

Datagate Orchestrator

Unrivalled Security

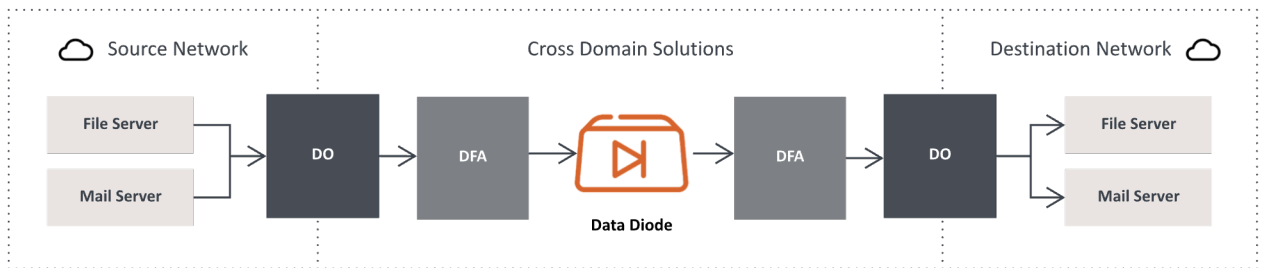
What is the Datagate Orchestrator?

Datagate Orchestrator (DO) is a platform for the management of data passing into and out of a network. 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 transformation (DFDL), sanitisation (XML, PuriFile), content analysis (dirty word, MIME type, XML schema validation), 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 3rd 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. A quarantine management system provides a mechanism for reviewers to inspect suspicious files.
- Can be clustered with additional DO nodes to provide a single logical audit and quarantine view for a cluster.

Technical Specifications

Data Input / Output Interfaces	File – Supports local filesystem and network shares (XFS, EXT4, NFS, CIFS) Email – SMTP with TLS support SFTP – support for certificate and user authentication Streaming – TCP (with TLS) and UDP Web – ICAP
Transformation	Daffodil
Sanitisation	XML, PuriFile
Anti-Virus Products*	Sophos, McAfee, ClamAV
Third Party Filters*	PuriFile, NiFi
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 & Monitoring	Web interface, Custom report generation, Email notifications, Log files, Syslog, SNMP traps (v1 & v3), Clustered audit
Minimum Hardware	8-Core 2.9GHz 32GB RAM
Operating Systems	Red Hat Enterprise Linux 7 and 8

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

For more information contact:

Web: cds.au.baesystems.com
Email: au.ilsales@baesystems.com
Telephone: +61 8 8480 7799.

2486DT00162 Rev B

This document gives only a general description of the product(s) or service(s). It shall not form part of any contract. From time to time, changes may be made in the products or the conditions of supply.

©BAE Systems 2024 all rights reserved. Permission to reproduce any part of this document should be sought from BAE Systems. Permission will usually be given provided that the source is acknowledged and the copyright notice and this notice are reproduced.

BAE SYSTEMS