Cogito Group

Jellyfish CASB Capability and Features

Next Generation Proxy Services

Proxy services are consumed transparently by routing outbound traffic through the Cogito Cloud Security Gateway. The proxy service grants high levels of visibility over user actions which provides security administrators insights into organisational risk, as well as the effectiveness of security campaigns. Security administrators can also use proxy services to enforce defined policies in their organisation as well as redirecting non-compliant activities to pages which can inform users that their actions are not compliant with policy. Most traffic should simply go in and out of the proxy services gateway without any further action, however all transactions passing through the gateway are securely logged for further analysis.

TLS Decryption [1]

To achieve visibility over the services consumed, it is required that the communications between a consuming agency and the cloud services are intercepted. A TLS proxy means that encrypted data transmitted to and received from a cloud service can be inspected, which enables other features of a CASB offering.

Targetable TLS decryption is available in the Jellyfish TLS Decryption service. This allows the users to define domains in which TLS encrypted data can be transparently decrypted for analysis by the DLP and IDS components.

Data Loss Prevention (DLP) [2]

A common offering in a CASB is data loss prevention activities. Typically, this is implemented using search strings. For example, if a document being uploaded to Office 365 includes high entropy data, then it is safe to assume that a password is contained in the file and an incident should be raised. Other types of information that is often included in DLP filters are credit card information, and personally identifiable information. Any DLP solution must have as a minimum, content inspection and whitelists and blacklists.

[1] Support provided by the JF PA coded module
[2] Support provided by the JF PA coded module

Whitelists and blacklists should support automatic updates via a vendor provided service and also allow an organisation to provide their own organisation specific additions to these lists.

The Jellyfish DLP component allows for data filtering and response based on either predefined patterns (e.g. credit card matching, SSN matching etc.) or user defined patterns. DLP can be configured to search in document attributes and in the content of the files using REGEXP. The Cogito CASB allows for configuration of these four parameters inside the Jellyfish Admin-UI.

IDS/IPS [3]

An Intrusion Detection System analyses whole packets, both header and payload, looking for known events. When a known event is detected a log message is generated detailing the event.

An Intrusion Prevention System analyses whole packets, both header and payload, looking for known events. When a known event is detected the packet is rejected.

Cogito's solution gives deep insight into network activity and provides a threat score based on correlation of user / device activities. It also allows for automated response to known risky activities, which can be filtered by the user down to either individual user or group of users. The IPS data can be displayed in either high granularity graphs or as individual events in Jellyfish Admin-UI. In addition to this Cogito's solution can utilise this data to prevent further attack from specific vectors by triggering an event in another part of Cogito's solution. An example is that if an attack is suspected from a specific user account, that account can be temporarily disabled.

Shadow IT discovery [4]

Shadow IT discovery is the ability to discover the use of applications that are not approved for use by the organisation. While the use of non-sanctioned applications may have valid use cases, their use has a number of serious implications for an organisation. They are:

- They often circumvent many of the security controls and policies of an organisation. This can cause data loss and compromise.
- They can increase the cost of providing services. Many applications doing the same thing is not only costly to support but does not allow for prices based on the larger scale of the whole organisation.
- The location of information becomes fractured and less accessible across the organisation. This not only causes information to be less available but can lead to data loss through the cessation of service, the movement of staff and just the knowledge of the data being on a separate service.

The Jellyfish shadow IT discovery service maintains a large database of cloud applications and provides reports of the SaaS application usage through its APIs. This enables users of the Cogito CASB to view

[3] Support provided by the JF PA coded module
[4] Support provided by the JF PA coded module

reports on both sanctioned and unsanctioned IT usage, and configure automated incident response through the Jellyfish Admin UI. Indications of the risk and trust level of SaaS applications are also provided.

Sanctioned IT usage / Analytics

Effective CASB solutions need to cover a wide range of scenarios, including sanctioned and unsanctioned cloud apps, business and personal accounts on sanctioned apps, mobile device and desktops and managed and unmanaged devices, to address these scenario's CASB must leverage application-specific security and access control.

UEBA

This is a type of machine learning model that uses advanced analysis, aggregates data from logs and reports and looks at packet flow, file and other types of information as well as certain kinds of threat data to determine what activity may be a threat.

