Management	✓
Workflows (User and Group Provisioning)	↻
Self-service portal to create requests and approval	✓
Out-of-office Access Delegation	✓
Application and Database Connectors	✓
Active Directory integration (AD/LDAP)	✓
Organisation Structure	↻
JIT Provisioning and Controls	✓
Access Management	
Flexible Password Management	✓
SSO Protocols (SAML, oAuth 2, Open ID, custom token)	✓
MFA with Configuration Rule Engine	✓
Contextual access to application with MFA	↻
Application specific access policies	✓
User self service (Password change, access delegation, self-registration, Additional MFA)	✓
Passwordless Authentication	✓
Governance	
Access Re-Certification with campaigns	✓
Segregation of Duties	↻
Risk Profiling	✓
Identity Discovery	↻
Audit Event Alerts	✓
Audit logs	✓
Reports	✓
Developer	
Extensibility Options	✓
Custom connector SDK	↻
RESTful API	✓
Documentation	✓

A single integrated & intelligent security platform which helps you visualise identities, secure access via adaptive Multi-Factor authentication, establish Rules and policies, Advanced User Life-cycle management, Workflows and much more!

An Intuitive and adaptive IAM with intelligent controls



Business Benefits

- Scale up and down IT Systems aligned to business requirements with a secured workflow engine
- Insights on access patterns, manager checks, review requests that optimises workloads
- Secured access governance and compliance with security policies and audit logs/reports

User Benefits

- Request access to various datasets, platforms, and tools you need through a self service portal
- Use a SSO and MFA with minimal password management on business applications
- Feel Secured & Confident while authorizing business transactions and managing team workflows

Admin Benefits

- Improve security posture by enabling employees', partners, & customers access to their designated resources
- Eliminate chance of Data Theft & Intrusion with a rule based auto deprovisioning and security layers
- Ensure adherence to regulations & trace the Who, What and Why of all identities, devices

Mission Critical Clients









Connect with us for a free consultation and get early access to our platform.