CASE STUDY

AlienVault USM™ Helps Community Bank Secure its Assets and Pass FDIC Audit

Opening its doors in 1893 with $12,000 in capital, the Bank of New Glarus was the first official bank in New Glarus, Wisconsin. Today, the New Glarus banking family includes over 100 employees at six locations who provide personal and commercial banking services to customers in the region, including many from the agricultural industry. Of the bank's approximately 100 employees, two people are responsible for the organization's entire IT infrastructure. To keep their network secure from outside cyber-attacks, the Bank of New Glarus relies on AlienVault Unified Security Management (USM).

In 2015 Patrick Collins, AVP IT/ISO, became one half of the Bank of New Glarus' two man IT team when he was hired as the lead IT manager. After he started, one of his first responsibilities was to find and implement an intrusion detection tool that would help the Bank of New Glarus pass an impending Federal Deposit Insurance Corporation (FDIC) compliance audit.

"Interestingly, the auditor's strongest statement to us was that cybersecurity would be the number one area they were going to focus on to make sure we were in compliance with the regulations. They notified us in advance that we'd be graded on quite a few items we weren't quite prepared for at the time," said Collins.

With less than four months to prepare for the audit, Collins began his search for security software that would help him achieve FDIC compliance. During his search, he considered GFI's LanGaurd as well as SolarWinds Log & Event Manager (LEM). However, after evaluating both, Collins determined that GFI's solution was not a strong enough offering while SolarWinds' product lacked some important features such as Netflow analysis.

The Bank of New Glarus® and Sugar River Bank Branches

Company	Bank of New Glarus
Headquarters	New Glarus, Wisconsin
Industry	Banking
Employee Count	~100
Website	thebankofnewglarus.bank
Solution	AlienVault Unified Security Management (USM) Platform

START YOUR FREE TRIAL ▸

"The FDIC auditors were enthralled by the amount of reports AlienVault USM provides, along with the ability to create custom reports."

- Patrick Collins (AVP IT/ISO)
Lead IT Manager
Bank of New Glarus

During his research of SolarWinds, Collins found a review comparing SolarWinds LEM to AlienVault's USM platform. From the article, Collins felt that AlienVault offered all the features that were included in SolarWinds LEM, but at a more reasonable price. After a few phone conversations and a demo with AlienVault, Collins decided that the product would be a perfect fit for the bank's requirements.

"After seeing AlienVault USM, I felt that it provided all the functionality we needed to help us prepare for and pass the upcoming audit. I also felt comfortable that the product's capabilities would help us detect and respond to future cyber-attacks," said Collins.

"Overall, AlienVault USM has been the best decision I have made. I wouldn't sleep as well without it."

- Patrick Collins (AVP IT/ISO), Lead IT Manager, Bank of New Glarus

In March of 2015, it was time for Bank of New Glarus' compliance audit. Collins had to show the auditors how he was leveraging the AlienVault USM platform to scan their system for vulnerabilities, act on all the reports that came through, as well as track the intrusion alerts that were flowing through the OEM devices.

"We had to prove to the auditors that we were tracking the traffic coming in and out and monitoring for denial-of-service attacks. We also had to prove that we had rules in place that were customized. Nearly all of the information that we provided to them was obtained using AlienVault technology," said Collins.

After reviewing the Bank of New Glarus' environment, Collins said the FDIC auditors were most impressed by the way AlienVault USM takes network data together with log information to generate alerts. They were also enthralled with the amount of reports AlienVault provides, along with the ability to create custom reports. "I actually think they were overwhelmed by all the reports that were provided for them," said Collins. After a week of waiting, the audit report came back and the Bank of New Glarus was informed they had passed the compliance audit with flying colors.

In addition to helping organizations like the Bank of New Glarus meet FDIC compliance, AlienVault USM provides hundreds of built-in compliance reports for managing PCI-DSS, ISO, SOX, HIPAA, GLBA, NERC CIP and GPG13 programs. These reports are automatically updated as asset and vulnerability assessment data changes, allowing users to quickly customize them based on their own compliance priorities.

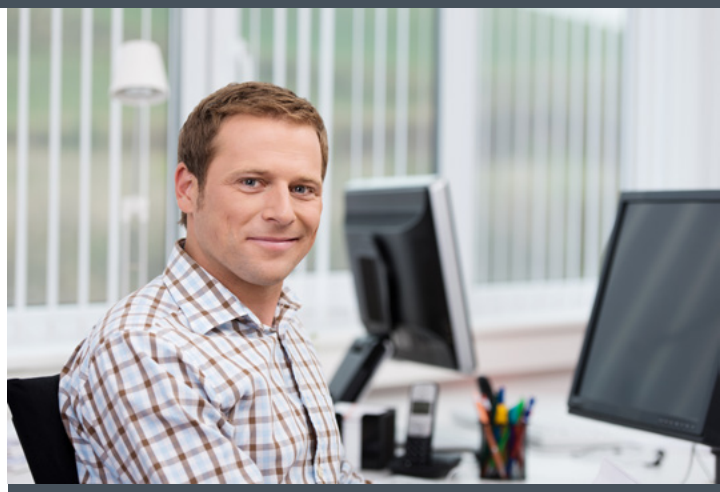
After passing the audit, Collins now finds himself learning new ways to utilize AlienVault technologies, particularly the Open Threat Exchange (OTX) and AlienVault Labs threat intelligence.

