

## Alaska USA Federal Credit Union

Exceeding Specifications for Event Alerts and Reporting with Symantec Security Information Manager



Faced with more complex threats and increasing regulatory requirements, Alaska USA Federal Credit Union sought a tool that would collect log data from the various parts of its security infrastructure so that it could be manually analyzed. The organization got much more than it asked for with Symantec Security Information Manager, which not only collects the log data, but provides automated analysis tools, custom alert notification, and reports that can be customized to specific criteria. Structured Communication Systems provided implementation services, and Symantec Consulting Services wrote custom data collectors for several systems. As a result, the credit union has avoided an estimated 1,000 hours of labor annually that was expected for the manual analysis, and is able to demonstrate compliance with PCI and other standards.

### ORGANIZATION PROFILE

Alaska USA Federal Credit Union ([www.alaskausa.org](http://www.alaskausa.org)) is a not-for-profit financial services cooperative, owned by its more than a quarter million members. It is a leading credit union in the U.S., and one of the largest financial institutions in the state of Alaska. Based in Anchorage, the credit union has more than \$3.5 billion in assets and 57 branches throughout Alaska and in western Washington state.

### INDUSTRY

Financial Services

### SOLUTION

Security Management,  
IT Compliance

### Filling an Unmet Need

After World War II, federal civil service personnel were transferred in record numbers to the territory of Alaska, which would not become a state for more than a decade. At Fort Richardson in 1948, 15 founding members started Alaska USA Federal Credit Union because they felt that local financial institutions were not meeting the needs of this new constituency. Members began pooling their savings and extending credit to one another, while volunteering their time to operate the credit union.

Sixty years later, Alaska USA is one of the largest financial institutions in Alaska, with locations in the Anchorage area, the Kenai Peninsula, interior and southeastern Alaska, and the Puget Sound area in Washington state. Its members, however, can be found around the world—testimony to both the mobility of Alaskans and a high level of customer loyalty that has been earned over the years.

### The Necessity of Protection

IT systems play a large role in maintaining customer loyalty at any financial services institution. Alaska USA's far-flung membership makes this element doubly important, and security is a critical piece of the puzzle. "In a competitive environment, it's crucial to our reputation and the trust that our members place in us to protect member data," says William Lidster, Alaska USA's manager of information security administration.

Two years ago, Lidster noted that the threat landscape was becoming more complex, with profit-motivated hackers generating new threats and data breaches becoming

**"We came with a limited requirement set simply because we didn't know that a solution like SSIM existed. SSIM has the logic built in that we can do the kind of trending that we're looking for."**

#### William Lidster

Manager of Information  
Security Administration  
Alaska USA Federal  
Credit Union

## Why Symantec?

- ▶ Exceeded stated requirements
- ▶ Easy to demonstrate PCI compliance
- ▶ Easy to configure and maintain
- ▶ Alerts keep member data secure

**“All in all, the consultants from both Structured and Symantec performed very in a very professional manner, and their work has served us well.”**

**William Lidster**

Manager of Information Security Administration  
Alaska USA Federal Credit Union

commonplace in newspaper headlines. Like most organizations, Alaska USA had several layers of security from gateway to desktop, but “we realized that these new threats were going to require more analysis of all these logs,” Lidster remembers.

Alaska USA also wanted to demonstrate compliance with internal standards as well as the increasingly complex standards of the National Credit Union Association (NCUA) and the Payment Card Industry (PCI).

### Going Beyond Requirements

Lidster approached Symantec Partner Structured Communication Systems, Inc., asking for a solution that would take the log data from the firewall, intrusion protection system, antivirus, and other security systems, and put it together into a database for manual analysis. “We wanted to harvest data from the logs,” Lidster recalls, “but didn’t want to run that process on the system that generated the logs, as that would have affected performance.”

Structured showed Lidster’s team two point solutions that met the stated requirements, but also introduced the team to a much more robust solution, the Symantec Security Information Manager (SSIM). The Structured team explained that with SSIM, the credit union could not only download log data into a single database, but also could correlate that data and set up automated reporting, analysis, and alert functionalities.

