FORTRA

WHITE PAPER (FORTRA DLP)

Forcepoint DLP Migration Services

Best in class data visibility, analytics, & controls in 90 days

Purpose

Our Customer Success team will partner with your organization to ensure a smooth transition from your existing Forcepoint DLP solution to Fortra DLP. Whether you are deploying our on-premises, software as a service, or managed service, our team will map your data protection and business goals to Fortra's data protection solutions. This document provides a description of the standard migration services, though customization, as required, is available.

Fortra DLP Migration Service Overview

Fortra has successfully helped both enterprise and midmarket customers transition from Forcepoint using our proven migration methodology.

Phase 1 – Transition Planning. Fortra's Customer Success team will walk you through the transition plan, milestones, and key objectives in preparation for your transition.

Phase 2 – Environment Build. Depending on your configuration (SaaS, Managed Service, or On-Premises) Fortra will provision the DLP Management Console and its Analytics & Reporting Cloud (ARC) for your deployment. If you're scope includes a network DLP solution, we will provision the desired appliances (physical machine, virtual machine, or container image) for your environment.

Phase 3 – Agent Qualification Pilot. For endpoint DLP environments, Fortra will build and test agent deployment packages for each operating system in scope and work with your desktop team to verify compatibility within your standard operating environment. Before uninstalling Forcepoint and installing the Fortra DLP agent, our software's script will be tested within your environment to ensure correct execution. Typically, Fortra DLP will then be deployed to your machines via your software deployment solutions, such as a SCCM, beginning with a pilot deployment to selected test users (25-50 endpoints).

Phase 4 – DLP Policies & Alerting-Reporting Configuration. Your Customer Success Representative will configure your Fortra DLP Policy Pack, alerts, reports, and dashboards in ARC. If custom policies are required, they will review and create those in Phase 4 as well.

Endpoint DLP use cases may include:

- **Classification-Based Policies:** Leverage classification labels applied to your sensitive data and intellectual property to enforce data protection policies and facilitate compliance.
- **Content-Based Policies:** Leverage pattern matching, keyword identification, and other identifiers found within files and documents to control data egress based on organizational data protection policies.
- **Context-Based Policies:** Leverage metedata embedded in your sensitive information to enforce data protection policies and control data egress. Such context includes:
  - **Location:** Where information is stored, including pre-defined file servers, file shares, GIT repositories, and more.
  - **Data Source:** Where the information was originally created (e.g., within defined desktop applications) or downloaded (pre-defined websites vs. unsanctioned sites).
  - **Data Types:** Enforce the appropriate data protection policies for different data types, from Office files, to AutoCAD files, HR files, and more.
- **User-based Policies:** Govern user actions and control data egress, covering a variety of channels.
  - **Email to external or webmail domains:** Control emails to unauthorized external or personal webmail domains via Outlook.
  - **File share applications:** Control egress of any file being uploaded via common cloud storage applications installed on the machines e.g. Dropbox, Google Drive, 360cloud, SkyDrive etc.
  - **Outlook data file:** Control egress of Outlook data files (.pst & .ost) that contain large amounts of sensitive data.
  - **Removable storage:** Control egress of any file to removable storage devices e.g. USB stick, external HDD, optical media.
  - **Removable media encryption:** Encrypt all files written to USB device with enterprise-level encryption.
  - **USB mount restrictions:** Block mount of all USB devices, except if authorized (whitelisted).
  - **Uploads:** Control egress of any file being uploaded to unauthorized sites via a web browser (including file share sites, webmail domains, or other sites).

- **Printing:** Control egress to printers, except if authorized (whitelisted).
- **Mass files egress:** Alert if upload/removable egress has crossed a threshold in a given amount of time.

