**DIGITAL GUARDIAN®**

Digital Guardian Data Discovery

Sensitive Data Discovery Across the Enterprise and the Cloud

Digital Guardian Data Discovery uses automatic, configurable scanning of local and network shares using specific inspection policies to ensure sensitive content is discovered wherever it is located. Data discovery is extended to the cloud through integrations with leading cloud storage providers to scan repositories, enabling encryption, removal, or other automated remediation of sensitive data before the file is shared in the cloud - data that is already stored in the cloud can be scanned and audited at any time.
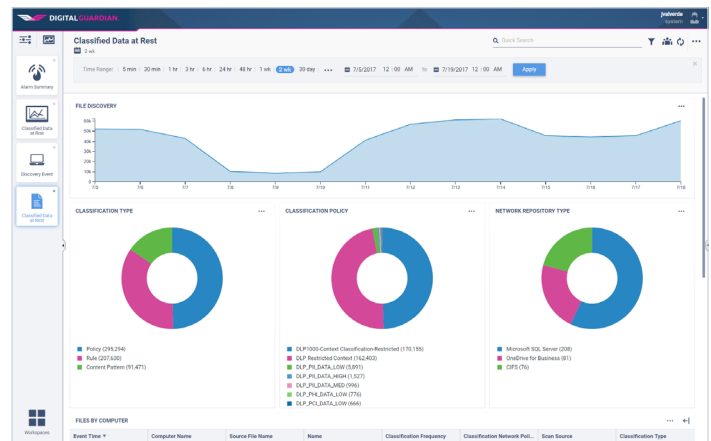
Deepest and Broadest Visibility

Network DLP   Cloud Data Protection   Data Discovery
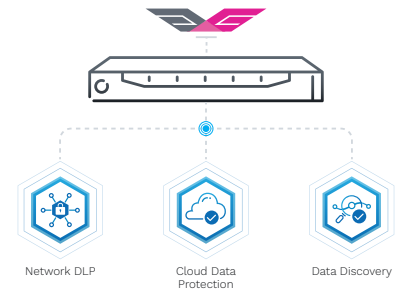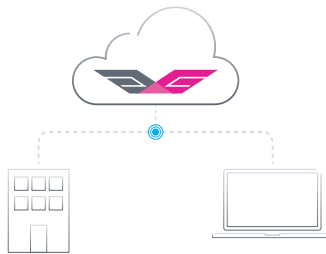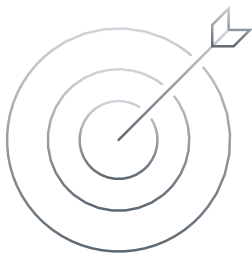
The Most Accurate Discovery for the Most Accurate Data Protection

Our unique fingerprinting technology is the industry's most accurate for identifying and controlling PII, PCI, & PHI data. By focusing on protecting PII/PCI/PHI, we provide the absolutely lowest false positive and false negative rate of any technology available. This allows your team to focus on the real risks.

The Most Flexible Deployment Options

Our compliance data protection is either delivered on premises or as a managed service. Backed by experts with 10+ years of implementation experience, our managed security program provides complete installation, administration, reporting, and semimonthly reviews.

Appliance Based Solution for Rapid Deployment and Low Overhead

Digital Guardian's Content Inspection engines combine content inspection, policy creation, and management in one, greatly simplifying deployment and management without sacrificing accuracy or effectiveness. Our approach is recognized for delivering the lowest total cost of ownership with no dedicated resources required to manage.

Key Benefits

Locates and Identifies All Sensitive Data at Rest

Allows your organization to find sensitive and regulated data on servers, shares, and in databases, within your enterprise or in the cloud. Pre-configured templates speed discovery of PHI, PCI, and PII data while customized templates deliver flexibility for other data types and emerging regulations including GDPR.
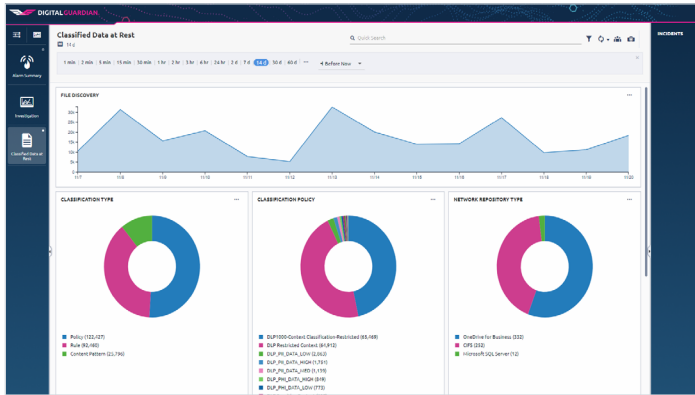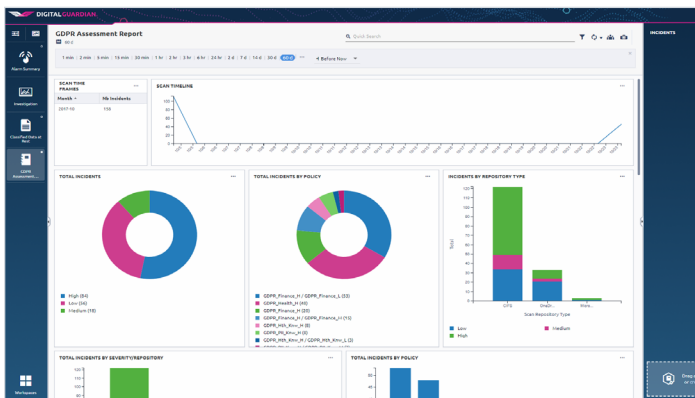
Delivers Automated, Flexible Remediation

Managers receive notification as well as the detailed list of files and their location that violate specific policy upon discovery scan completion. If certain file(s) violated a policy and based on assigned action (delete, encrypt, move) a file marker will be automatically left with policy violations details.
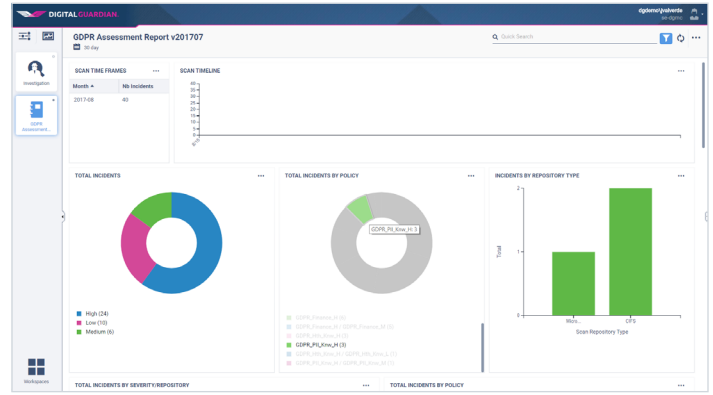
Demonstrates Data Security and Compliance

Documents the location and composition of sensitive data to support organizational security policies and to demonstrate compliance with external regulations.

SHARE