Key Management & Data Privacy

A common customer requirement and a regulation in some jurisdictions (especially for Government) is that all data stored in a cloud service must be encrypted. A CASB offering key management and data security operations can ensure that data is encrypted making compromise by a third party considerably more difficult. Further, key management can provide protection to the customer from the provider of the cloud service itself and the laws governing the service provider or the data's location.

Centralised Key Management Services

Cogito's Jellyfish platform can provide central key management services using centralised virtual or FIPS Certified hardware components. This service can be provided as an on premises, cloud or hybrid solution.

BYOK

The BYOK feature allows client to use a key from a source outside provider as the encryption key. That source can be their own on-premises key generation service or a third-party service provider. Cogito's Jellyfish BYOK capability provides application or service specific BYOK options as required by those services and applications.

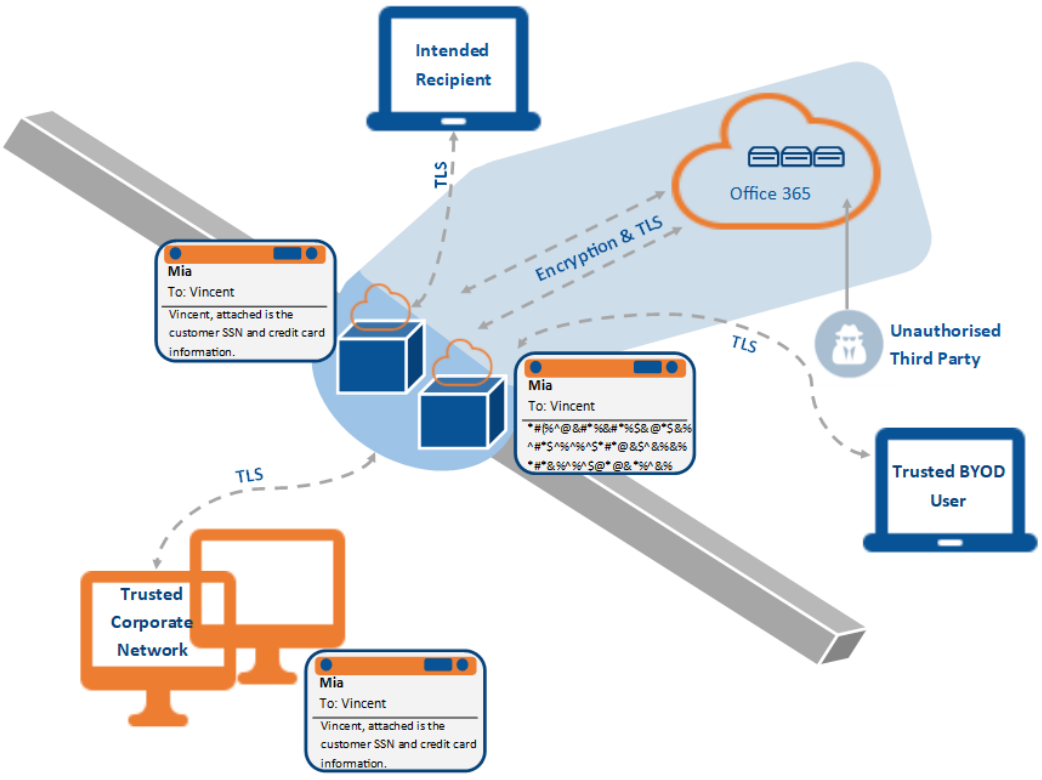
HYOK

HYOK allows client to keep their own keys in their on-premises environment. Unlike BYOK, HYOK is a configuration where client keep their own encryption keys, and all the encryption and decryption work is done with client's on-premises hardware. Cogito's Jellyfish HYOK capability provides application or service specific HYOK options as required by those services and applications.

