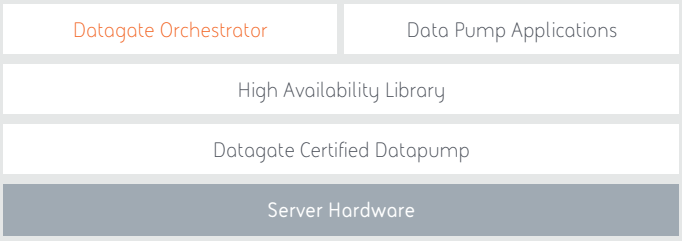
BAE SYSTEMS

Cross Domain Solutions Datagate Orchestrator

Unrivalled Security

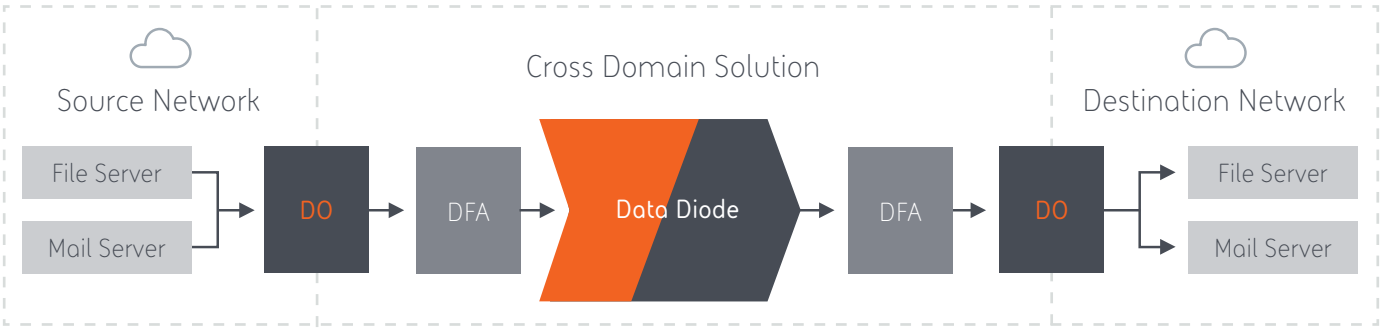
What is the Datagate Orchestrator?

Datagate Orchestrator (DO) is a platform for the management of data passing into and out of a network, providing an information assurance decision making framework. A risk assessment engine performs analysis on data using a suite of content filters, while a data routing engine ensures that only the data that meets the configured set of rules is allowed to pass into the destination network. The flexible workflow system and wide variety of input and output interfaces allows DO to securely connect a Cross Domain Solution to the rest of the enterprise.



How does it work?

A flexible drag-and-drop web interface allows the configuration of workflows which define the checks to be performed, and the actions that occur as a result of these checks. Data that does not meet the defined rules can be stored in quarantine for later review by an administrator. All movement of data is thoroughly audited, and notifications can be configured for a range of important events.



Key features

- Contains over 25 built-in filters to perform content analysis (dirty word, MIME type, XML schema validation, etc), XML sanitisation, XML digital signing, virus scanning and metadata checks (web and email domains, file size)
- A Java API allows the development of new content filters, and integration with existing third party content filters.
- A powerful content extraction engine ensures that all of the contents of a transfer are analysed, including nested content such as ZIP files and office document attachments.
- Can be used to enforce a manual review and release of data, in addition to the automatic data routing capabilities, using a quarantine management system that allows reviewers to inspect suspicious files.

Technical Specifications

Data Input / Output Interfaces	– File – Supports local filesystem and network shares (XFS, EXT4, NFS, CIFS, SFTP) – Email – SMTP with TLS support (RFC 821, RFC 3207) – Web – ICAP (RFC 3507)
Supported Anti-Virus Products*	– Sophos – McAfee – ClamAV
XML Validation	XSD, DTD, ISO Schematron
Configuration	Web interface (with drag-and-drop workflow configuration)
Authentication and Security	– Role-based access control to web interface (RBAC) – Two-person integrity – LDAP integration
Auditing and Monitoring	– Web interface – Custom report generation – Email notifications – Log files – Syslog – SNMP traps (v1 & v3)
Minimum Hardware	– 8-Core 2.9GHz – 32GB RAM – Additional hardware required if installed as part of a BAE Systems CDS
Operating Systems	Red Hat Enterprise Linux 6 and 7

* Third party anti-virus products must be purchased and/or installed separately

For more information contact:
BAE Systems Australia

T: +61 (8) 8480 7799
E: au.ilsales@baesystems.com
W: cds.au.baesystems.com

2486DT00162 Rev A