

United States Postal Service Federal Credit Union

The U.S. Postal Service Federal Credit Union (USPS FCU), established in 1934, serves more than 23,000 members with branches in California, Maryland, Pennsylvania, Virginia, and Washington D.C. The credit union manages assets in excess of \$180 million and is subject to National Credit Union Administration (NCUA) regulations.

Log and Event Management Challenge

The USPS FCU faces strict regulatory guidelines and annual audits executed by the NCUA, created to interpret and enforce the provisions of the Federal Credit Union Act (FCUA). Consequently, the credit union needed a solution that could monitor and respond to all network and user activity, down to each endpoint, while providing auditors with granular and customizable reports and ensuring forensic traceability in the event of a breach or policy violation.

With 75 employees, the USPS FCU stumbled upon a couple of challenges known to other small to mid-sized enterprises:

1. Outsourced log management was too expensive and incredibly risky. "Our network data is too valuable to share with another company," said Alan McHugh, Manager of Information Technology for USPS FCU. "Our members trust us to keep all sensitive data in house."
2. Enterprise-grade security information and event management (SIEM) solutions were priced for large companies and thus stretched well beyond USPS FCU's IT budget. Additionally, all that money didn't buy real-time analysis and blocking capabilities, which were the most important proactive defense to stop emerging attacks. Enterprise tools watch, aggregate data, and report, but they don't take action. USPS FCU needed more advanced solutions to provide comprehensive network management capabilities in real time.

CLIENT STATISTICS

130-node network

3 full-time IT
employees

\$18K savings in
staff hours

\$180M in assets

"With SolarWinds LEM, we're exposing potential threats and preventing them from damaging our business"

—Alan McHugh, Manager of Information Technology for USPS FCU

Solution

The credit union selected SolarWinds Log & Event Manager (LEM) for four specific reasons:

- Right-sized for smaller budgets: The solution's architecture and pricing are tailored to smaller companies. The appliance-based technology is plug-and-play, meaning that implementation takes hours, not weeks or months. And the cost starts at \$20,000 – a fraction of competitors' prices.
- 24/7 monitoring: SolarWinds LEM monitors all network activity – even when no one is watching – and stops policy violations and network and data breaches in real time, notifying network administrators of threats instantly via email, pager, and/or cell phone. "I'll even know if the cleaning crew or security guard is trying to log on after hours," said McHugh.

- Outing the insider: SolarWinds LEM provides a forensic trail of user activities. It identifies insider policy

breaches instantly – including unauthorized USB flash drive insertions and downloads – and stops violators in their tracks while notifying network managers.

- Security at the end point: SolarWinds LEM's solution controls policies from servers to endpoints, giving IT administrators the ability to shut down any system or user group across USPS FCU's seven branches in the event of threat detection. This granular control prevents fast-moving worms from spreading, quarantining at-risk systems before they can compromise member data.

"With SolarWinds LEM, we're exposing potential threats and preventing them from damaging our business," said McHugh. "In one case, SolarWinds LEM instantly red-flagged multiple, simultaneous log-on failures. We examined the attempted user names, passwords, and incoming IP addresses, and quickly recognized that a bot was attempting to hack into our network. With the evidence provided by SolarWinds LEM, we contacted the hacker's Internet service provider and shut them down."

Results and Extra Benefits

USPS FCU is gaining other unanticipated benefits with SolarWinds LEM. Its 130-node network, managed by three full-time IT employees, generates terabytes of log data weekly. Before SolarWinds LEM, the team invested four to eight hours each week manually searching through logs for policy violations and forensic clues. SolarWinds LEM, however, automates this process and delivers significant benefits for USPS FCU:

1. Savings: The hours eliminated save \$18,000 in annual staff hours. This time-saver alone nearly covers the cost of SolarWinds LEM's solution.
2. Accuracy: SolarWinds LEM catches all policy violations, while manual reviews can easily overlook problems buried in countless lines of logs. The system ensures that every log file is examined with the same level of scrutiny.
3. Bandwidth: IT employees wear many hats within the organization. With SolarWinds LEM keeping an eye on their network, they have increased bandwidth to handle other IT responsibilities.

"SolarWinds LEM is a natural extension of our network," said McHugh. "In reality, we consider the SolarWinds LEM appliance to be our fourth IT employee."

IT Management
Inspired by You.

SolarWinds (NYSE: SWI) provides powerful and affordable IT management software to more than 100,000 customers worldwide — from Fortune 500 enterprises to small businesses. We work to put our users first and remove the obstacles that have become "status quo" in traditional enterprise software. SolarWinds products are downloadable, easy to use and maintain, and provide the power, scale, and flexibility needed to address users' management priorities. Our online user community, thwack, is a gathering place where tens of thousands of IT pros solve problems, share technology, and participate in product development for all of SolarWinds' products.

solarwinds.com

solarwinds® 

3711 S. MoPac Expressway, Building Two, Austin, Texas 78746
T: 866.530.8100 | F: 512.682.9301

©2012 SolarWinds, Inc. All rights reserved. SolarWinds®, the SolarWinds logo, ipMonitor®, LANsurveyor®, and Orion® are among the trademarks or registered trademarks of the company in the United States and/or other countries. All other trademarks are property of their respective owners.
CS-120203