CUSTOMER SUCCESS STORY

Major U.S. Natural Gas Producer

ENERGY

Industry
- Energy

Environment
- 14,000 workstations
- 400 Citrix servers
- Internal users
- Contractors and business partners from external networks (via Citrix sessions)
- Privileged users with direct physical access to Citrix server hardware

Challenges
- Non-employee business partners must access corporate data and network resources from remote virtual servers (Citrix)
- Multiple data types
- Internal users, privileged users, and business partners

Results
- Over $4 million in saved costs compared to alternative solutions
- Eliminate the need for split farms or customizing applications running in Citrix
- Immediate visibility into all user activity, without impacting productivity
- Application control prevents unauthorized executables in the Citrix environment
- Automatic encryption of critical files moved by email or to removable devices

DIGITALGUARDIAN™ by VERDASYS

IP Protection, Secure Partner Collaboration and $4 Million in Cost Savings

One of the largest natural gas producers in North America needed to share critical information with business partners, but was concerned about losing data. The company is constantly bidding for drilling rights and developing new technology to maximize its output. Energy exploration, in particular, is an expensive undertaking. This information is valuable to the company and its competitors.

Data needs are massive in this industry. Seismic testing data, multiple geological modeling applications, and custom software help to estimate the appropriate investment input and energy output from each property. This data is critical to the firm's success, and its use and distribution is tightly controlled.

THE BUSINESS CHALLENGE

The energy industry includes hundreds of contractors and companies that provide specialized services to larger organizations. These business partners may assist in analysis, drilling operations, or legal matters, and therefore must access confidential data from their customers. The company had deployed multiple Citrix servers to allow its partners to access corporate data. While this provided access, it also allowed users to launch other network-capable applications, such as web browsers, and a sophisticated user could bypass controls to launch other software. To "lock out" this ability, the company's internal application deployment team needed to customize each application published to Citrix for contractor use, costing hundreds of labor hours per application. As an alternative, a split-farm deployment of Citrix was considered, but was determined to be cost prohibitive.

CRITICAL SUCCESS FACTORS

- Streamline the process by which partners accessed data through the Citrix servers
- Enforce appropriate use of data by people and applications according to business workflows
- Gain visibility into where data resided, where it was used, and by which people or processes
- Allow simple access to data by employees and business partners with appropriate privileges, while preventing critical data from being used improperly or stolen
- Enable privileged users in IT to perform upgrades and maintenance on servers and workstations without compromising data security

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

Citrix was a logical technology for accessing the organization's data, but only under three conditions:

- The use of other, unauthorized applications must be prohibited
- Users must only have access to data for which they had a legitimate business use
- Users must only be able to use the data in approved ways

Digital Guardian worked with its customer to document legitimate data flow models and build DG policies to support these. Context-based data awareness and content inspection features were used to identify and classify all data in the system. With Digital Guardian agents installed on virtualized Citrix desktops and servers, all policies were enforced at the endpoint. This allowed users and applications to use data freely, but only in authorized transactions. For example, users could move data to specific, approved drives, but attempts to move data to unapproved drives would be blocked.

THE RESULTS

The deployed solution was simple, manageable, and saved the company over $4 million in hardware, software, and physical security infrastructure. Digital Guardian allowed the company to monitor and manage a shared Citrix server farm without the added expense of a split farm or customizing each application running on Citrix.

Digital Guardian allowed employees, contractors, and partners ready access to the data they required, with full auditing and without risk of misuse. When information was required to leave the network by email or removable device, Digital Guardian policies enforced automatic encryption of the data. Since policies and permissions travel with the data, only an authorized user could view encrypted files, and only on a Digital Guardian protected device. Digital Guardian's Application Control functionality prevented unauthorized applications from executing in the virtual environment. Privileged users could perform system updates and maintenance while being blocked from viewing, moving, or copying confidential files. Digital Guardian blocked unauthorized actions while simultaneously notifying the incident response team of the event.

The company improved information sharing and user productivity while reducing risk overall. Business partners now have the information they need, while Digital Guardian monitors its use and prevents misuse.