Energy Federal Credit Union

Headquartered in Rockville, Maryland, Energy Federal Credit Union (EFCU) was founded in 1948 by employees of the U.S. Atomic Energy Commission. EFCU has 53 employees and its assets total $100 million. With four locations surrounding the Washington D.C. area, EFCU is sponsored by the U.S. Nuclear Regulatory Commission and the U.S. Department of Energy and is subject to regulations put forth by the National Credit Union Administration (NCUA).

Appendix A of Part 748 of the NCUA's Rules and Regulations calls for credit unions to identify internal and external threats that could result in unauthorized disclosure, misuse, alteration or destruction of member information systems, as well as assess the potential of these threats.

CLIENT STATISTICS

$100 M total assets

4 branch locations

53 employees

25% capacity gained

Log and Event Management Challenge

EFCU was using passive log capture technology to track traffic entering and exiting its network by manually examining firewall activity logs. The result; without correlation, EFCU had limited visibility into vital network activity — leaving the credit union vulnerable to network-based internal and external threats and susceptible to NCUA penalties.

"We were using Kiwi Log Viewer to watch the firewall logs," said Ted Carmack, IS Manager at EFCU. "While the approach seemed to be working, it wasn't the best solution because we were missing too much activity on the network and couldn't see any trends, make any predictions or do any analysis that would deliver the type of insight that we needed."

With an overworked IT staff of three people and an audit approaching fast, EFCU needed to find and deploy an easy-to-use network security solution that would provide real-time visibility into all network activity across EFCU's four branches, help the business meet NCUA compliance and take action when a threat or violation was detected with very little management.

Solution

Carmack turned to trusted colleagues at other credit unions for recommendations on technology solutions that would fit his requirements.

"The credit union community is extremely tight knit," said Carmack. "We share our IT experiences with each other and SolarWinds Log & Event Manager came highly recommended from several other credit unions because of its ability to extend small IT departments by proactively alerting and responding to threats and policy violations. It sounded like it was exactly what we needed."

EFCU selected TriGeo SIM for five reasons:

1. SolarWinds Takes Action. SolarWinds Log & Event Manager (LEM) is the only SIEM solution that proactively responds to policy violations and network threats in real-time — giving EFCU the ability to actively defend its network, prevent damaging data loss or theft, and catch events often missed during manual log analysis.
2. 360-degree visibility. SolarWinds LEM gives EFCU a clear picture of everything that's happening on its network and the crucial context to be able to identify and alert staff of abnormalities immediately. The solution packages intelligence in an understandable format that makes it easy for administrators to interpret and report when needed.
3. Made for the Mid-market. SolarWinds LEM is designed to complement and extend midmarket IT departments — usually with fewer full-time IT staff members. The technology doesn't require a team of analysts to manage it and is competitively priced to fit tight IT budgets.
4. Strong Security = NCUA Compliance. SolarWinds LEM helps hundreds of midmarket credit unions achieve NCUA compliance through strong information security practices. The technology actively monitors all network log data in real-time and actively responds to policy violations and network threats to ensure data security and integrity.
5. USB Device Lockdown. SolarWinds LEM's USB-Defender helps network administrators put a leash on unauthorized USB device use. The solution goes beyond simple alerting, giving businesses the ability to actively "eject" the device, disable the user account or even quarantine the workstation to prevent information leakage or worm propagation.

Results

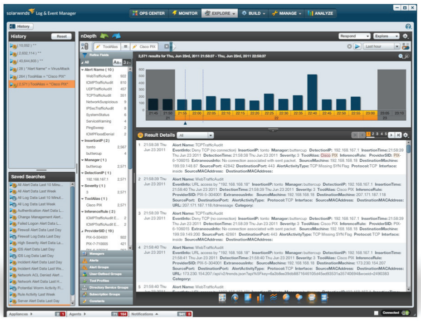
"Within weeks of implementing SolarWinds LEM, we were receiving valuable, actionable reports and have since passed several audits," added Carmack. "SolarWinds' support made it quick-and-easy for us to configure the appliance to fit our network security needs and each time that we've called — we've been connected to a live person that resolves our issue immediately."

The unexpected benefits:

- Network Device Diagnostics. EFCU uses SolarWinds LEM to monitor the "health" of network-attached devices across all four of its locations. Network administrators are alerted as soon as a device goes offline — helping them pinpoint connection problems and avoid prolonged outages.
- Proactive Maintenance Planning. SolarWinds LEM helps EFCU identify trends in network behavior allowing the IT team to better plan for traffic spikes and schedule routine network upgrades and maintenance more effectively.
- Twice the Space, Half the Hassle. EFCU's previous log capture device was only collecting logs from its firewall, and exceeded the allotted storage space in nine months. With SolarWinds LEM, EFCU is collecting log data from all of the devices across it network and has used 25 percent of SolarWinds LEM's capacity within a one-year period.

