CASE STUDY

# Bank of Marin Gains Detailed Visibility into their Network with AlienVault USM

Bank of Marin is a leading business and community bank in the San Francisco Bay Area with assets of over $1.9 billion. Founded in 1989 and headquartered in Novato, CA; Bank of Marin has 21 offices located in San Francisco, Marin, Napa, Sonoma and Alameda counties. The bank provides business and personal banking, commercial lending, and wealth management and trust services.

In early 2015, Bank of Marin's Security team was looking to increase visibility into their network by adding a Host-based Intrusion Detection System to their existing security program. Over the course of their search, they evaluated a number of popular vendors such as Palo Alto, FireEye and Carbon Black. Although each of these products seemed capable of meeting Bank of Marin's need for a HIDS security layer, the team found that the cost of each was too high to justify implementation.

Jeff Dalton is the Information Security Officer at Bank of Marin. In his search for a more affordable product, he spoke with a few members of his CISO group and they recommended that he check out AlienVault's Unified Security Management (USM) platform. When he did, he realized that USM includes HIDS plus much more than he expected.

"When I first looked at the offering, I was surprised to see that it is actually five products in one. I was very pleased to discover that, in addition to intrusion detection, AlienVault USM also includes asset discovery, vulnerability assessment, behavioral monitoring, and SIEM," said Jeff.

"AlienVault USM has performed head and shoulders over the competition because of its rich functionality, low cost, and ease of use."

*–Jeff Dalton, Information Security Officer, Bank of Marin*

After speaking with a few AlienVault account reps and exhaustively researching competitive security products, the Bank of Marin team decided that they would move ahead with implementing USM, confident that it was a cost-effective solution that would meet their HIDS needs and also provide many additional capabilities.

When Bank of Marin acquired USM they also purchased the five-day AlienVault beginner's training course. Jeff found this training to be a huge help in jump-starting the install of the product and allowing him to be able to take advantage of the product's features immediately.

"The course helped me better understand all that USM has to offer. With the training, I've been able to easily use a few of the tools that are available. However, eventually I'd like to go more in-depth with training on how to correlate the events and alarms. I think I'll continue to evolve with the product but it will just take time," said Jeff.

**Company name:** Bank of Marin

**Industry:** Banking

**Headquarters location:** Novato, California

**Employee count:** 201-500

**Website Link:** www.bankofmarin.com

START YOUR FREE TRIAL ▸

Since purchasing AlienVault USM and incorporating it into his existing security system, Jeff says that he has successfully increased visibility into his network and also addressed Bank of Marin's missing HIDS security layer.

"I'm really pleased that USM allows me to have greater visibility into my network. 99 percent of the time the threat alerts it generates are false positives, which is as it should be, and that is fantastic. It's been a great tool to help us identify anomalies and overall it aids my understanding of what is going on in the enterprise network at Bank of Marin, which is exactly what I was looking for in this product," said Jeff.

When researching anomalies at Bank of Marin, Jeff relies on AlienVault's global open threat intelligence sharing community,

"Nine times out of ten what I tell people looking for a security solution is that when it comes to security, with AlienVault USM I can do it all, which is fantastic."

–Jeff Dalton, Information Security Officer, Bank of Marin

the Open Threat Exchange (OTX). He said that although he hasn't found too many malicious events yet, the information that OTX provides about USM alerts is very useful.

"The information in OTX helps me to effectively prioritize threats from high to low. That in turn allows me to spend more time analyzing events that are deemed higher priority. It's also educating me about what kind of threats security professionals are observing around the world. Many of the actual alerts OTX is sending allow me to also take preventative measures. Even if I haven't seen any of the traffic, I am able to look at what malicious actors are doing, and then actually close malicious IP addresses," said Jeff.

One of the busiest times of the year for Bank of Marin's security team is during months that typically have high retail sales, like November and December. This is due to the high volume of financial transactions that their customers make during these months. "We find that hackers like November and December because there are so many transactions. That in turn makes finding their malicious actions more like finding a needle in a haystack," said Jeff.

## Key Benefits:

#1 - AlienVault USM's HIDS functionality allows Bank of Marin greater visibility into activity on their network.

#2 - Although Bank of Marin were only in the market for a HIDS solution, they were pleased to find AlienVault USM is actually five security products in one.

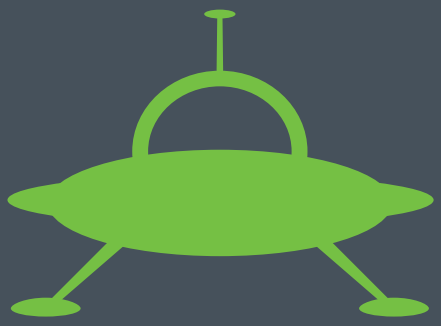
#3 - During busy retail months, Bank of Marin saves a large amount of time researching threats because of AlienVault USM's functionality.

START YOUR FREE TRIAL ▸

Before using AlienVault USM, Bank of Marin was spending a large amount of time having to monitor the increased number of transactions during this time period. However, with USM they've found it much easier to be alerted and be provided with detailed information on anomalies that occur, saving them time from having to manually dig into data and ensuring the environment is safe.

Overall, Jeff has found that "AlienVault USM has performed head and shoulders over the competition because of its rich functionality, low cost, and ease of use," and it has greatly improved the efficiency of his small security team.

"Nine times out of ten what I tell people looking for a security solution is that when it comes to security, with AlienVault USM I can do it all, which is fantastic. Plus, I personally have two other jobs to do as well.  AlienVault USM is easy to deploy, easy to maintain, does exactly what you want it to do, and you don't have to have an army of 4 to 6 different analysts trying to figure things out," said Jeff.



## 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).