



CASE STUDY

Crosskey Gains Complete Security Visibility with AlienVault USM™

About Crosskey

Crosskey is a Finnish company that develops, delivers and maintains systems and solutions for Nordic banks and capital markets. Customers range from small and regional banks to the third largest bank in Finland. Altogether, Crosskey deals with the management of over 3 million banking customers (half of Finland's population) in the Nordic region.

Unlike many other actors in the Nordic region, Crosskey develops and maintains its own banking system. Due to the system's modular form, it can adapt it to specific customer needs and offer solutions that match the needs of all companies that operate banking businesses, whether the company is an actual bank, insurance company or retail business.

Crosskey's mission is to make it easier and more profitable for customers to operate a bank and focus on their core business activities. This includes support for processes and innovative IT solutions that embrace all components in a banking system, regardless of the distribution channel being used.



"It became more challenging the more logs we had and when you deal with critical systems, you want to be finding issues in minutes and seconds rather than hours or days."

*-Kim Halavakoski, CSO,
Crosskey Banking Solutions*

Challenges

When it came to the security of the systems it runs, Crosskey had been outsourcing that aspect to an MSSP. But it was constantly challenged by the increasing amounts of log volumes - likely running into the millions of lines each day in a banking system environment. Coping with these log increases and doing it in a cost-effective way was becoming difficult with a third party service provider.

Furthermore, as a service provider itself, Crosskey wanted to reduce the chain and amount of information being sent back and forth to a third party, thus helping its systems to achieve PCI DSS compliance.

As a banking system provider with three datacentres and a lot of servers, it was becoming unfeasible to push all of the infrastructure logs to a third party for correlation.

"It became more challenging the more logs we had and when you deal with critical systems, you want to be finding issues in minutes and seconds rather than hours or days," said Halavakoski.

In addition, Crosskey did not want to lose the broad threat intelligence view its MSSP provided for detecting "known badness", but equally it could not rely on an external partner any more to facilitate this, so the solution had to provide this intelligence.



Customer Profile

Company: Crosskey Banking Solutions

Industry: Financial Services

Country: Finland

Employees: 200+

Website: <https://www.crosskey.fi>

START YOUR FREE TRIAL ▶





Solution

To forgo reliance on a third party for security, Crosskey decided to take its security services in-house. This would help increase security and privacy for Crosskey customers as well as help it meet PCI DSS compliance requirements more easily.

After researching a number of options, Crosskey selected AlienVault Unified Security Management (USM), due to its many features, in particular the threat intelligence and OTX integration, gave it the edge over the competition. USM is a platform that combines five essential security capabilities (including asset discovery, vulnerability assessment, threat detection, behavioural monitoring and security intelligence) in one easy to use console, giving the business complete security visibility as well as meeting compliance requirements and providing invaluable threat intelligence across all of its environments.



“By using AlienVault’s Unified Security Management platform, with its correlation engine and threat intelligence, we were able to save on both of these fronts while still delivering effective security.”

-Kim Halavakoski, CSO, Crosskey Banking Solutions

Benefits

The very nature of managing financial systems for customers meant that there were a vast amount of logs to go through and keep pushing to a third party provider. By taking the security in-house and installing AlienVault’s USM platform, Crosskey could improve the security and visibility and use a much smaller security team and still deliver superior security in its own systems that are now PCI compliant.

The solution provides consolidated log management, consolidated security event and incident management, real time threat analysis and real time event and incident analysis, all with configurable alerting. With AlienVault, Crosskey could correlate all logs, not just IDS logs but Unix, Windows, system and firewall logs as well giving the security team a more complete security view.

Halavakoski expects that in the future, breaches on payment systems will continue to be a problem and coping in “finding badness” from environments will become more and more difficult. Therefore, security products that incorporate threat intelligence, like USM, will gain importance.

“Intrusions can happen in minutes, but detection can sometimes take months. We can defend our networks one by one or we can collaborate and share information,” he said. “It’s easy enough to say, harder to implement, but finding a way is the only way to cope with the sheer amount of threats.”

Key Benefits:

#1 - Crosskey selected AlienVault Unified Security Management (USM) due to its many features, in particular the threat intelligence and OTX integration gave it the edge over the competition.

#2 - By taking the security in-house and installing AlienVault’s USM platform, Crosskey was able to improve security and visibility, use a much smaller security team, and still deliver superior security in its own systems that are now PCI compliant.

#3 - With AlienVault, Crosskey was able to correlate all logs, not just IDS logs but Unix, Windows, system and firewall logs, as well as give the security team a more complete security view.

START YOUR FREE TRIAL ►