"SolarWinds LEM truly is an amazing tool with no limitations," said Carmack. "I don't know of anything else on the market today that can match the quality of results SolarWinds LEM delivers."

We would need three or four experienced network administrators working around the clock to manage the same workload that SolarWinds LEM does. Even if we had the money to staff an IT department like that, we still wouldn't get the same value and results that SolarWinds LEM delivers day in and day out."



2,571 results for Thu, Jun 23rd, 2011 21:58:37 - Thu, Jun 23rd, 2011 22:58:37

1 21:58:38 Thu Jun 23 2011 Alert Name: TCPTrafficAudit EventInfo: Deny TCP (no connection) InsertionIP: tonto Manager: buttercup DetectionIP: 192.168.167.1 InsertionTime: 21:58:39 Thu Jun 23 2011 DetectionTime: 21:58:38 Thu Jun 23 2011 Severity: 3 ToolAlias: Cisco PIX InferenceRule: ProviderSID: PIX-6-106015 ExtraneousInfo: No connection associated with sent packet. SourceMachine: 192.168.168.18 DestinationMachine: 199.59.148.87 SourcePort: 42842 DestinationPort: 443 AlertActivityType: TCP Missing SYN Flag Protocol: TCP Interface: inside SourceMACAddress: DestinationMACAddress:

2 21:58:39 Thu Jun 23 2011 Alert Name: WebTrafficAudit EventInfo: URL access by "192.168.168.18" InsertionIP: tonto Manager: buttercup DetectionIP: 192.168.167.1 InsertionTime: 21:58:40 Thu Jun 23 2011 DetectionTime: 21:58:39 Thu Jun 23 2011 Severity: 3 ToolAlias: Cisco PIX InferenceRule: ProviderSID: PIX-5-304001 ExtraneousInfo: SourceMachine: 192.168.168.18 DestinationMachine: 207.171.187.118 SourcePort: DestinationPort: AlertActivityType: Protocol: TCP Interface: SourceMACAddress: DestinationMACAddress: URL: 207.171.187.118:/tdmessage Category:

3 21:58:39 Thu Jun 23 2011 Alert Name: TCPTrafficAudit EventInfo: Deny TCP (no connection) InsertionIP: tonto Manager: buttercup DetectionIP: 192.168.167.1 InsertionTime: 21:58:39 Thu Jun 23 2011 DetectionTime: 21:58:39 Thu Jun 23 2011 Severity: 3 ToolAlias: Cisco PIX InferenceRule: ProviderSID: PIX-6-106015 ExtraneousInfo: No connection associated with sent packet. SourceMachine: 192.168.168.18 DestinationMachine: 199.59.149.200 SourcePort: 42861 DestinationPort: 443 AlertActivityType: TCP Missing SYN Flag Protocol: TCP Interface: inside SourceMACAddress: DestinationMACAddress:

4 21:58:40 Thu Jun 23 2011 Alert Name: WebTrafficAudit EventInfo: URL access by "192.168.168.18" InsertionIP: tonto Manager: buttercup DetectionIP: 192.168.167.1 InsertionTime: 21:58:41 Thu Jun 23 2011 DetectionTime: 21:58:40 Thu Jun 23 2011 Severity: 3 ToolAlias: Cisco PIX InferenceRule: ProviderSID: PIX-5-304001 ExtraneousInfo: SourceMachine: 192.168.168.18 DestinationMachine: 173.230.154.207 SourcePort: DestinationPort: AlertActivityType: Protocol: TCP Interface: SourceMACAddress: DestinationMACAddress: URL: 173.230.154.207:/api/v2/trends.json?api%5Fkey=6a3b8ee39db8871646105d45ed93531a35740694&woeid=2490383 Category:

5 21:58:40 Thu Alert Name: WebTrafficAudit

SolarWinds LEM quickly identifies attacks, highlights threats, and uncovers policy violations with real-time log analysis and powerful event correlation.

> "We would need three or four experienced network administrators working around the clock to manage the same workload that SolarWinds LEM does. Even if we had the money to staff an IT department like that, we still wouldn't get the same value and results that SolarWinds LEM delivers day in and day out," said Carmack.

IT Management
Inspired by You.

SolarWinds (NYSE: SWI) provides powerful and affordable IT management software 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, TX 78746
T: 866.530.8100 | F: 512.682.9301