Fact Sheet

Cogito Group

Identity and Access Management

The Challenge

The technological landscape organisations face today is one of constant change. As use of digital services and mobile devices grows, the need to secure data generated by these connections presents a significant challenge to organisations. Often, organisations will require this data to be managed from a single, secure point, and to be shared across siloed systems. This sounds daunting, but this challenge presents the organisation with the opportunity to do more with less.

As the number of interconnected people, devices, and services grow by the billions, systems are no longer contained to an organisations physical premises. They can be accessed by millions of devices at any time, from anywhere in the world. These systems aren't limited to employees, but can be accessed by contractors, customers, and partners.

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

Jellyfish Identity and Access Management Solution

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

COGITO'S JELLYFISH SOLUTION

Secure

Adaptable

Integrated

Simple

Modular

Scalable

Cost-effective

Identity and Access Management

Fact Sheet

Cogito Group's Jellyfish solution allows organisations to manage their users, credentials, devices and access through:

- Enhanced security and sensor fusion.
- Better visibility.
- Simplified and central control.

Organisations can also 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

Cogito Group's Identity and Access Management (IdAM) solution offers the cost benefits of a cloud service, whilst improving productivity of resources and transparency through monitoring, auditing, and the reporting of security breaches. The IdAM solution is highly scalable through a customised modular approach. Jellyfish provides a single access interface for:

Identity Management

Identity Management with CRUD operations, data transformation between source and target systems for users and resources and configurable workflows.

Identity and Access Management

The 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.

Mobile Device Management

Mobile Enterprise and BYOD devices can be managed from within the system as well as to use these devices as one factor in secure multifactor authentication.

Credential Management

Credential Management services provide administrators with the ability to issue and manage certificates, Smartcards, and OTP tokens. An Auto-enrolment capability is also provided.

Identity and Access Management

Fact Sheet

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 are 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 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

Cogito Group's 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. The Access Management system makes the logical connection of Human Resource (HR) Workflows (commencing employment, termination, transition) and the Access Workflows to both physical access, logical access, and Web SSO. Access Management is based on known and assured identity.

Mobile Device Management

Our Mobile Device Management (MDM) 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. The MDM solution gives customers fast and simple online authentication with a convenient single ID password, protects privacy, and reinforces online security.

Credential Management

The Cogito Group Credential Management solution manages the association between an identity and their issued credentials. It manages the lifecycle of trusted tokens such as Smartcards and provides capabilities for the management of virtual Smartcards 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 protect 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, and 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. Threat actors using correct credentials to compromise an account will behave differently from the legitimate owner of those credentials. Our solutions can distinguish between legitimate log-in activity and unauthorised access to maximise security of systems.

About Cogito Group

Cogito Group is an award-winning, Australian owned and operated 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. Cogito Group protect data not only from unauthorised access and disclosure, but also from being altered by an unauthorised third party or a trusted insider with malicious intent. This assists in the detection and prevention of fraud or other malicious activities by third parties or trusted insiders.