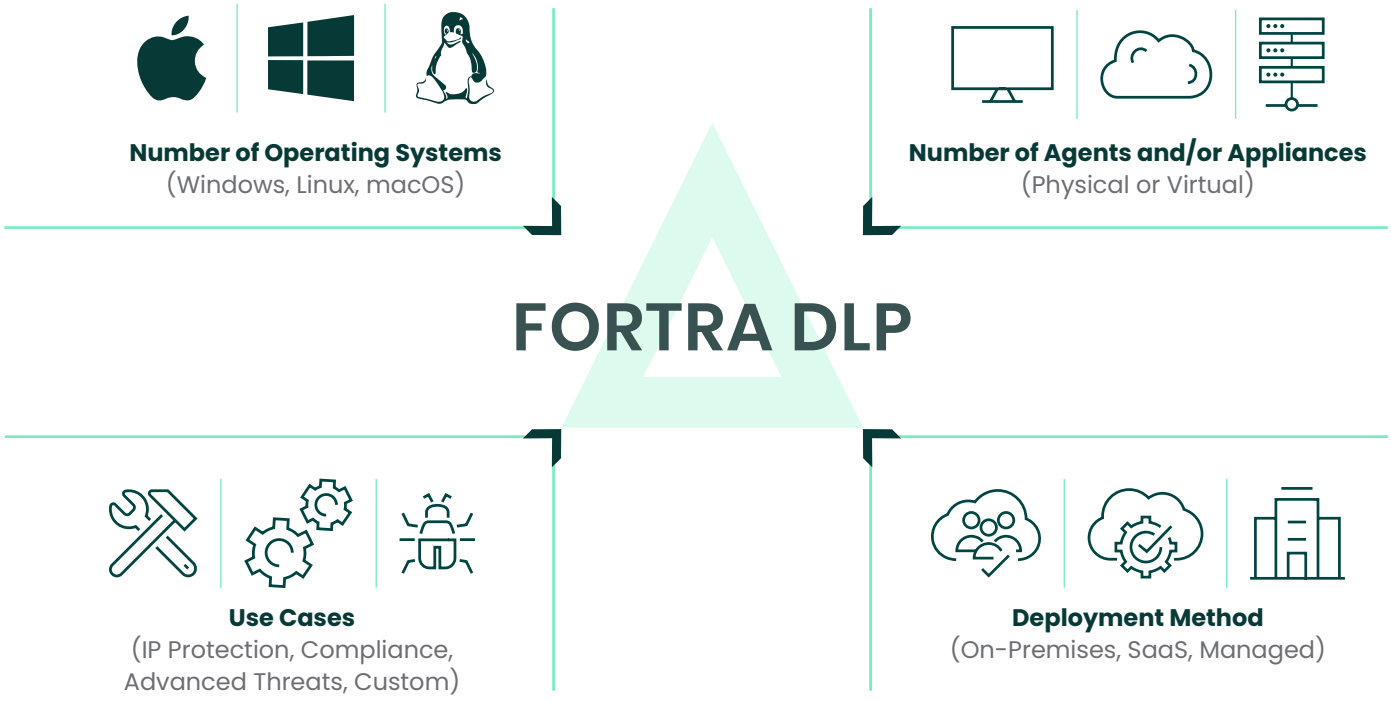
Network DLP use cases may include:

- **Email traffic:** Inspect and control outbound email traffic, including the message header, body content, and attachments.
- **Web traffic:** Inspect and control HTTP, HTTPS, and FTP traffic for sensitive data.
- **Data at rest server discovery:** Discover and remediate data in network file shares, databases, and repositories.
- **Cloud data protection:** Inspect cloud storage providers, including Accellion, Box, Citrix ShareFile, OneDrive, SharePoint and Egnyte, allowing for removal or other remediation of sensitive data.

Phase 5 – Production Deployment. A phased deployment plan will be executed on your production machines, replacing your existing Forcepoint DLP solution with Fortra DLP and minimizing downtime during the transition. Fortra will closely monitor your deployment for any issues and validate correct functioning of alerting/reporting mechanisms.

Our team will support Forcepoint workflow integrations as part of your customized migration program, ensuring support processes and knowledge transfer are complete before adopting Fortra DLP.

After cutover to full production, whethere on-premises, SaaS, or managed service, the Fortra Customer Success team can provide the support and security expertise required for a successful DLP program. Speak with your account representative to discuss optimal support options for your organizational needs.



FORTRA

Fortra.com