Fact Sheet

Cogito Group

Jellyfish Overview

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 siloed systems presents a challenge and an opportunity to do more with less.

Our systems are no longer just on our physical premises, but in the cloud and accessible via the internet, accessed by many devices anytime from anywhere in the world. They are accessed not only by employees but contractors, customers, and partners. Controlling and monitoring access to data is crucial.

To balance security, usability and cost effectiveness, Cogito Group has developed a customisable modular approach. This allows components to be added or removed dependent on an organisations' individual requirements.

The Jellyfish Solution

The Jellyfish solution is modular, designed as an integrated cohesive stack purpose-built to handle complexity. Jellyfish is not a set and forget solution, it is organic and will grow with your security requirements. The Jellyfish solution is secure, adaptable, integrated, simple and modular, highly scalable, and cost effective.

Jellyfish enhances your security through increased visibility, greater control, stronger protection, and seamless authentication. Jellyfish is a simple, cost-effective, low-risk, complete solution for connecting identities such as users, devices, and services to each other. Jellyfish is a complete and integrated cyber security platform.

Jellyfish allows you to manage your users, credentials, devices and access through enhanced security, better visibility, and simplified and central control. You can improve end-user productivity through seamless authentication and automation of processes and changes, reducing your administrative burden. Jellyfish is self-service and enables significant cost reductions. Further improve streamlining by adding and removing resources from a single point across multiple applications and services.

Jellyfish Overview

Fact Sheet

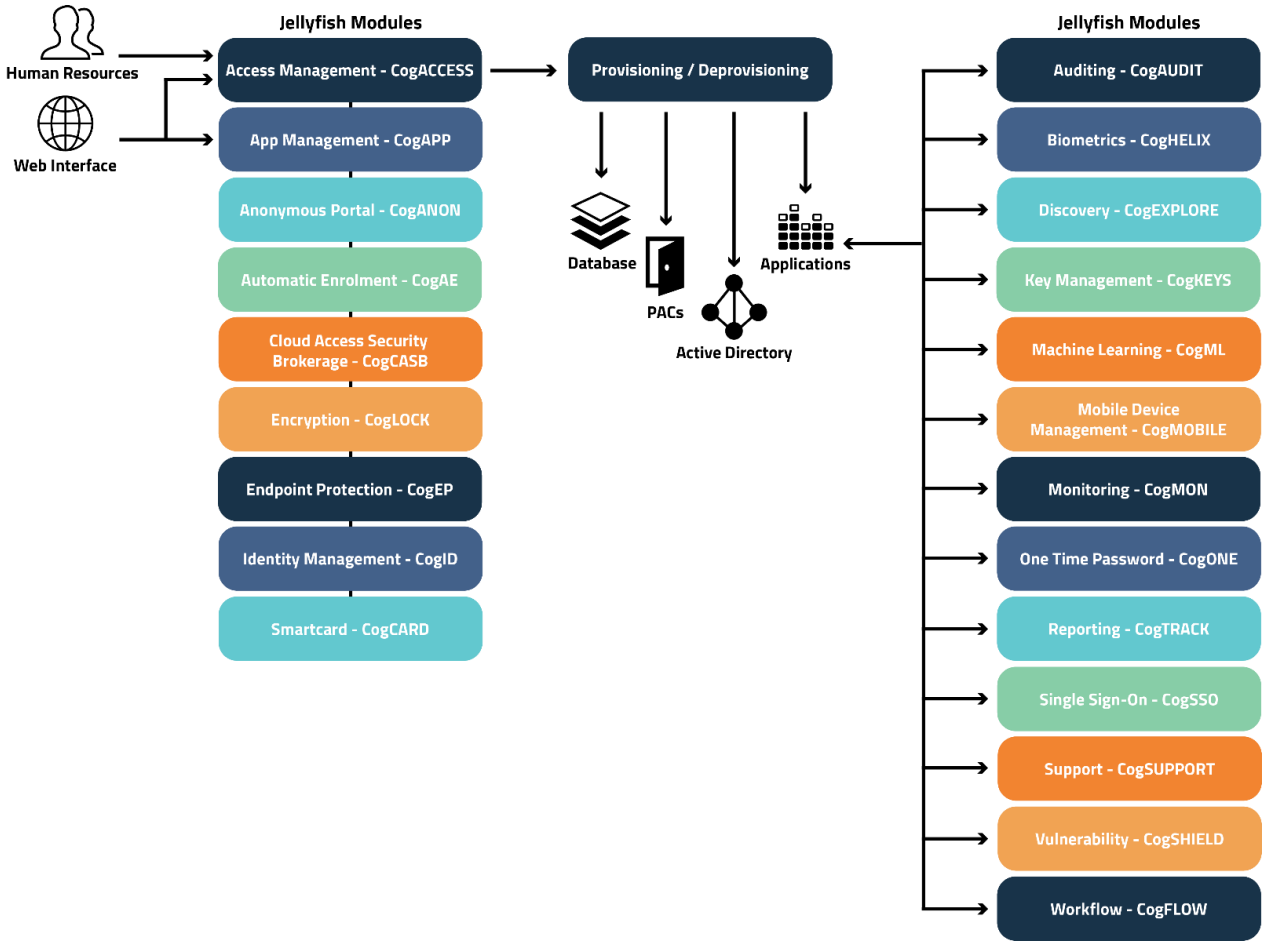

Figure 1: Challenges Overcome by Jellyfish

Jellyfish Capabilities

Jellyfish provides a single access interface for:

Identity Management (IdM)

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

Identity and Access Management (IdAM)

IdAM services are 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 Multi-Factor Authentication (MFA). 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 (MDM)

Jellyfish can manage Mobile Enterprise and BYOD devices from within the system as well as use these devices as one factor in secure MFA.

