FORTRA™

WHITE PAPER (DIGITAL GUARDIAN)

Forcepoint DLP Migration Services

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

Purpose

The Fortra™'s Digital Guardian® Customer Success team will partner with your organization to ensure a smooth transition from your existing Forcepoint DLP solution to Digital Guardian. 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 Digital Guardian's data protection solutions. This document provides a description of the standard migration services, though customization, as required, is available.

Digital Guardian Migration Service Overview

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

Phase 1 – Transition Planning. Your DG 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) DG will provision the Digital Guardian Management Console (DGMC) and its Analytics & Reporting Cloud (ARC) for your deployment. If you're scope includes a network DLP solution, we will provision DG appliances (physical or virtual) for your environment.

Phase 3 – Agent Qualification Pilot. For endpoint DLP environments, DG 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. DG will test its script to uninstall Forcepoint and install the DG agent; typically, this will be deployed to your machines via your software deployment solutions, such as SCCM. A pilot deployment to selected test users (25-50 endpoints) will also be performed.

Phase 4 – DLP Policies & Alerting-Reporting Configuration. Your Customer Success Representative will configure the DG 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 Policies** identify and tag your sensitive data and intellectual property
  - **Content-Based Policies:** Classify (tag) and control egress of files based on content. Content patterns identify keywords or alphanumeric patterns in files. Files are classified either during file operations based on properties defined in classification rules, or by the DG Scanner when it performs scans of files on drives.
    - **PCI data**
    - **PII data**
    - **PHI data**
    - **ITAR data**
  - **Context-Based Policies:** Classify (tag) and control egress of files based on context.
    - **Sensitive file shares:** All data located in pre-defined file servers and shared on the internal network can be tagged.
    - **Sensitive websites:** Files downloaded from pre-defined websites (or browser-based applications) can be tagged.
    - **Source code repositories:** Source code stored within predefined repositories, such as GIT, can be tagged.
    - **Sensitive file types:** Data generated by specific desktop applications, such as AutoCAD, can be tagged
- **Control 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.

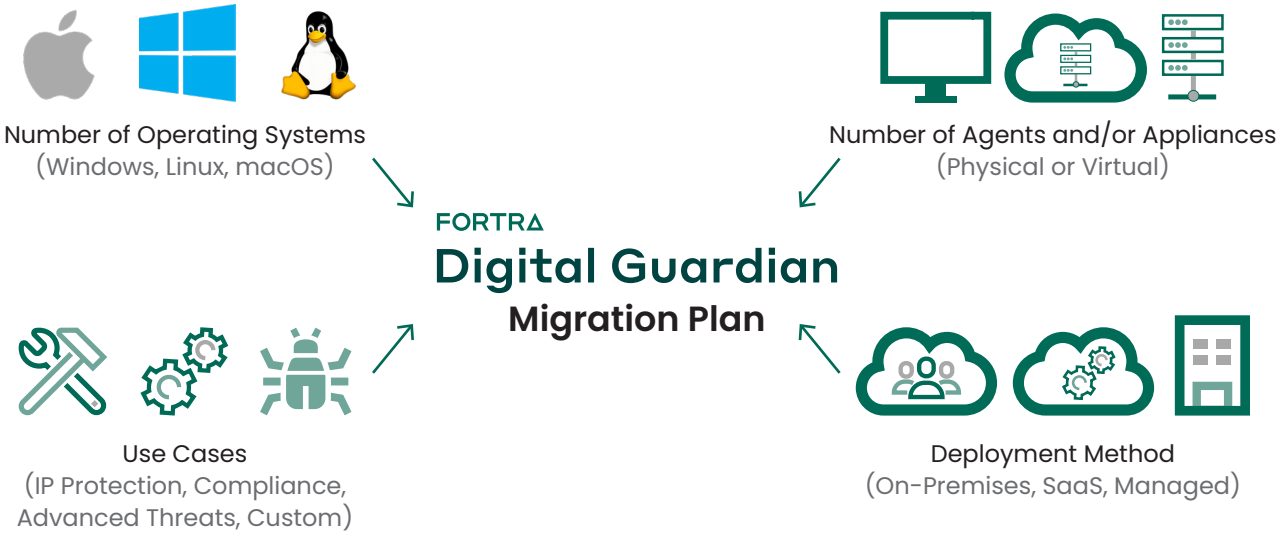
Network DLP use cases may include:

- **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 Digital Guardian and minimizing downtime during the transition. DG 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 the customized migration program (extra charges may apply). DG will work with your team to ensure that support processes and knowledge transfer are complete before you adopt the solution.

After cutover to full production, whethere on-premises, SaaS, or managed service, the DG 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

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

© Fortra, LLC and its group of companies. All trademarks and registered trademarks are the property of their respective owners.