

Customer Success Story



South Western Federal Credit Union

Protecting its endpoints from data leakage and preventing the introduction of malware through removable media.

Background

South Western Federal Credit Union (SWFCU) is a full-service credit union with \$172 million in assets. Miriam Neal, vice president of information systems, oversees the IT security initiatives at the La Habra, California headquarters and the Whittier, California branch. With slightly more than 50 employees, the IT environment includes over 70 workstations and 11 servers.

Challenge

Today, financial institutions face the severe reality that anyone - including both employees and outsiders - carrying an MP3 player, PDA, USB memory stick, etc. has the potential to quickly and discretely upload reams of sensitive data from the IT network to the tiny device and walk out the door undetected.

“Removable media is so ubiquitous and it creates a new threat vector that must be addressed,” said Neal. “The increased storage capacity and functionality of today’s portable devices enables employees to seamlessly transfer critical information in and out of the organization or unintentionally introduce malware into the network via CD or unknown device.”

Data theft and introduction of malware via removable devices were top concerns for Neal and SWFCU. As a particularly progressive credit union, Neal was acutely aware of its need to stay steps ahead of these emerging “insider” threats. Neal began a search for a network security technology

to aid in protecting internal assets and to enforce written policies concerning use of removable media: SWFCU prohibits the use of USB ports or CD-ROMS without permission, and employees are not permitted to remove software licenses or private information.

“We wanted to lock down our workstations to prevent people from downloading information they shouldn’t to USB drives. We also wanted a means of tracking what our IS staff did with USB drives when working on our computers.”

Miriam Neal, VP of Information Systems

Solution and Benefits

In April 2006, Neal implemented Lumension Data Protection™ (formerly Sanctuary) to protect the confidentiality, integrity and availability of all SWFCU endpoints. Lumension allows Neal to customize a “whitelist” of devices that are allowed access on the credit union’s PCs, laptops and servers.

“Many portable storage devices help our employees better serve our customers, so we cannot take drastic measures like stripping out all USB ports.”

Miriam Neal, VP of Information Systems

“[Lumension] allows us to control exactly what devices can be used on our PCs and laptops while providing employees with the technologies they

need. [Lumension] also enables us to enforce policy for allowed devices, adding an extra layer of protection.”

This proactive policy enforcement approach safeguards SWFCU from known and unknown threats because any device that is not on the whitelist simply will not work. Neal has the option to assign permissions at a high level or to allow particular user groups or individual workstations to access certain devices at specific times. Policies can also be enforced by specific models of USB devices, such as those with automatic encryption, and by time constraints, encryption, volume of data, data transfer and much more granular criteria.

“We locked down USB ports and CD and floppy drives on our computers so any storage media that are plugged in cannot be read from or written to, while still allowing mice and printers to work,” said Neal. “But if need be, we can easily make quick changes. For example, our CEO may need to use a CD-ROM. With [Lumension], we can open up the drive for her for a period of time.”



In addition to Lumension Data Protection’s flexibility and ease of use, the software’s detailed audit logging capabilities enable Neal to shadow all activity related to removable storage media.

“The product is seamless and unobtrusive to employees. If employees are allowed to use a flash drive or compact disc, [Lumension] shadows it. If employees upload a spyware engine that would transmit private information to a flash drive or from a flash drive, I have a shadow of it,” said Neal.



Global Headquarters

15580 N. Greenway-Hayden Loop, Suite 100

Scottsdale, AZ 85260 USA

phone: +1.888.725.7828

fax: +1.480.970.6323

www.lumension.com

Vulnerability Management | Endpoint Protection | Data Protection | Reporting and Compliance