“We came with a limited requirement set simply because we didn’t know that a solution like SSIM existed,” Lidster explains. “We quickly realized that we could automate what I was going to do myself manually. SSIM has the logic built in that we can do the kind of trending that we’re looking for.”

## SOLUTION AT A GLANCE

### Business Drivers

- Consolidate log data from a diverse security infrastructure
- Demonstrate compliance with NCUA and PCI standards
- Map event monitoring against internal exception policies
- Automate and customize alerts to optimize security response

### Symantec Products

- Symantec™ Security Information Manager

### Symantec Services

- Symantec Consulting Services
- Symantec Essential Support Services

### Symantec Partner

- Structured Communication Systems, Inc. ([www.structured.com](http://www.structured.com))

### Technology Environment

- Server platform: Almost 300 Dell servers running Microsoft Windows Server 2003, with a few assorted IBM AIX and Linux servers
- Applications: Symitar share and loan system; tools for collections, accounting, personnel management, data warehousing, mortgage lending, and trust and insurance services
- Databases: Mostly Microsoft SQL Server 2003; a few proprietary databases on the RS6000 platform

### Business Value and Technical Benefits

- Avoidance of approximately 1,000 employee hours expected per year for manual analysis of security logs
- Enhanced ability to avoid compromising customer data, maintaining Alaska USA’s brand value
- Ability to integrate and correlate log data from the entire security infrastructure
- Ability to demonstrate PCI compliance

## Implementation in a Heterogeneous Environment

Alaska USA made the decision to purchase the Symantec solution in March 2007. Structured assisted with implementation of the base product, and by July, it was deployed to approximately 20 critical servers in two categories—servers with transaction data of interest for PCI compliance, and servers of interest for event monitoring, such as Active Directory domain controllers.

Alaska USA also contracted with Symantec Consulting Services to create custom data collectors for Symantec Security Information Manager for several of the credit union's systems: the card production system and Tandem platform used by Alaska Option, a subsidiary of Alaska USA, as well as the badge access system for Alaska USA's physical facilities.

"The Symantec team wrote and installed the collectors," Lidster states, "and while we had a few delays, most of them were due to resource constraints on our end. All in all, the consultants from both Structured and Symantec performed very in a very professional manner, and their work has served us well."

Lidster and key members of his team now receive customized alerts according to his specifications. "For instance, we get alerts when login attempts are made on two separate accounts from a single, unknown IP address," Lidster explains. "If we investigate and find that it's a public computer at a federal facility where we have members, we add that IP address to the list of trusted sites."

## Realizing Benefits

After almost a year of using SSIM, Lidster is realizing significant business value from the solution. "I estimate that the manual correlation and event analysis that I was planning to do would likely have taken 1,000 hours per year—almost half a headcount," Lidster states. "And as I have gone through this process, I realize that I probably would have abandoned the effort due to its complexity, and having to re-tool every time a new technology is brought in. This would have left the credit union less secure."

Lidster has also realized benefit in the area of PCI compliance. "At the time we were looking for a solution, PCI was not yet requiring that log data collection be separated from the source system," Lidster notes, "but that's a requirement now. SSIM has proven to be a turnkey solution for PCI compliance."

Alaska USA is covered by Symantec Essential Support Services, which provides 24-hour technical support service. "The product is so good that I've not had to use them much to date," Lidster notes.

Finally, though harder to quantify, the enhanced security of member data contributes to brand value and customer loyalty for Alaska USA. "With mortgage companies going bankrupt and data breaches in the news, it's important to do everything possible to protect member data. SSIM helps us accomplish this."

## Looking to the Future

Alaska USA is now in the final stages of purchasing Symantec Endpoint Protection and Symantec Network Access Control as its new standard on desktops and laptops—with Structured providing installation services. "We were impressed with the number of features included in a single console and agent," Lidster says, "and we were also very happy to realize that these products will integrate seamlessly with SSIM."

"Symantec and Structured have been great partners in securing our enterprise," Lidster concludes. "The solution we now have is much more than we asked for, but exactly what we need."