CUSTOMER SUCCESS STORY

DIGITAL GUARDIAN®

Securing New England Federal Credit Union's members PII

About the Customer

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 and needed to ensure their member's could entrust them with their personal information.

The Business Challenge

The credit union historically had a strong security culture and continued 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 holds frequent employee training and education on security and data protection. The credit union works with several vendors, partners and service providers, and they all require differing amounts of data and access.

What NECFU lacked was enterprise wide visibility and granularity into sensitive, regulated data movement; NECFU could not determine exactly what data was received by whom. 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."

Critical Success Factors

- Improve visibility into data sharing with vendors, partners and service providers
- Classify data quickly and accurately
- Rapid deployment, low overhead
- Enforce appropriate use of data by users with varying privileges
- Maintain client trust

Industry

- Financial Solutions

Environment

- 88,000 members
- $1 billion in assets
- External partner network
- Largest credit union in Vermont

Challenge

- Maintain competitive advantage of safety and soundness
- Understand what data is shared with partners
- Granular coontrol where and how data is distributed
- Meet new and emerging compliance regulations without disrupting business processes

Results

- Visibility into all user activity, without impacting productivity
- Automatic blocking, encryption and rerouting of data
- Credit union data protection regulations compliant

Data Types We Protect

Banking

- Personally Identifiable Information (PII)
- Payment Card Industry Data Security Standard (PCI DSS)

Insurance

- Protected Health Information (PHI)
- Personally Identifiable Information (PII)
- Payment Card Industry Data Security Standard (PCI DSS)

FInancial Markets

- Intellectual Property (IP): Deal Management Information, Trading Algorithms, Financial Modeling, IPO Plans, M&A Plans

The Solution

NEFCU selected Digital Guardian (DG) Network DLP for its simplicity, cost effectiveness and completeness of functionality in its architecture, which Stridsberg calls “elegant.” Digital Guardian began looking for a way to determine what data was being exchanged as well as any patterns of use. For the first three months, the NEFCU simply monitored the network. From detailed analysis provided by the Network DLP, Stridsberg and his team saw clear data usage patterns. While some matched the expectations of the infosec team, they also learned of other patterns they needed to address. 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. They were also able to integrate protections to get visibility into web traffic.

Digital Guardian Network DLP installation took only a few hours and requires minimal ongoing maintenance, this meant no additional staff and low TCO. “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.”

The Results

Today, they feel confident that their business rules and automatic blocking, encrypting and rerouting of data are accurate. Additionally, NEFCU has created a white list of vendors with whom they share information. Utilizing DG Network DLP, they have set-up different security controls to determine what data each vendor is able to receive.

New England Federal Credit Union
nefcu.com

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

DIGITALGUARDIAN®