FORTRA™

CASE STUDY (Digital Guardian)

Data Visibility, Secure Remote Connections, and Increased Compliance Policy Awareness

About The Customer

Despite spending more than $1M per year on HIPAA compliance training, an internal audit at one of the largest managed healthcare providers in North America identified a significant risk of noncompliance. The company's auditors recommended stricter controls, both on and off the corporate network.

The Business Challenge

The organization had strong network defenses, but also many mobile users. A Virtual Private Network (VPN) was in place, but users were not diligent in using it. Enforcing controls on users that were not connected to the network was impossible. The training program failed because it was a specific, one-time event rather than an ongoing process. When people used data, their focus was on the task, not on the training from months ago.

The managed healthcare provider's business also required many users to travel with data. Medical personnel moved between facilities, claims agents traveled to visit clients, and many workers brought their laptops home each night. These users required the ability to connect to other networks.

The company needed to reinforce existing policies as data was used, and create a culture that educated users about the potential risks. They needed to change user behavior when interacting with sensitive, regulated data.

Critical Success Factors

- Ensure traffic flows through their network to take advantage of their investment in infrastructure security
- Block data egress for users disconnected from the corporate network
- Prevent the use of multiple network adapters used to bypass corporate controls
- Educate users on corporate policies in real time to influence behavior and reinforce training

INDUSTRY

- Healthcare

ENVIRONMENT

- Managed healthcare provider
- Geographically distributed workforce
- Users accessing PHI
- 40,000 Windows; 4,000 Mac workstations

CHALLENGE

- Widespread distribution of regulated data
- Mobile users off the corporate network
- Allow authorized use on network, while blocking risky actions on network
- Poor user awareness and training

RESULTS

- Visibility to all data movement
- Support for mobile and remote workers
- Internet access requires VPN
- Multiple network adaptors blocked

The Solution

Fortra™'s Digital Guardian® was the only solution that provided real time policy application based on network awareness, enforced connections through the company's VPN and prompted users in real time.

Digital Guardian structured policies supporting its requirements in the Digital Guardian Management Console. Digital Guardian endpoint agents, operating at the kernel level, enforced these policies on and off the network.

Network awareness allowed Digital Guardian to distinguish the corporate network from others and enforce appropriate policies. If a mobile user required internet access, Digital Guardian could allow access to a login page, then block further traffic until connected to the company's VPN. Once on the VPN, the user benefitted from the company's extensive network controls and could perform their job functions.

Enterprise security policies can be difficult to remember while conducting daily business on tight timelines. To augment training, Digital Guardian's prompt mode was used extensively. In prompt mode, when a user attempts an action that could increase risk or violate a policy, Digital Guardian presents a screen requiring the user to acknowledge the company policy and provide justification to continue. The response and action are recorded and stored in evidentiary-quality log files.

Data Types We Protect

HOSPITALS

- Personal health information (PHI)
- Patient Financial Information Including Payment Card Industry (PCI) Data

HEALTHCARE IT

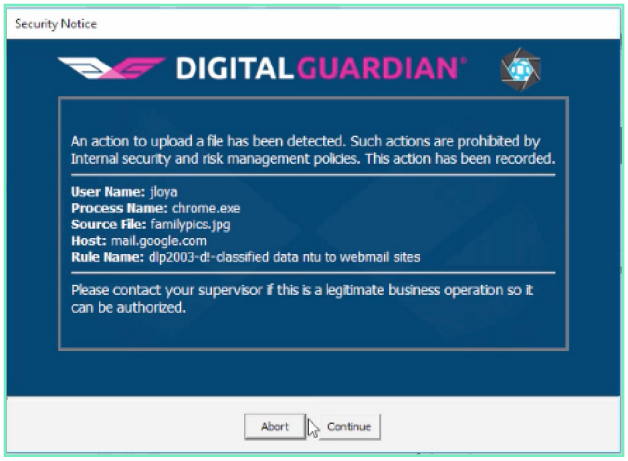
- Patient Care Data
- Personal health Information (PHI)
- Personally Identifiable Information (PII)

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 Results

After deploying Digital Guardian, the customer could monitor all data movement, enforce the use of the company's VPN for remote users, block multiple network adaptors and communicate company requirements. In the first six months of use, they reported an 85% decrease in prompts to users, indicating a significant increase in policy awareness and secure employee behavior.

About Digital Guardian

INSTALLED BASED

- Over 600 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

- On-Premise
- SaaS
- Managed Security Program

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.