FORTRA™

SOLUTION BRIEF (DIGITAL GUARDIAN)

Moving from Forcepoint DLP?

It’s Never Been Easier.

Reduce Vendor Uncertainty. Increase Data Protection Coverage.

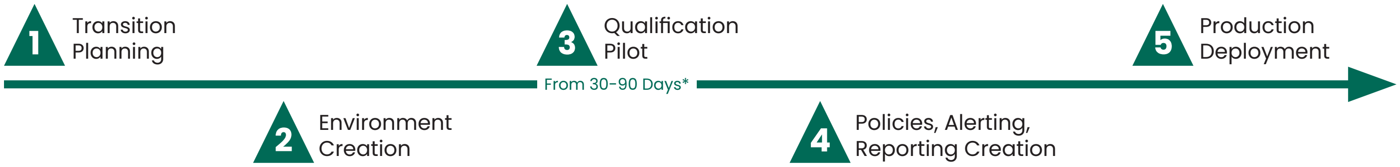
With the pending sale of Forcepoint to the private equity firm Francisco Partners, Forcepoint customers may be evaluating DLP alternatives to de-risk their data protection program. If you are one of those customers, Fortra™’s Digital Guardian®’s has created a special offer to help you make a streamlined transition to our enterprise endpoint and/or network DLP. This program can reduce your vendor risk, increase your data protection coverage, and cut your DLP overhead.

Why Choose Digital Guardian over Forcepoint?

Capabilities	Digital Guardian	Forcepoint	Business Value
Broadest Endpoint OS Coverage	▲	△	Organizations rely on multiple operating systems to give their employees the right tool for the job. Only Digital Guardian delivers endpoint DLP to protect data on Windows, macOS, and Linux endpoints.
Persistent Protection	▲	▲	Only Digital Guardian can automatically tag sensitive files based on content inspection or contextual analysis. These persistent tags resist any attempts to bypass DLP via archiving, file extension change, or encryption and are inherited with the content into new documents.
Optimized Policies	▲	▲	When migrating to a new platform, inheriting existing policies blindly may perpetuate existing gaps. With Digital Guardian you can deploy without a policy and watch how sensitive data is being accessed and used within your organization. With this insight you can create new and better policies.
Focus and Responsiveness	▲	▲	Digital Guardian is the only Gartner Magic Quadrant enterprise DLP leader that is 100% focused on data protection. Our entire organization is built around protecting your data and our support team is there when you need them with 24x7 coverage and rapid response.
Security Orchestration and Integration	▲	▲	Unlike Forcepoint, Digital Guardian uses industry standard RESTful APIs to enable you to share deep insights into how sensitive data is being used and how it moves with your SIEM and SOAR tools. You can automate and streamline workflows to simplify security operations.
DLP Program as a Service	▲	▲	Digital Guardian is the only software company that offers a managed service directly. This eliminates finger-pointing between the technology vendor and the managed service provider.

Proven Migration Methodology

Digital Guardian has transitioned both Fortune 50 and midmarket companies from Forcepoint endpoint and network DLP using our proven migration methodology.



1 Transition Planning

2 Environment Creation

3 Qualification Pilot

From 30-90 Days*

4 Policies, Alerting, Reporting Creation

5 Production Deployment

Here is an overview of the migration process for a cloud-based SaaS deployment.

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 Creation. DG will provision its cloud hosted Digital Guardian Management Console (DGMC) and its Analytics & Reporting Cloud (ARC) tenant for your deployment. If you're scope includes a network DLP solution, we will provision DG appliances for your environment.

Phase 3: Qualification Pilot. 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 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.

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.

*Migration timelines vary based on policies, operating systems, etc. An environment with one operating system (i.e. Windows) that leverages only the DG standard DLP policy pack can be migrated in 30 days, while environments with multiple operating systems and custom policies may take up to 90 days to migrate. Any additional custom policies will be subject to additional charge – review these with your DG account manager.

The Time to Switch is Now

Contact us or a certified Digital Guardian partner today to get expert guidance and a demo on switching from Forcepoint. Our Customer Success team can scope your migration and ensure a smooth transition to Digital Guardian Enterprise DLP.

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.