FORTRA

DATASHEET *(Digital Guardian)*

Digital Guardian Software as a Service (SaaS)

Increase Data Protection | Reduce Overhead, Friction & Cost

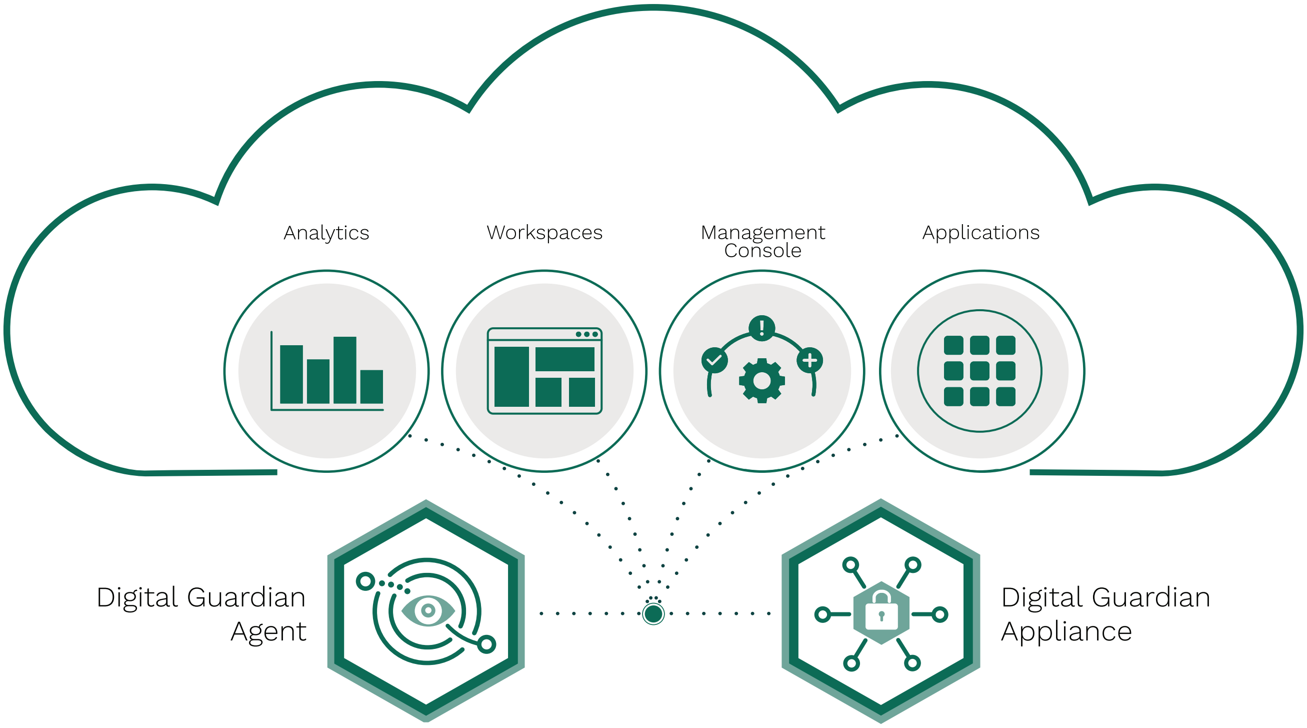
Digital Guardian's purpose-built SaaS infrastructure enables you and your team to focus more time, energy, and resources on identifying and mitigating risks to your sensitive data and less time on acquiring, building and maintaining the infrastructure.

The Digital Guardian Data Protection Platform is now available as a service that leverages a scalable cloud architecture which provides the ability to aggregate, analyze and query massive data sets from the network sensor and endpoint agent events in real-time. This new cloud architecture was built with the latest tools and methodologies to provide the scalability, data visualization and ease-of-use security analysts have come to expect from software as a service. The service delivers workspaces and workflows tailored for the unique needs of CISOs, InfoSec Analysts, Incident Responders and Threat Hunters.

Benefits of Digital Guardian SaaS

- **Cut Costs and Maintenance Cycles.** Digital Guardian hosts and manages a big data security architecture for you. You cut costs and the complexity of patching, updating and maintaining on premise hardware and software.
- **Immediate Time to Value.** No hardware, additional software or configuration required.
- **Scalability.** Our service takes advantage of the scalability of the cloud. We can scale up to meet your demand and provide sufficient storage and compute power to drive world class data protection at lower cost.

Cloud-Delivered Data Protection



What You Get

Infrastructure
Provision and support for all back-end infrastructure and software systems required to run the DG solution.

Infrastructure & Application Monitoring
Monitoring for the Digital Guardian Management Console (DGMC), Reporting & Analytics user interface and Network DLP cloud hosted infrastructure.

Environment Monitoring
Regular monitoring, auditing and testing of the environment for vulnerabilities.

Environment Access
Full "System Administrator" level access to the DGMC and Analytics user interface within the boundaries of these applications.

Backups
Backup and resiliency for cloud hosted components including DG event bundles.

Upgrades
Backend system upgrade tasks of the cloud hosted infrastructure.*

Content Packs
Access to standard content packs for DLP use cases.

Agent Installation Files
An initial installation package for SaaS deployment environments.

SIEM Integration
DG Server connectivity setup and configuration for data exports to customer SIEM for all supported platforms.**

Bundle Playback
Set-up of ARC tenants for playback purposes and investigations for eDiscovery.

VPN
Connectivity between the client and the DG cloud to ensure secure communication.

Penetration Testing
Regular scheduled penetration testing for compliance and security purposes.

Audit Compliance
All SSAE 16 and other certifications will be maintained by the DG support team.

Operations
Ticketing and CRM system for issue and change control tracking.

Support
Ticketing system for issues, reporting and tracking, as well as access to knowledge base and general training.

*Updates occur as a normal business practice, and scheduling of updates happens routinely.

**DG will not be responsible for configuration activities on the customer SIEM required for data processing. Refer to the Digital Guardian Website for a list of supported SIEMs.

SaaS Setup Services

DG has built three predefined SaaS Setup Services to enable the implementation of the DG SaaS environment. Setup Services are based on a variety of factors, but primarily are defined by the size (number of agents), scope of deployment (target systems, use cases, operating systems, etc.) and project deployment timelines.

Optional Add-On Services

1. **Ongoing Professional Services** – Help you deploy faster, reduce data security risks and get the most out of your DG SaaS implementation. Our expert security teams deliver comprehensive, enterprise-wide security assessment, design, and deployment services to help you build effective data-security programs.

2. **Virtualization / Citrix Use Case Support / Virtual Desktop Infrastructure** – This use case requires an additional setup fee due to the increased complexity of the environment. Operating costs for managing multiple virtual environments will be subsumed by the Managed Service.

3. **Custom Data Extracts** – Customers requesting custom data extracts / custom reporting outside of DG that require additional configuration and data storage/bandwidth will require a custom sizing and set-up fee to be added, due to the extra infrastructure requirements and time to setup.

4. **Additional Servers / Additional Storage / Server Agents / Development Environments** – Customers that require more environments than our standard production and/or require data separation from a data privacy perspective or Server Agent storage requirement will need to be sized and priced accodingly.

5. **Technical Account Management (TAM)** – A dedicated resource and customer contact within DG's Customer Support Organization who understands the client's environment and provides priority support for any technical issues. This offering is generally consumed with large deployments (10k seats and up).*

6. **iDP SAML Integration** - iDP SAML integration for self service provisioning via customer iDP.

*Please see the TAM Offering Document for more information.

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.