The AlienVault Open Threat Exchange™ (OTX) is a global community of threat researchers and security professionals. It includes more than 37,000 participants in 140 countries, who contribute over 3 million threat indicators daily. It provides organizations like the Bank of New Glarus with community-generated threat data that can feed directly into the USM platform. This has allowed them to automate the process of updating their security infrastructure with threat data from any source.

"The fact that many other individuals are contributing threat intelligence in the AlienVault OTX community to make sure that our systems are as updated as possible is really helpful. A lot of the products that I looked at claimed they could provide the same kind of resources, but when I looked more closely, this functionality wasn't truly there or built-in like it is in the OTX platform," said Collins.

The AlienVault USM platform also receives updates every 30 minutes from the AlienVault Labs threat research team. This dedicated team analyzes different types of attacks, emerging threats, suspicious behavior, vulnerabilities and exploits they uncover across the entire threat landscape.

Once the Labs team has discovered threats, they publish AlienVault Threat Intelligence updates to the USM platform in the form of correlation directives, IDS signatures, vulnerability audits, asset discovery signatures, IP reputation data, data source plugins, and report templates.



Key Benefits:

#1 AlienVault USM allowed the Bank of New Glarus to pass their FDIC audit with flying colors.

#2 The Bank of New Glarus selected AlienVault USM because it is a stronger solution than GFI's LanGaurd and offers the same functionality as SolarWinds LEM but at a lower price point.

#3 Instead of spending upwards of 8 hours a week reviewing logs, AlienVault USM saves the Bank of New Glarus hours in the work day by providing easy to understand threat data in a single pane of glass.

START YOUR FREE TRIAL ▸

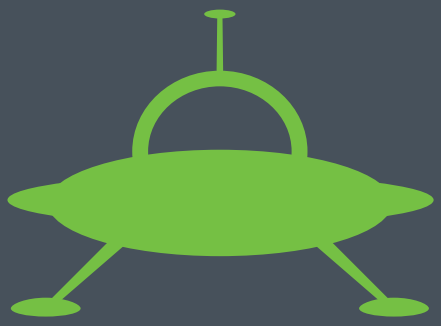
"I have recently started customizing the AlienVault Labs Threat Intelligence based on specific compliance standards we get from the FDIC. Basically, I can customize the AlienVault rules so that we can address the specific items required to meet FDIC compliance standards. That has been a great help, not just by adding rules through the interface, but also by going into the hard file structures and actually being able to complete some things there," said Collins.

Currently, Collins finds himself spending roughly twenty-five percent of each workday on security related tasks. AlienVault USM has allowed him to automate many of his tasks instead of having to manually check in on individual systems, saving him a lot of time.

"AlienVault USM has been a huge time saver. Before USM it was likely we could spend over 8 hours a week reviewing logs. As a two-man shop, that is time that we just don't have. Instead, USM tracks everything coming through the logs on each of our systems, whether it be workstations, servers or networking hardware, it can all be viewed and understood quickly, in one single pane of glass. That has been the biggest benefit for us: being able to gather everything we need to identify security issues from one source," said Collins

Collins has also found how to save time by setting alerts in USM. This helps him avoid having to go through all of his raw data to confirm an attack is not underway.

"The AlienVault USM platform will generate an email alert telling me, 'Hey, you need to look at this log and this system.' It's a huge time saver when you're able to avoid digging into all your individual hardware assets. Overall, AlienVault USM has been the best decision I have made. I wouldn't sleep as well without it," said Collins.



About AlienVault

AlienVault has simplified the way organizations detect and respond to today's ever evolving threat landscape. Our unique and award-winning approach, trusted by thousands of customers, combines the essential security controls of our all-in-one platform, AlienVault Unified Security Management, with the power of AlienVault's Open Threat Exchange, the world's largest crowdsourced threat intelligence community, making effective and affordable threat detection attainable for resource-constrained IT teams. AlienVault is a privately held company headquartered in Silicon Valley and backed by Trident Capital, Kleiner Perkins Caufield & Byers, Institutional Venture Partners, GGV Capital, Intel Capital, Jackson Square Ventures, Adara Venture Partners, Top Tier Capital and Correlation Ventures.

For more information visit www.AlienVault.com or follow us on Twitter (@AlienVault).