CUSTOMER SUCCESS STORY

New England Federal Credit Union

FINANCIAL SERVICES

Industry

- Financial Services

Challenges

- Maintain competitive advantage of safety and soundness
- Understand what data is shared with partners and control where and how data is distributed
- Meet new and emerging credit union compliance regulations regarding data protection without disrupting established business processes

Solution

- Use Network DLP to identify how and where data leaves the organization
- With Network DLP discovery capability, locate sensitive data that should be protected
- Integrate data protection with the web proxy to get visibility into web traffic

DIGITAL GUARDIAN®

Stopping Data Egress with Digital Guardian DLP

NEW ENGLAND FEDERAL CREDIT UNION

New England Federal Credit Union (NEFCU) is a member-owned financial institution serving communities in the six counties of northwestern Vermont since 1961. With more than 88,000 members and $1 billion in assets, it is the largest credit union in the state.

The credit union has had a strong security culture for years and continues to deploy technologies to augment existing policies and infrastructure. For example, USB ports are blocked, network access control and authentication protect systems and the network, and sensitive documents and email are encrypted. The organization also does frequent employee training and education on security and data protection.

THE BUSINESS CHALLENGE

Michael Stridsberg, Information Security Program Manager, says:

“In security, you are always concerned about what’s coming in to your organization,” he notes. “What we wanted to know here at New England Federal Credit Union was what data was going out – a 180 degree change from the typical security approach.”

“We work with a number of vendors, partners and service providers, and we realized they all required differing amounts of data and access,” said Stridsberg. But the credit union could not determine exactly who got what data.

So we began looking for a way to determine what data was being exchanged and patterns of use.

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

DIGITAL GUARDIAN®

www.digitalguardian.com

THE SOLUTION

Stridsberg had heard about DLP and realized it might help him understand what was going out of the organization. After due diligence on three DLP vendors, NEFCU selected Digital Guardian Network DLP for its simplicity, cost-effectiveness and completeness of functionality in its architecture, which Stridsberg calls "elegant."

THE RESULTS

For the first three months or so, the NEFCU simply monitored the network. From detailed analysis provided by Digital Guardian Network DLP, Stridsberg and his team saw clear patterns of data usage. During that period they continued to build and refine their data security policies, around their business rules, creating a system in which false positives are basically non-existent. Today, they feel assured that the business rules and the automatic blocking, encrypting and rerouting of data they put in place are accurate.

Additionally NEFCU has created a white list of vendors with whom they share information. For each vendor, they have set up different security controls, utilizing Digital Guardian Network DLP, as to what data each receives.

Despite the reputation of some DLP solutions for complexity, installing Digital Guardian Network DLP took only a few hours and requires very little ongoing maintenance. Today Stridsberg receives alerts via email and text, depending on priority level.

"Once Digital Guardian Network DLP was installed, visibility into our network traffic was significantly improved," said Stridsberg. "We could see exactly what data was being transmitted and where. Today I can't imagine doing security work without it!"

> "Today I can't imagine doing security work without Digital Guardian Network DLP"
>
> *- Michael Stridsberg, Information Security, New England Federal Credit Union*

New England Federal Credit Union
nefcu.com