SecureWave
Safeguarding Tomorrow

Sanctuary
Device Control

South Western Federal Credit Union

South Western Federal Credit Union

South Western Federal Credit Union protects its endpoints from data leakage and prevents the introduction of malware through removable media by using SecureWave Sanctuary

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, Calif. headquarters and the Whittier, Calif. 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," said Neal.

Solution and Benefits

In April 2006, Neal implemented SecureWave's Sanctuary® endpoint security software to protect the confidentiality, integrity and availability of all SWFCU endpoints. Sanctuary 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," said Neal. "Sanctuary allows us to control exactly what devices can be used on our PCs and laptops while providing employees with the technologies they need. Sanctuary 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 Sanctuary, we can open up the drive for her for a period of time."

In addition to Sanctuary'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, Sanctuary 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.

Conclusion

Sanctuary enables Neal to manage the potentially crippling risk of exposing sensitive information, regardless of motive. "We needed to make sure our private info was truly secure," said Neal. "With Sanctuary, we got immediately to the bottom line. It requires little or no effort on my part to guarantee that our data is going no where. And we know exactly who is attempting to access it and when."

SecureWave
Safeguarding Tomorrow

www.securewave.com
info@securewave.com

North America

13755 Sunrise Valley Drive
Suite 203
Herndon, VA 20171
United States of America
+1 (703) 713 - 3960 Phone
+1 (703) 793 - 7007 Fax

United Kingdom

Midsummer Court
314 Midsummer Boulevard
Milton Keynes MK9 2UB
United Kingdom
+44 (0) 1908 357 897 Phone
+44 (0) 1908 357 600 Fax

Continental Europe and Rest of World

Atrium Business Park
23, rue du Puits Romain
L-8070 Bertrange
Luxembourg
+352 265 364-11 Phone
+352 265 364-12 Fax

SWFCU - Mar. 07 - V1.0