Encryption Services

Encryption Gateway Key Management [5]

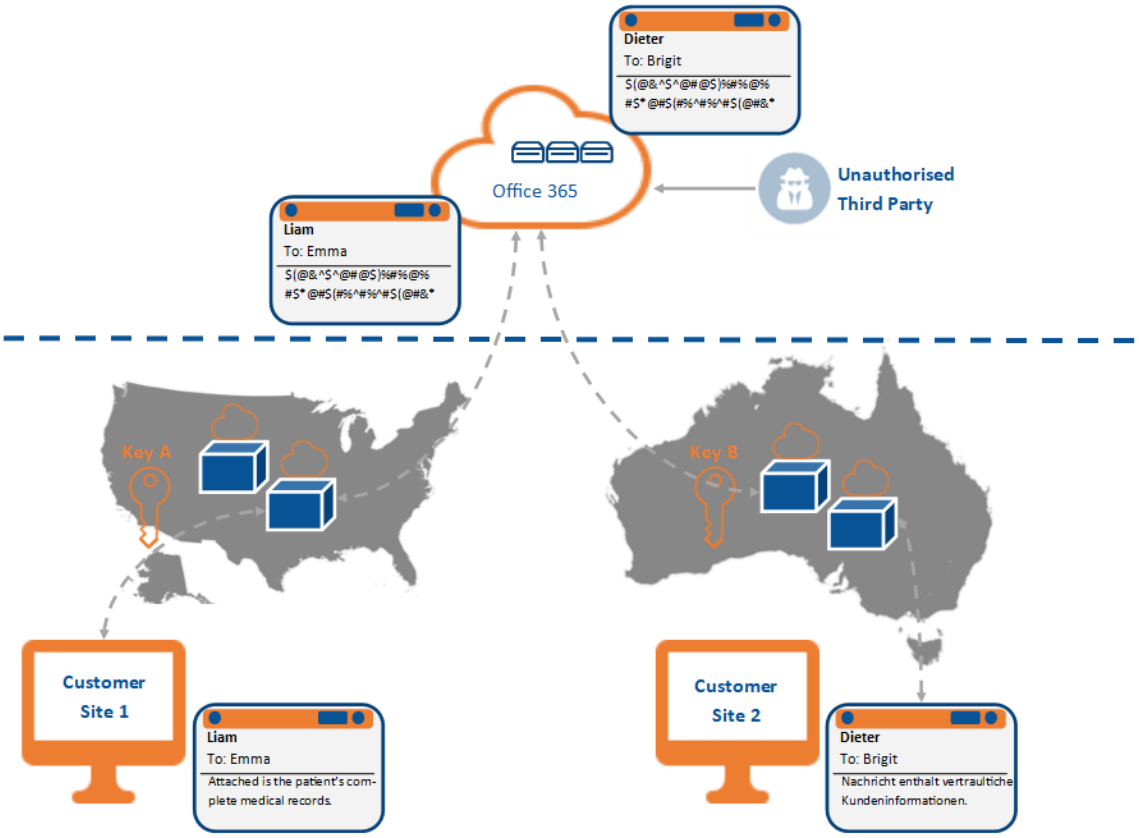
The data encryption gateway allows for key management of externally and internally hosted infrastructure and services. The Jellyfish service allows for a centralized management of encryption keys. Using a variety of encryption technologies, various forms of structured and unstructured data at rest can be encrypted. Access to the encryption keys and therefore the unencrypted data can be managed by administrators using a key management software. By deploying a Key Management service within the Cogito environment and encryptors within the client's environment we can offer the ability for clients to control access to their data without the need for them to purchase the FIPS 140-2 Level 2 and 3 platforms used by Cogito. This results in significant savings for the customer. Encryption Gateway Service shows how the service operates.



Encryption Gateway Service

[5] Support provided by the JF GEM and JF VOR coded modules

The Cogito Encryption Gateway not only provides the option for different keys for each tenancy, but can even provide different keys inside the same tenancy (see Encryption Gateway Multi-Key Option). This is particularly useful for a single organisation which may have offices across different jurisdictions. An example is where an organisation might have an office in the US and another in Europe. The different laws in the two jurisdictions require different levels of disclosure. Despite the company in this instance having the same domain names they can still have separate keys so that information for uses in the US for instance can still comply with a US Court ruling without compromising the information of the European users.



Encryption Gateway Multi-Key Option

In Service Encryption

File Protection [6]

Jellyfish's file protection module is a cloud agnostic solution that works across cloud providers (AWS, Microsoft Azure, IBM Bluemix (formally SoftLayer), VMware) to encrypt files, folders and shares. The Jellyfish file protection module secures: SQL and NoSQL databases, big data (Apache Hadoop) implementations, DAS, NAS and SAN storage and other solutions such as SharePoint, Gemstone, CHEF, Docker, and Office Tools

This service also supports on premises or hybrid cloud solutions.

