CUSTOMER SUCCESS STORY

Large Managed Healthcare Provider

HEALTHCARE

Industry
- Healthcare

Environment
- 40,000 Workstations
- Windows
- 4,000 OS X

Challenges
- Widespread distribution of critical 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 blocked except through company's VPN
- Multiple network adaptors blocked
-

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

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 non-compliance. 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 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 change user behavior when interacting with sensitive data, reinforce existing policies as data was used, and create a culture that held users accountable for their actions.

CRITICAL SUCCESS FACTORS

- Guarantee that all traffic flows through their network to take advantage of their investment in infrastructure security
- Block all 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

DIGITALGUARDIAN™ by VERDASYS

DIGITAL GUARDIAN FACTS

Customers

- Over 250 customers
- Inlcudes 130 of the Global 2000 and government agencies
- Used by 7 of the top 10 patent holders
- Over 2.1 Million endpoints protected
- Only solution to scale to 250,000 agents

Information Discovery and Classification

- Context-based data awareness
- Content inspection
- User classification
- All content is tagged with permissions
- Permissions persist through reuse, renaming
- Over 300 data types
- 90 languages

Response Options

- Monitor, log, report
- Prompt, justify, and report
- Block and report

Supported Platforms

- Desktop/Laptop
- Server
- Network
- Virtual
- Supports devices on network and off network

Supported OS

- Microsoft Windows®
- Linux
- Mac OS X®

Deployment Models

- On Premise
- Managed Security Program (MSP)
- Hybrid MSP

DIGITALGUARDIAN™ by VERDASYS

www.digitalguardian.com

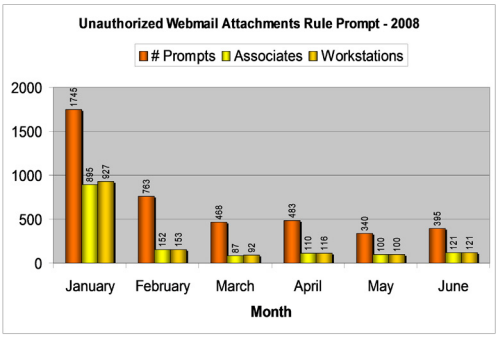
THE SOLUTION

Digital Guardian was the only solution that could provide real time policy application based on network awareness, enforce connections through the company's VPN and prompt users who might otherwise violate appropriate use policies.

Digital Guardian personnel worked with this client to structure 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 other, untrusted networks, and enforce appropriate policies in each case. If a mobile user was onsite with a customer or at a hotel and required internet access, Digital Guardian could allow access to a login page, and then block any further traffic until the user connected to the company's VPN. Once on the VPN, the user benefitted from the company's extensive network controls and could perform all legitimate job functions.

Users do not always violate policies deliberately. Complex policies can be difficult to remember while conducting daily business. To augment training, Digital Guardian's prompt and warn modes were used extensively. In prompt and warn modes, when a user attempts an action that would increase risk or violate a policy, Digital Guardian presents a screen requiring the user to acknowledge the appropriate company policy and provide justification to continue. The response and action are recorded and stored in evidentiary-quality log files.



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 to users attempting to violate policies. 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.

Copyright © 2014 Digital Guardian, Inc. All rights reserved. Digital Guardian and Security's Change Agent are trademarks of Digital Guardian, Inc. in the U.S. and other countries. All other trademarks are the property of their respective owners.