ALIEN VAULT

CASE STUDY

# Defending the Enterprise from Cyber Attacks

We've seen several cyber attacks occur over the course of 2014 – from Home Depot to Target and most recently Sony. The one thing I think most of us in the industry can agree on is that we don't want to be the next company in headlines marked by a breach.

As the information security administrator of Save Mart Supermarkets, a California corporation that owns and operates 220 stores in Northern California and Northern Nevada, I've quickly learned that when it comes to cyber attacks, it's not a matter of "if," but rather "when" you should expect to be breached these days. With that, the focus needs to shift from pure prevention strategy to detection and response planning – the goal being to become a resilient organization that can bounce back quickly from an attack. In addition, by keeping security top of mind within your organization, sharing threat data, educating employees and deploying the right tools to match your organization's needs, you have a better chance at protecting it.

Having the right security technology in place gives you visibility into the enterprise and allows you to monitor traffic through servers before an attack happens, rather than after, when you're apologizing to consumers for your breach. With the right tools in place, you can see when an attack happens, and you're given an opportunity to react to it.

"With the right tools in place, you can see when an attack happens, and you're given an opportunity to react to it."

*–Stephen Molina, Information Security Administrator*

SAVE MART SUPERMARKETS

**Company name:** Save Mart Supermarkets

**Industry: Primary:** Supermarket

**Secondary:** N/A

**Headquarters location:** Modesto, CA

**Employee count:** 213 Stores

**Website Link:** www.savemart.com

START YOUR FREE TRIAL ▸

At Save Mart, we use the AlienVault Unified Security Management (USM) platform, which is an easy-to-use, affordable solution that enables us to effectively defend against today's evolving threat landscape. USM has an Open Source Host Intrusion Detection System (HIDS) known as OSSEC built-in for file integrity monitoring and log collection. OSSEC is particularly key as an agent on all point-of-sale (POS) systems and serves to provide a 360-degree view of what's happening on the systems. With OSSEC, we can watch users who access the machines and their patterns of access, see attempted exploits, scan the system, and determine changes made to critical files and registry entries in Windows. OSSEC also notifies us if files are being modified – as the IT or security team tends to know which files should allow for modifications and which ones don't. File modification can be a telltale sign that a system has been compromised.

AlienVault USM has a number of built-in tools, including Snort/Suricata that provides visibility and intrusion detection at the network level. It also includes behavioral analysis with its Netflow integration capabilities. USM also includes a fully functional Security Information and Event Management (SIEM) to provide log file aggregation and correlation, as well as a vulnerability management system.

The SIEM allows all the individual functions in AlienVault to be put into context and operate as a collective whole. The Save Mart implementation uses the Host IDS functionality to the greatest degree. Once it's installed on a machine, it monitors the machine and communicates with the server – not to mention, it's extremely useful and easy to set up.


"At Save Mart, we use the AlienVault Unified Security Management (USM) platform, which is an easy-to-use, affordable solution that enables us to effectively defend against today's evolving threat landscape."

– Stephen Molina, Information Security Administrator

We also use AlienVault's Open Threat Exchange (OTX) because it gives us a good idea of where threats are coming from within our organization, which is often difficult to pinpoint. Threats and attacks come from all over the world - China, Russia, Europe and here in the U.S., too. In many cases, OTX helps our team focus on what we need to pay closer attention to and

what we need to be watching for. The ability to see threat trends occurring in the world at-large combined with AlienVault's

tools allows us to better protect the business by alerting security teams to emerging threats immediately.

Another way to approach security is to understand the ways damage can be minimized. The majority of security has to do with people. It is a people problem, and the first step to be successful is to educate users. Let employees know what they need to do to protect themselves, their information, their devices and data, and also, what they need to avoid.

Think about your first line of defense being education. If employees are bypassing tools, or working around security parameters, security can't be successful. Implement security tools that encourage employee buy-in and are easy to use and teach them why that's important. It's a mistake to think that a cyber attack won't happen to you or your company, but the first step to attempt prevention is education.