Virtual Machine Protection [7]

This feature allows for the protection by encryption of whole or part of virtual machines. This solution also allows for access to the virtual machine to be control and can address many industry security standards when services are hosted in the cloud. This service supports cloud services such as Microsoft Azure and AWS.

This service can be provided as an on premises, cloud or hybrid solution.

DB Protection [8]

Jellyfish's DB protection module transparently encrypts data at the column-level in multi-vendor database management systems located on premise or in the cloud. Policy-based controls restrict column access to roles, users, and time of day - among other variables - to preserve finely tailed data ownership.

App Protection [9]

The Jellyfish app protection module encrypts application data as it is created and keeps it secure across its entire lifecycle on premise or in any cloud - no matter where it is transferred, backed up, or copied to.

[6] Support provided by the JF GEM, JF DMP and JF VOR coded modules
[7] Support provided by the JF GEM and JF VOR coded modules
[8] Support provided by the JF GEM and JF DMP coded modules
[9] Support provided by the JF GEM coded module

Identity and Access Management

Identity and access management (IAM) is a key component of a CASB offering. Identity is key in a borderless environment. Organisations expect users to be able to access services from anywhere, on any device and are moving security controls closer to applications and data. IAM is the security discipline that enables discrete control over the access of resources by individuals.

This is required to identify users and client applications wishing to access protected resources. This includes identity federation to enable authentication across different agencies. It also includes multi-factor authentication using certificates, one-time passwords and other methods, such as authentication of users on network connected devices as well as on mobile devices.

Access control of protected network resources utilises access policies that defines not just who can access the resource but also defines the actions that a user can perform on a resource, and also takes into account environmental conditions such as time of day and IP address range.

It can support interagency communication and secure sharing of infrastructure, applications and data.

Identity Provisioning & Deprovisioning [10]

Jellyfish IdAM provides an automated identity provisioning capability through the SCIM protocol to supported applications. This allows administrators to easily provision accounts to sanctioned cloud services which can reduce the likelihood of shadow-IT usage. This also reduces the amount of work required from consuming staff as part of on-boarding and retiring identities.

Single Sign On [11]

Jellyfish CASB Single Sign On (SSO) services allow the control of access to protected applications to authorised users only. The use of SSO also ensures that the user is known to the CASB service to ensure that user activity can be monitored for both compliance and reporting but to also ensure that the user activity is not outside their normal behaviour.

Jellyfish IdAM can provide single sign on capability to supported application providers. This is part of the Jellyfish CASB's secure configuration management capabilities and can reduce the risks that are introduced through the proliferation of passwords. This service is consumed when a user from a given organisation accesses a supported cloud service provider. The service provider then redirects the request to Jellyfish IdAM to provide authentication and authorization tokens for the given user. This process is transparent to the user. All authentication and authorization activities are logged in the SIEM and made available for

[10] Support provided by the JF MP coded module
[11] Support provided by the JF GLU coded module

correlation and analysis by security administrators in the Jellyfish Admin UI. Single sign on may also leverage smart cards in supported environments.

Threat Detection

Organisations consuming cloud services need to ensure that the data going to, and coming from the cloud services is not going to compromise their security. Performing traffic analysis on the data sent to and received from services can give an indication of compromise – either through knowing that a user is about to download malware, or through knowing that an infected machine is communicating out using cloud services. Jellyfish CASB offering can provide insight into the most at risk users, as well as prevent and quarantine threats for further analysis later.

It provides:

- Threat intelligence
- Malware identification
- Correlated activities analysis

Incident Response

Jellyfish CASB offer visibility over an organisation's interactions with cloud services. This increased visibility can be used to initiate incident response activities when cloud services are being misused. Minor incidents can often be responded to automatically through use of 'just in time education'. This means that when a user is about to perform an action that breaches the security policies of an organisation, the user can be blocked from completing the action and then informed that their actions are in breach of policy. Further follow up activities can then be completed – such as sending emails to the relevant authorities (managers, SOC staff, or higher authorities dependent on the significance of the event. Jellyfish CASB can also integrate with task management systems and create a workflow of actions to be completed after during an incident. Based on the analysis provided by analytics the components should be able to components raise alerts, incidents or perform automated actions.

