SOLUTION SHEET

DIGITAL GUARDIAN®

Managed Security Program Deliverables for Network DLP

Program Overview

Digital Guardian Network DLP helps support compliance and reduce risks of data loss by monitoring and controlling the flow of sensitive data via the network, email or web. Our network DLP appliances inspect all network traffic then enforce policies to ensure protection. Policy actions include: allow, prompt, block, encrypt, reroute, and quarantine.

Our Managed Security Program security analysts are experienced professionals with the ability to sift through mounds of log data and identify when your most sensitive assets are at risk. We provide the people, process and technology behind your data protection program so that you can focus on other important initiatives. Let us be the "Eyes on Glass" and provide timely insight and alerting into anomalous and suspicious end user behavior.

What You Get

Security Experts Continuously Hunting For Insider Threats

- A dedicated security analyst is assigned to your account for custom requests and questions
- An entire analyst team is continuously hunting through your logs to identify any signs of potential insider threats

Fully Managed Data Security Compliance Infrastructure

- Appliance installation and ongoing administration
- Active Directory and SIEM integration
- Software upgrades

Ongoing Protection

- **Optimized PII & PHI Protection:**
  - Continuous PII & PHI data discovery, classification and monitoring
- **Alerting & Incident Escalation:**
  - Our team of experts watch for events that put your data at risk and take action
- **Ongoing Improvement Of Your Security Posture:**
  - Monthly expert risk analysis will assess, iterate and improve your data protection policies and procedures

Fast & Flexible Deployment

- With our industry first Managed Security Program for DLP, you can offload the configuration, management and analysis to Digital Guardian experts
- We identify high-risk events and provide detailed reporting to better gauge effectiveness of your program and/or help demonstrate compliance

Highest Accuracy

- Digital Guardian's Database Record Matching (DBRM) delivers the accuracy needed to reduce false positives and false negatives
- BRM recognizes, registers and protects a wide range of both structured e.g. fields in databases or columns in spreadsheets) and unstructured data types (e.g. document formats such as Microsoft Office, source code and PDFs)

Proven, Insight-Driven Framework

- Our unique ability to protect data from both insider and outsider threats is a result of three distinct capabilities:
  - **Deepest Visibility:** DG sees and correlates system, user and data events in real time
  - **Real-Time Analytics:** DG filters out the noise allowing InfoSec to focus on real threats
  - **Flexible Controls:** DG acts at machine speed with controls that adapt to your business

Demonstrate Regulatory Compliance Quickly and Easily

- Digital Guardian can be deployed, configured and protect data in just a few hours
- Pre-configured policies for PII, PHI, and PCI, along with the flexibility to create customized policies, ensure you protect what matters most to your organization and support compliance needs
- Reports provide a detailed picture of data movement for audits

Simplified Architecture

- The appliance consists of specialized sensors that monitor the full TCP stack, providing policy protection and enforcement for both inbound and outbound connections
- Scalable architecture provides flexible deployment options; single network appliances can perform multiple functions from network monitoring and enforcement to discovery of data stored in various repositories
- Capabilities may be decoupled and deployed across multiple locations reporting into a single management platform