## Key Benefits:

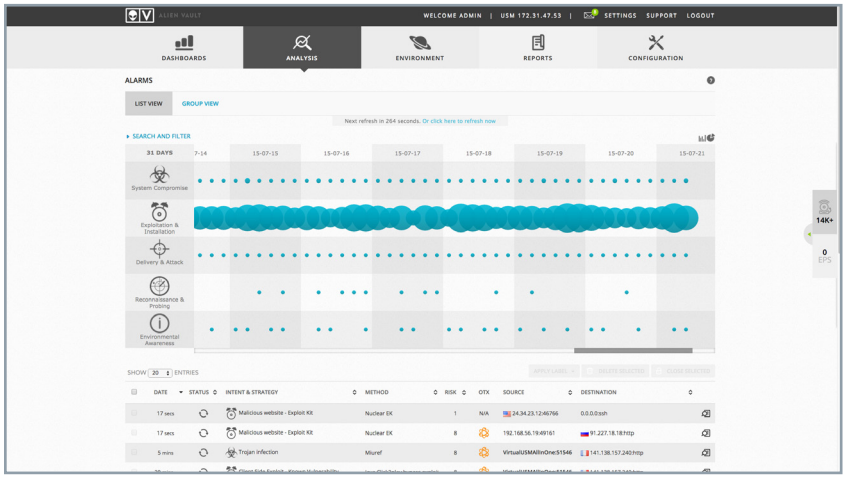
#1 - Save Mart uses AlienVault's Open Threat Exchange (OTX) to identify where threats are coming from within their organization, which ones they need to pay close attention to, and what they need to be watching for.

#2 - Threat Intelligence from AlienVault USM gives Save Mart the visibility needed to collect information from different devices and network traffic and put it all into context, allowing them to react to attacks before they become disastrous.

#3 - Save Mart uses AlienVault USM's Host Intrusion Detection System (HIDS) for file integrity monitoring and log collection, providing them with a 360-degree view of what's happening on their systems.

START YOUR FREE TRIAL ▸

All in all, security is getting a lot tougher as attacks are becoming more sophisticated. Some argue that as technology advances, it is also becoming a little easier – but security isn't like other fields. We're up against other people, not just nature – and these people [or hackers] are not static. If we develop a strong strategy on the defensive technology side, the bad guys aren't going to sit back and relax. Their attack techniques are going to evolve.




START YOUR FREE TRIAL ▸

Security is an adversarial environment and there will always be something new in the works. That's where the threat intelligence we glean from AlienVault's USM gives us the visibility we need and ability to collect threat information from different devices and network traffic and put it into context. Once we have that information, we can then compare it with other data to evaluate network traffic and activity. That provides us with the ability to react to attacks before they become disastrous.

As a retailer, there are lots of transactions on the POS system side, and if you're anything bigger than a mom-and-pop shop, you have thousands of transactions everyday. My advice to other folks on the retail front – and really anyone in the industry – is to take security seriously. You're going to need to get ahead of cyber attacks and implement systems that encourage employee buy-in and usage but mainly protect the business and its bottom line.

*To read more about how Stephen Molina protects Save Mart Supermarkets' networks, read his story, recently featured in Baseline Magazine.*

## About AlienVault

AlienVault's mission is to enable organizations with limited resources to accelerate and simplify their ability to detect and respond to the growing landscape of cyber threats. Our Unified Security Management (USM) platform provides all of the essential security controls required for complete security visibility, and is designed to enable any IT or security practitioner to benefit from results on day one. Powered by threat intelligence from AlienVault Labs and the AlienVault Open Threat Exchange—the world's largest crowd-sourced threat data network — AlienVault USM delivers a unified, simple and affordable solution for threat detection, incident response and compliance management. 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).