FORTRA™

SOLUTION BRIEF (DIGITAL GUARDIAN)

Switch from Symantec DLP

It's Never Been Easier.

Reduce Vendor Uncertainty. Increase Data Protection Coverage.

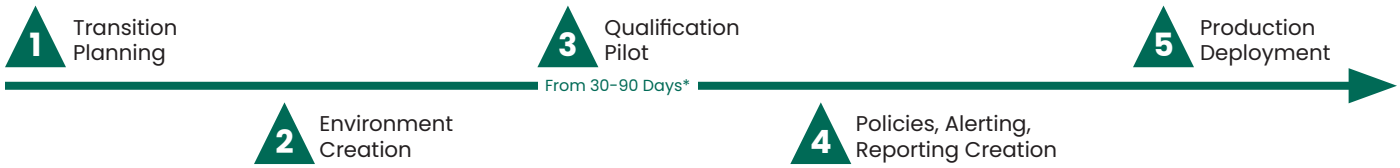
With the pending sale of Symantec Enterprise assets to Broadcom, many Symantec DLP customers have been informed that the company will not renew their contracts. If you are one of those customers, or if you want to de-risk your data protection program, Fortra™'s Digital Guardian® has created a special offer to help you make a streamlined transition to our Enterprise Network and/ or Endpoint DLP. This program can reduce your vendor risk, increase your data protection coverage, and cut your DLP overhead.

Why Choose Digital Guardian over Symantec?

Capability	Digital Guardian	Symantec	Business Value
Superior IP Protection	▲	△	Ranked #1 for intellectual property protection in the latest Gartner Critical Capabilities for Enterprise DLP report.
Deepest Data Visibility	▲	△	Our agent delivers the deepest visibility into system, user, and data-level events. We see what no one else can to protect your sensitive data.
Broadest Endpoint OS Coverage	▲	△ (no Linux support)	Digital Guardian provides endpoint protection across Windows, macOS, and Linux endpoints.
Responsiveness	▲	△	Digital Guardian is the only Gartner Magic Quadrant Enterprise DLP Leader that is focused on data protection. That translates into greater responsiveness to your data protection needs.
Migrate to Cloud DLP for Additional Advantages			
SaaS Delivery Option	▲	▲	Our exclusive DLP SaaS subscription includes everything you need to succeed. This cuts costs and eliminates the complexity of updating and maintaining on-premises DLP server infrastructure.
Digital Guardian-Delivered Managed DLP Option	▲	▲	Digital Guardian is the only company that offers a managed service directly. This eliminates fingerpointing between the technology vendor and the managed service provider.

Proven Migration Methodology

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



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 Symantec 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 Symantec 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 Symantec 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 Symantec. 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.