PRODUCT DATA SHEET

DIGITALGUARDIAN®
Add-On Modules

ENHANCE AND EXTEND YOUR DATA PROTECTION

Digital Guardian offers a suite of add-on modules that provide advanced encryption, extend your protection to the network and more.

ADAPTIVE FILE ENCRYPTION MODULE

The Adaptive File Encryption (AFE) Module, extends Digital Guardian's comprehensive monitoring and control polices to perform automated and transparent file encryption. The Digital Guardian AFE module uses patented data encryption and enterprise key management technology to flexibly apply encryption to protect content on local drives or file shares.

This module provides:

- Policy-based automated file encryption using AES-256 encryption.
- Encryption protection for data stored on local disks, network addressable storage (NAS) and Server storage.
- Centralized key management architecture with full file recovery capabilities.
- Visibility, auditing and reporting to understand what data is encrypted when a system or device is lost or stolen.

INVESTIGATION MODULE

The Investigative Module extends Digital Guardian's data event recording capabilities to include advanced evidence like screen capture images, file content and key logs. The additional forensic information captured by the Investigation Module is then preserved and correlated with other event metadata and Alerts logged by endpoint agents to provide investigators with greater incident context and guide them quickly to artifacts of highest interest.

The Investigative Module, configured in the Digital Guardian Management Console can be deployed for a specific individual or group of individuals whom an organization is actively investigating. The module allows investigators to record additional evidence and securely retain a complete series of activities on a user's system before, during and after incidents or events of interest occur.

Policies are user-aware so any physical or virtual machine where the module is operational will "know" to begin recording activities as necessary when a specified employee logs in, eliminating any risk of lost evidence if multiple machines are used to perform actions against policy.

ADAPTIVE MAIL ENCRYPTION MODULE

The Adaptive Mail Encryption (AME) module extends Digital Guardian's comprehensive mail monitoring and control polices to perform on the fly, automated email encryption. Our patented, automated key management greatly simplifies system management.

This module provides:

- Policy-based automated enforcement avoiding the requirement that employees remember to apply encryption.
- Support for Microsoft® Outlook/Exchange and Lotus® Notes/Domino protecting content and attachments with AES-256 encryption.
- WinZip and DG password based collaborative encryption designed to support mobile, joint venture, outsourcing and other partner related work environments.
- Centralized visibility, auditing and reporting enabling you to understand what encrypted data moved in emails and as attachments.

MEMORY FORENSICS MODULE

The Memory Forensics Module extends the advanced threats defense capabilities of the DG agent by analyzing code in memory to reveal malware, risky applications, and other advanced threats.

This module:

- Forensically scans a snapshot of endpoint memory and uses Digital DNA® to rate threat severity of executable code in memory - without relying on signatures.
- Provides actionable alerts and points directly to the implicated processes.
- Enables forensics based investigation of anomalous behavior detected by the DG core agent.
- Assigns a machine risk score that can be used by the DG agent to enforce adaptive rules.
- Memory evidence can be preserved and retrieved via the DG Management Console.

DIGITALGUARDIAN® by VERDASYS

For more information, visit
www.digitalguardian.com

NETWORK AGENTS MODULE

Digital Guardian Network Agents complement endpoint agents to provide multiple layers of real-time data protection. The Network Agent Module architecture consists of specialized sensors that log and manage data use for internal, SMTP, ICAP enabled proxy, and inbound or outbound traffic.

Using a patented Deep Session Inspection™ technology, Network Agents deconstruct, analyze, and control network sessions by policy across all network ports and protocols in near real-time. They capture packets for reassembly into sessions, and then deconstruct payloads for analysis by ten separate content analysis technologies to identify sensitive information. Deep Session Inspection detects and stops data theft by insiders and external threats with real-time policy management derived from file- and session-level forensics across inbound and outbound network traffic.

When Digital Guardian detects a policy violation, network agents can drop the session or inject resets to prevent data from leaving the network. DG Network Agents are the only network DLP solution proven to prevent data loss across all ports and protocols without slowing multi-gigabit network traffic.

This module enables you to:

- Control both proxied and direct to internet traffic.
- Inspect all network traffic for sensitive content (including attachments and compressed files).
- Stop unauthorized traffic based on content, application, and protocol.
- Quarantine sensitive or unencrypted emails before they leave the network.
- Monitor all channels including email, Web, Webmail, instant messaging, file transfers.

USER DRIVEN CLASSIFICATION MODULE

Digital Guardian's User Classification (UC) module complements DG's automated data classification methods by allowing users to classify data manually. Empowering data owners to accurately identify their sensitive data can deliver a more effective approach to classifying data than using automated methods alone.

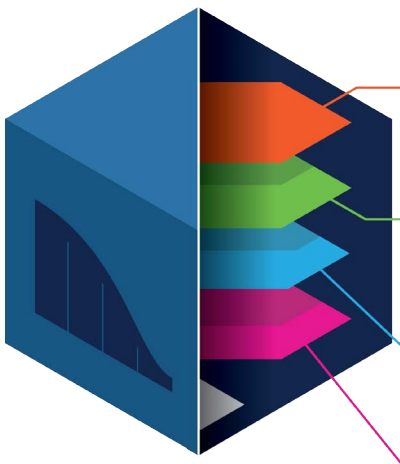
Digital Guardian policies can enhance UC-driven classification by offering real-time prompts to check and train users to identify data correctly. Combining content, context, and user-enabled classification rules allows an agent's automated assessment to check a user's manual assessment to resolve conflicting tags for reporting and policy enforcement.

DIGITIAL GUARDIAN PRODUCT PLATFORM

Digital Guardian is the only data-centric security platform designed to stop data theft.

DGMC
Digital Guardian Management Console

Your web-based command center. Deploy Agents, create and manage policies, alerts and reports.



Advanced Threat Protection
Advanced threat detection, incident response and prevention that ensures security travels with the data.

Data Loss Prevention
Everything you need to stop sensitive data from getting out of your organization.

Data Visibility & Control
Out-of-the-box data visibility and device control.

DG Agent
The only endpoint agent compatible with Windows, Mac & Linux.

ABOUT DIGITAL GUARDIAN

Digital Guardian is the only data-centric security platform designed to stop data theft. The Digital Guardian platform performs across traditional endpoints, mobile devices and cloud applications to make it easier to see and stop all threats to sensitive data. For more than 10 years we've enabled data-rich organizations to protect their most valuable assets with an on premise deployment or an outsourced managed security program (MSP). Our unique data awareness and transformative endpoint visibility, combined with behavioral threat detection and response, let you protect data without slowing the pace of your business.

SHARE