BAE SYSTEMS

Cross Domain Solutions Datagate Orchestrator

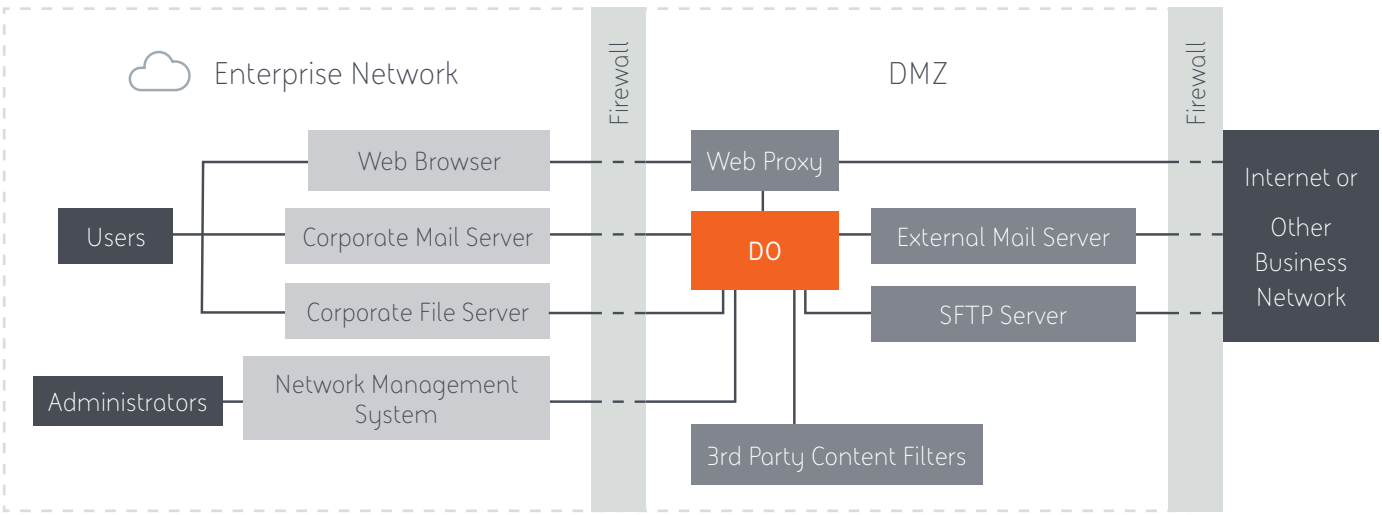
Unrivalled Security

What is a Datagate Orchestrator?

Datagate Orchestrator (DO) is a platform for managing the data passing into and out of a network. It acts as a gateway between the enterprise and other networks, such as the internet or another business 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 through the gateway. In addition to providing a wide range of built-in filters, DO integrates with third party content filters and anti-virus software. The flexible workflow system and wide variety of input and output interfaces allows DO to protect an enterprise network from the ingress of security threats, and the egress of sensitive information.

How does it work?

DO can be configured as an incoming and outgoing filter for file, email and web traffic. Data is routed to DO via enterprise network services such as SFTP, mail, and web proxies. DO applies a set of rules that are configured via an intuitive drag-and-drop workflow configuration interface. Notifications can be sent to users and / or administrators whenever traffic is blocked, and a rich auditing system provides details of the paths that data has taken through the network.



Key features

- Contains over 25 built-in filters to perform content analysis (dirty word, MIME type, XML schema validation, etc.), 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 data.

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
Supported Third Party Filters*	– PuriFile – Daffodil
XML Validation	XSD, DTD, ISO Schematron
Configuration	Web interface (with drag-and-drop workflow configuration)
Authentication & 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)
Minimum Hardware	– 8-Core 2.9GHz – 32GB RAM
Operating Systems	Red Hat Enterprise Linux 6 and 7

* Third party filters and 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