CUSTOMER SUCCESS STORY

DIGITAL GUARDIAN®

St. Charles Healthcare System - Enabling Care Providers While Protecting Patient Data

About the customer

St. Charles Health System (SCHS), a healthcare delivery system comprised of three hospitals and some twenty clinics in Central Oregon, provides a full range of medical specialties and services. Wanting to ensure HIPAA/EDI compliance, SCHS undertook a Baseline Security Risk Assessment with a healthcare information-security management consulting service to better understand their security posture.

The Business Challenge

With multiple locations and nearly 3,000 caregivers, SCHS wanted to locate all their sensitive data, monitor employee data-policy adherence, and then determine where and how to securely store the data. Their consultant organized a two-week Data Loss Risk Assessment, using Digital Guardian's Compliance appliance to track sensitive healthcare data throughout the integrated delivery network.

SCHS discovered that one of their hospital information-system vendors had set up a secure point-to-point FTP channel over which the two companies would communicate. However, the vendor misconfigured the system, as a result, data was being sent out via the Internet instead of over the secure channel. Additionally, various business associates (e.g. coders, insurers) were processing sensitive data and emailing it back to SCHS using unencrypted, clear text messages.

Critical Success Factors

- Complete security risk assessment
- Data location and encryption
- Support multiple use cases
- Comply with HIPPA and EDI protocols

St. Charles HEALTH SYSTEM

Industry

- Healthcare

Environment

- 3,000+ care givers
- Multiple facilites
- EHR systems with medical, financial, and personal information

Challenge

- Widespread distribution of critical data
- PHI, PII, and PCI data
- Poor user awareness
- Government regulation requirements
- Incorrectly configured/installed systems

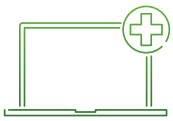
Results

- Visibility to all data movement and storage
- No additional IT or security headcount
- Fully compliant with HIPAA/EDI requirements

Data Types We Protect

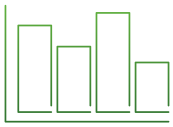
Hospitals

- Protected Health Information (PHI)
- Patient Financial Information Including Payment Card Industry (PCI) Data



Healthcare IT

- Patient Care Data
- Protected Health Information (PHI)
- Personally Identifiable Information (PII)



Healthcare Analytics

- Claims & Cost Data
- Unstructured Data Such as R&D, Clinical Data, Patient Behavior & Sentiment Data

Benefits Management & Insurance

- Personal health information (PHI)
- Claims Data
- Patient Care Data

The Solution

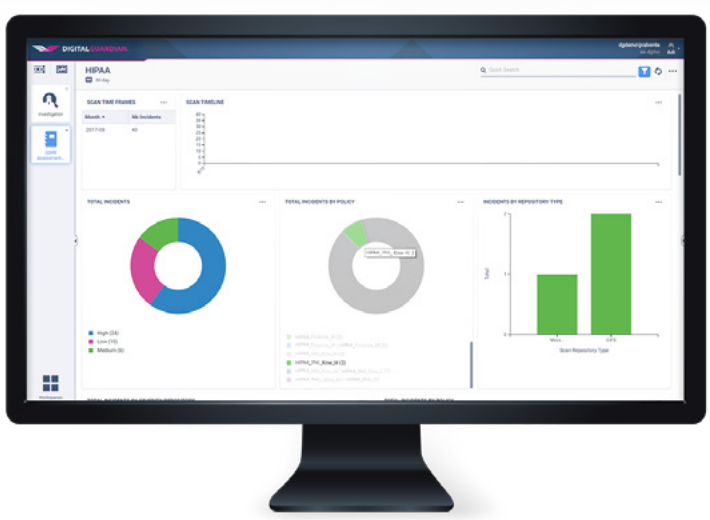
The Digital Guardian appliance was initially installed in a monitor-only mode to analyze network transmissions for sensitive data. When Digital Guardian and the consultant co-presented the findings, SCHS's IT team became aware of two major communication channels that would require immediate attention.

Digital Guardian's network appliance is designed for rapid installation and configuration, within minutes of powering it on, SCHS was collecting data. Steve Scott, InfoSec Manager, said "Once we saw items that could become major issues for us, we were able to remediate potential problems right away." This instant visibility meant SCSH could identify issues and correct them before stringent breach notification laws came into effect. "The appliances were easy to set-up and configure," said Steve. "They worked just as advertised. We were up and running in an hour with the basic information in place to begin monitoring our systems."

The appliances arrived preloaded with a wide range of HIPAA code set, healthcare EDI protocol identifiers, and preconfigured policies. Integrations with the EHR system meant deeper visibility into sensitive, healthcare databases. After SCHS registered their sensitive data/documents, they activated the preloaded policies and reporting templates to begin detecting sensitive healthcare data movement over the network before it was an external leak.

The Results

Based on the successful Data Loss Risk Assessment, SCHS decided to implement the complete Digital Guardian compliance solution for on-going monitoring, blocking and discovery. SCHS can now effectively enforce their data policies. "Our strategy is about educating behavior through our policies. We use Digital Guardian to supervise and reinforce the behavior," said Scott.



About Digital Guardian

Installed Based

- Over 700 customers from across the globe
- Industries served: Business services, education, energy, financial services, government, healthcare, manufacturing, retail, technology
- Used by 7 of the top 10 patent holders

Discovery and Classification

- Endpoint, network, cloud and local data storage
- Content, context, and user classification
- Fully automated to fully manual classification
- Over 300 data types, over 90 languages

Educate and Enforce

- Monitor log, prompt, justification request
- Auto-encrypt, quarantine, move, block

Actionable Analytics

- System, user, and data level event visibility
- Analytics that filter out the noise
- Drag and drop incident management
- Right click remediation in real time

Operation System Support

- Full visibility, analytics and controls across multiple operating systems
- Mac
- Windows
- Linux

Deployment

- Managed Security Program
- SaaS
- On-Premise

DIGITALGUARDIAN®