Fact Sheet

Cogito Group

Jellyfish Product Datasheet

What is Jellyfish?

Cogito Group's Jellyfish is a complete and integrated cyber security platform. Jellyfish enables organisations to manage their users, credentials, devices, and access through a single integrated interface. Your organisation will immediately benefit from enhanced security through improved visibility and reporting on who is accessing what systems and data.

This means resources can be added or removed from a single point across multiple applications and services. This creates a source of truth for data and automates workflow. Importantly, end user productivity is improved through an easy an intuitive self-service interface that provides seamless authentication and workflow automation. This reduces administration burdens of the organisation and generates further cost reductions through automated changes implemented across the network.

Jellyfish is purpose-built to handle complexity. Designed as an integrated, cohesive stack, Jellyfish can evolve with your security requirements. Each module is created with connectivity and emerging technologies in mind. Jellyfish is the ultimate agile cyber-security platform. With Jellyfish one interface connects disparate components such as IdM, PKI, OTP, SSO, Password Management, LACS, PACS, LDAP, DB, MDM, Monitoring and Audit.

Features	Benefits
Modular Architecture	➤ An integrated cohesive stack. ➤ Only purchase what you require. ➤ Additional layers and modules can be inserted, and existing modules replaced as your security requirements evolve. ➤ Existing solutions can be integrated into the Jellyfish interface.
Single Interface	➤ Consolidate all security products and services to provide a single point of view to manage services.
Identity Management	➤ User management. ➤ Single source of truth. ➤ Credential management.

Public Key Infrastructure (PKI)/ Certificate Services	➤ API. ➤ Full certificate lifecycle management. ➤ Non-repudiation. ➤ Search and reporting capability. ➤ Authenticate the identity through a process of testing and verifying assertions. ➤ Integrity through digital signatures that data has not been altered at rest or in transit. ➤ Confidentially exchange sensitive data. ➤ SSL certificates for users. ➤ Interfaces: ACME, Microsoft Auto enrol, SCEP, F5, BMC Remedy, ServiceNow. ➤ Digicert and Let's Encrypt capability for externally trusted certificates. ➤ Multiple CA software support including AD CS. ➤ Integration to other components. ➤ Identity linkage between devices, users, and certificates. ➤ Certificate discovery. ➤ Certificate import. ➤ Bulk certificate (revocation?). ➤ CA generation. ➤ CMDB. ➤ Key management. ➤ Signing.
Single Sign On (SSO)	➤ Remove the need for users to remember and manage multiple passwords. ➤ Improve user experience through automatic login. ➤ Reduce the risk of user account lockout.

Jellyfish Product Datasheet

Fact Sheet

Provisioning	Updates and deprovisioning available for third party systems including but not limited to: ➤ JDBC databases (such as MySQL, PostgreSQL, Oracle, MSSQL). ➤ LDAP based directory servers, including AD. ➤ CSV files. ➤ Solaris, Linux, AIX. ➤ AD. ➤ MS Exchange. ➤ Office365. ➤ Gitlab. ➤ Liferay Portal.
Integration with Client Applications and Services	➤ Fully integrated Physical and Logical Access Controls. ➤ Create stronger security controls by linking access to the building with network access. ➤ On-premise PACS systems. ➤ AD. ➤ Translation to client systems. ➤ Shared accommodation services – shared WiFi, Meeting rooms, and printers between organisations with no duplicate accounts.
Token Management	➤ Card management module. ➤ Card application management. ➤ Hardware security module. ➤ Yubikey 5. ➤ YubiHSM.
Online Storage	➤ Enhanced data security. ➤ No data loss. ➤ No server maintenance. ➤ BYOK and HYOK. ➤ Work from anywhere with remote users able to access the most up-to-date versions of working documents. ➤ Data is secure and easily moved.

Jellyfish Product Datasheet

Fact Sheet

Subscription / Usage / Billing services	➤ Tenant template. ➤ Tenant registration. ➤ Subscription info. ➤ Tenant usage.
Mobile Device Management*	➤ Support of MDM platforms such as Intune, Mobile Iron and Airwatch. ➤ Supports mobile applications. ➤ Adaptive authentication.
Browser Based User Interface	➤ Administrator and User UI. ➤ Management of Users, Roles, Organisations. ➤ User Certificate Enrolment. ➤ Device Certificate Enrolment. ➤ Certificate Template selection.
Multi-Factor Authentication	➤ Adds an additional layer of protection beyond a password to better protect data. ➤ Smart card management. ➤ OTP (One Time Password) on mobile devices and tokens. ➤ Improved HSM authentication.
Secure Data Transfer	➤ Secure data transfers with advanced security capabilities. ➤ Meet regulatory compliance requirements. ➤ Assured data delivery. ➤ Securely transfer files over public or private networks. ➤ Monitor the file transfer process with integrity checks and protocol fidelity. ➤ Visibility and monitoring for better data movement. ➤ Network access Engine Improvements.
Configuration Management	➤ Asset registration. ➤ Tracking and maintenance of asset details. ➤ Maintain association between device, owner, user, location, and certificates.
Hardware/ OS/ Infrastructure	Support for: ➤ HSM. ➤ HSM key management.

	➤ YubiHSM2. ➤ nCipher. ➤ Thales/ SafeNet ➤ Utimaco.

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.