Visibility

Analytics [12]

Data captured in the Jellyfish CASB service should be available for the service consumer to perform analysis on. Actions that are in breach of security policy need to be correlated to assess the scope of the problem at hand. Effectively for each single action, the Jellyfish CASB service s provides information on who performed an action, when the action was performed, where the action was performed, where the action took effect, and how the action was performed. These details need to provide enough context for the user to be able

[12] Support provided by the JF EL coded module

to discern why the action was performed. Individual actions should be able to be correlated using a dashboard. The CASB service should also provide less granular analytics, such as consumption of sanctioned IT versus consumption of non-sanctioned IT. The data stored must be retained for full auditability so that the consumer of the service can meet any compliance requirements. Furthermore, the Jellyfish CASB offering provides user behaviour analytics, which will help pinpoint which activities are anomalous.

Jellyfish CASB includes:

- User behaviour analytics.
- Risk analytics
- Consumption analytics
- Who, what, when, where, how' with enough data provided to discern why
- Auditability
- Dashboards (geolocation is a big pull)

Key requirements that are met by Jellyfish CASB include:

- UBA / UEBA analyse not only when the User is in control of an account but when an entity is
- Detect actions that are out of the ordinary for the user and act on that action. This needs to happen in (near) real time otherwise action is performed and then action to prevent it occurs.
- Consume event streams from SaaS apps, IaaS, and PaaS. This may mean a large storage requirement capability as the apps are unlikely to store event data like the creation of an account or storage of a file etc. indefinitely.
- Provide an API that allows access to administrative events to monitor key Applications.

Monitoring [13]

Most CASB providers look at Monitoring as a function of monitoring the activity of users. The Jellyfish CASB certainly sees this as a core function of the monitoring it provides, but goes past this to provide other monitoring services to allow for customers to determine other events in their cloud instances and even to their private cloud instance if available. Things like CPU usage, error warnings, and storage capacity issue can all be monitored. Our service can monitor a variety of operating systems, network devices and server hardware platforms.

[13] Support provided by the JF NAG and JF AV coded modules

Reporting [14]

In addition to monitoring Jellyfish allows for reports to be quickly generated on any of the core functions that it is providing. Reports on demand for usage, issues and errors are available within the Reporting capability. Even current billing can be found here. This reporting can support a number of SIEM like activities and services as well.

Log Storage [15]

The Cogito Jellyfish service also allows for the storage of logs gathered by other services. These logs can be shipped to the Jellyfish service, processed and actioned if required. The information provided in these logs can also be incorporated into reports generated by Jellyfish.

Configuration Management and Control

Through traffic analysis, it is possible to discern the configurations in use by various cloud services. This information can be leveraged to determine if the cloud services are being ran in compliance with the consuming organisation's security policies. Services which allow for API based configuration can use the Jellyfish CASB to automatically ensure that the cloud service configuration is compliant with policy, allowing for secure provisioning of new cloud services.

Policy Control

The Jellyfish CASB product provides functionality to allow the consuming organisation to translate their security policies into something that can be actioned by the other components. These policy rules can usually be expressed as a series of conditional statements – e.g. "if the user is in Marketing, and the device is her BYOD device, do not grant access to sensitive financial resources". Each component in a CASB offering should have a set of configurable policy items associated with it.

This involves access to a risk registry; defining and enforcing policy; and stream processing tools that extract data. This allows an organisation not only to detect threats but act on them immediately, raising real-time or near real time notifications.

Jellyfish Admin UI

Jellyfish Admin-UI provides a frontend to the underlying products in the CASB offering and is the primary interface that administrators of the CASB use and it provides visibility and control over these components. The Jellyfish Admin UI provides full configuration of proxy services, and provides reporting and usage information for all Cogito CASB components.

[14] Support provided by the JF EL coded module
[15] Support provided by the JF EL coded module

About Cogito Group

Cogito Group is an award winning Australian owned and operated ICT company that specialise 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.

Canberra Office
t +61 2 6140 4494
w www.cogitogroup.com.au

Wellington Office
t +64 4909 7580
w www.cogitogroup.co.nz

Cogito Group