FACTSHEET

IDENTITY MANAGEMENT & ACCESS MANAGEMENT

Cogito Group - IdMaaS

THE CHALLENGE

Today's technological landscape is one of permanent change. While connections to digital services and mobile devices grow, securing the data generated by those connections is a challenge to manage. Managing it all in one place and sharing this data across typically siloed systems presents a challenge and an opportunity to do more, with less.

As the number of people, devices, services and connections continue to grow by the billions, our systems are no longer only on our physical premises. They are accessed by many devices any time, day or night from anywhere in the world. They are accessed not only by employees but contractors, customers and partners.

To balance security, usability and cost effectiveness, Cogito Group has developed a customisable, modular approach to identity management. Jellyfish allows components to be added and removed based on organisational security requirements.

Cogito's Jellyfish IdMaaS Solution:

- ✓ *Secure*
- ✓ *Adaptable*
- ✓ *Integrated*
- ✓ *Simple*
- ✓ *Modular*
- ✓ *Scalable*
- ✓ *Cost-effective*

Enhance your security through:

- ✓ *Increased visibility*
- ✓ *Greater control*
- ✓ *Stronger protection*

OUR JELLYFISH IdAM SOLUTION

The Jellyfish solution is modular. It is designed as an integrated cohesive stack that is purpose-built to handle complexity. This is not a set and forget solution, it's organic and will grow with your security requirements.

Jellyfish is a simple, cost-effective, low-risk, complete solution for connecting identities such as users, devices and services to each other.

Cogito Group's Jellyfish is a complete and integrated cyber security platform.

- **Manage your users, credentials, devices and access through:**
  - **Enhanced security and sensor fusion**
  - **Better visibility**
  - **Simplified and central control**
- **Improve end user productivity through:**
  - **Seamless authentication**
  - **Automation**
    - **Reduce your administration burden**
    - **Enables cost reductions**
    - **Automate changes across your network**
  - **Self-service**
    - **Add and remove resources from a single point across multiple applications and services**

BENEFITS

- **Offers the cost benefits of a cloud service**
- **Improves productivity of resources**
- **Improves transparency through monitoring, auditing, reporting of security breaches**
- **Highly scalable through a customised modular approach**

Jellyfish provides a single access interface for:

- **IdM – Identity management with CRUD operations, data transformation between source and target systems for users and resources and configurable workflows.**
- **IdAM – Access management service is also able to provide integration with logical and physical access control systems (including integration with legacy systems) through adaptive support for modern authentication protocols as well as emerging standards and multifactor authentication. This ensures access to systems and building areas can seamlessly be added and removed as people join, move within or leave an organisation through existing HR functions.**
- **MDM – The ability exists to manage Mobile Enterprise and BYOD devices from within the system as well as to use these devices as one factor in secure multifactor authentication.**
- **Credential Management – Credential management services provides administrators with the ability to issue and manage certificates, smartcards, and OTP tokens. An Auto-enrolment capability is also provided.**

LAYERS OF SECURITY

Identity Management

Our Identity Management solutions provide strong authentication to ensure users and devices accessing your network are who they claim to be.

Identity and Access Management (IdAM) applications such as network authentication, digital signatures and other services based on Public Key Infrastructure (PKI).

Identity Management systems provide the basis for the collection, management and synchronisation of identity information and attributes between disparate systems.

These systems reduce the effort and cost of the management of data by managing the identity data throughout its lifecycle. Identity Management systems provide workflow for the automation of access to systems and services either by an approval process or based on identity attributes.

Access Management

Our access management solutions allow organisations to provide integrated physical access to their buildings, paired with logical access to ICT systems and data, alongside web-based access to services. Making the logical connection of Human Resource (HR) workflows (commencing employment, termination, transition) and the access workflows to both physical access (building); logical access (ICT) systems and Web SSO. Access Management is based on the known and assured identity.

Mobile Device Management

Our mobile device management solution enables operators to remotely manage the entire life cycle of a device, significantly reducing support costs, considerably increasing data revenue, and maximising customer satisfaction. Giving customers fast and simple online authentication with a convenient single ID password. In addition, it protects privacy and reinforces online security.

Credential Management

Our card/Credential Management solutions manage the association between an identity and their issued credentials. They manage the lifecycle of trusted tokens such as smart cards and now provide capabilities for the management of virtual smart cards and credentials delivered to smartphones and other mobile devices.

Protected Data

Our Protected Data Store provides key management and protection as well as transparent encryption of structured, sensitive data residing in databases, files and file systems, storage units, directories and applications.

These security products provide protection of data in transit and at rest and are ideal for implementation in physical, virtual or cloud environments.

Monitor

Our solutions can monitor a variety of operating systems, network devices and server hardware platforms. The various components that make up your overall solution package will be monitored and may include, Microsoft products, Microsoft infrastructure services, Hardware platforms,

Environmental Services, Network and Storage Devices.

Audit

Auditing can publish and log all relevant system activity to the targets you specify. Auditing can include data from reconciliation as a basis for reporting, access details, and activity logs that capture operations on internal (managed) objects and external (system) objects. Auditing provides the data for all the relevant reports, including orphan account reports.

Report & Analytics

Our solutions apply behavioural analytics technology to providing real-time, risk-based authentication. Bad actors using good credentials to compromise an account will behave differently from the legitimate user. Our solutions distinguish between legitimate log-in activity and unauthorised access.

Cogito Group is an award-winning ICT company specialising in authentication, cloud security, identity management and data protection. Cogito Group protect the authentication methods used to access information through the use of Identity and other security technologies.