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.

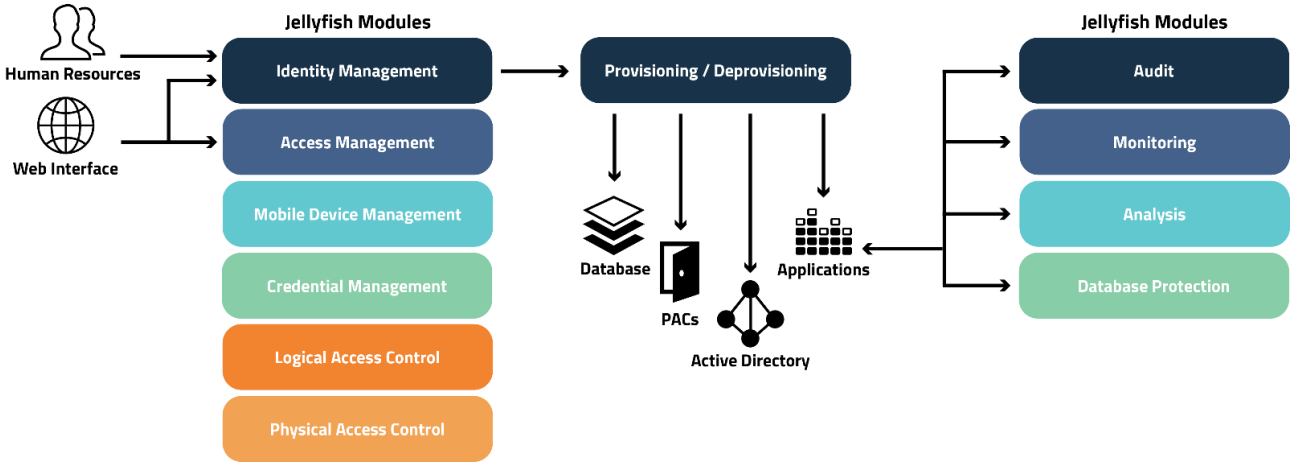

Figure 2: The Jellyfish Solution

The Jellyfish solution connects all the pieces of the security puzzle. Start with one piece and add more as your security requirements grow. Additional layers and modules can be inserted, and existing modules can be replaced with new and better technology.

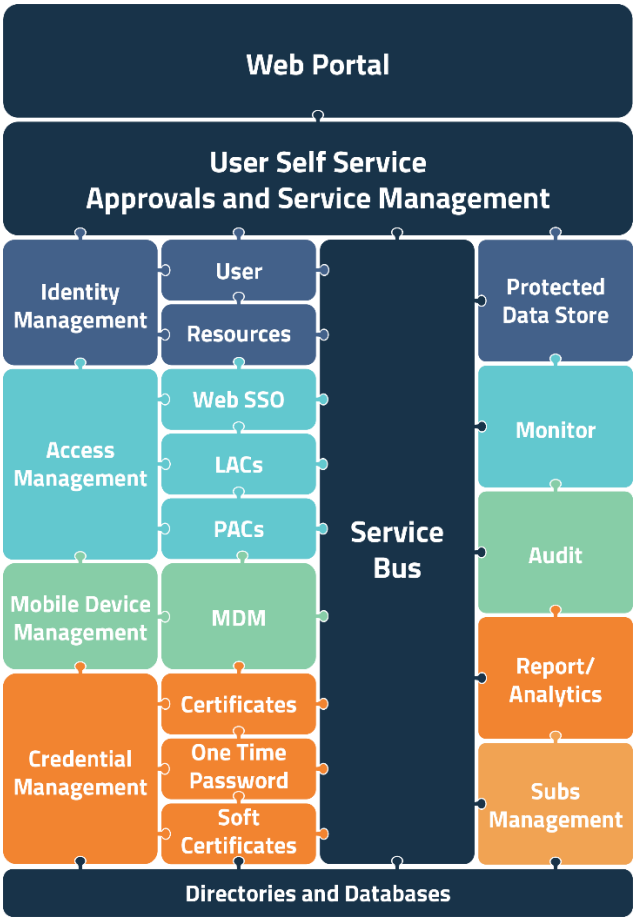

Figure 3: The Jellyfish Solution Security Puzzle

Jellyfish Overview

Fact Sheet

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.