CASE STUDY: SUNRISE IDENTITY

TOP BRANDS REQUIRE PCI COMPLIANCE AND THREAT DETECTION

With Fortune 500 customers from Microsoft and Starbucks to Nike and GameStop, security and compliance cannot be a second thought. For many of their largest clients, Sunrise Identity develops and hosts e-commerce stores or employee/partner portals leveraging credit card payment processing and mandating PCI DSS compliance requirements. Sunrise Identity needed to achieve PCI DSS compliance as well as make sure the company is operating under security best practices. So PCI compliance was a given and the right security solution was a necessity.

To address their security and compliance mandates, they first identified key capabilities that would address requirements: Log management, vulnerability scanning, and intrusion detection. Initially, the team attempted to address this internally with a homegrown solution to store and maintain log files, but this was too time intensive and was not cost effective to tie-up limited resources in-house. Most importantly, the team was spread thin. The Sunrise team searched for options and first learned about Alert Logic from a PCI consultant. As one of four vendors suggested for consideration, Alert Logic's Log Manager and Threat Manager proved to be the best solution as it is fully managed, delivered as-a-service, addresses key PCI DSS compliance mandates and can work in hybrid IT environments. Other solutions required a large capital outlay, professional services, and/or multiple vendors to address the same.

"Maintaining a high level of security and compliance is part of our brand – we want our customers to have great confidence in doing business with Sunrise Identity," said Bob Stahr, Director of Information Systems. Sunrise Identity's business is growing on an exponential scale so they must focus their IT personnel on their core business to support growth and strategic projects.

sunrise identity

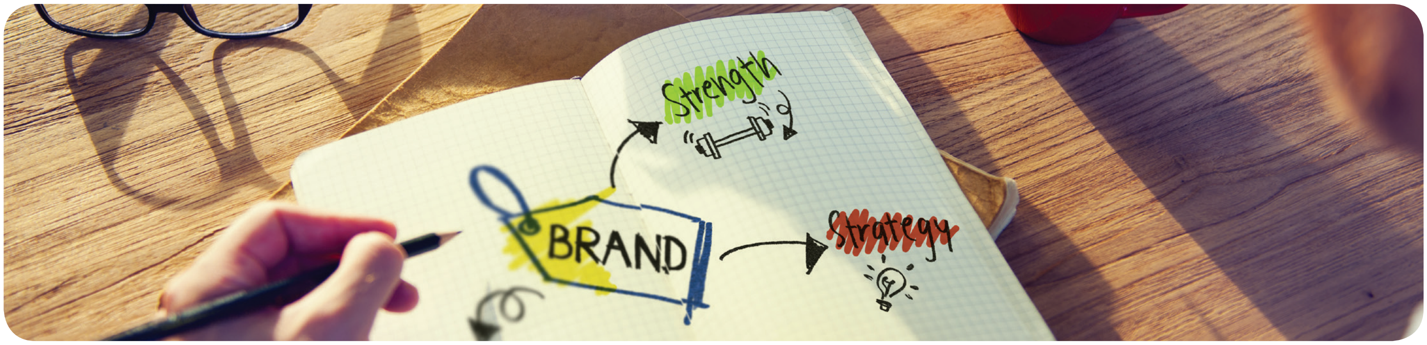
ABOUT

For over 35 years, Sunrise Identity has provided end-to-end solutions from product design, e-commerce stores, to delivery and beyond. Developing custom manufactured branded merchandise; Sunrise Identity works with the biggest brands in the USA and delivers world-class promotional marketing materials from uniforms to employee recognition programs.

SOLUTIONS

Alert Logic Threat Manager with ActiveWatch: Managed intrusion detection and vulnerability scanning system

Alert Logic Log Manager with ActiveWatch: Managed daily log review service



With the Alert Logic solution, Stahr's team receives alerts and escalations from Alert Logic's 24 x 7 Security Operations Center (SOC) when incidents are identified in real time. PCI vulnerability scans are run on a regular basis and any issues or risks that are identified are remediated with the help of the Alert Logic SOC. Sunrise is also able to run pre-built PCI compliance reports to prepare and support PCI audits and can perform log and event research when there is a perceived threat or issue. This proactive protection and notification from Alert Logic gives Sunrise Identity the right level of protection at a fraction of the cost of building and maintaining it in-house.

> *THIS IS AN ONGOING TIME-SAVER AND WE'VE SEEN A SUBSTANTIALLY HIGH ROI SINCE FIRST PURCHASING THE SOLUTION IN 2009. WE STRIVE TO WORK SMARTER AND WE'VE FOUND THAT ALERT LOGIC HELPS US DO THAT.*
>
> - Bob Stahr, Director of Information Systems

CHOOSING A HIGH ROI AND PRACTICAL RESULTS

A benefit of subscribing to a managed service was that the time to implement the solution was short. The Alert Logic team did much of the work in collaboration with the Sunrise team. Alert Logic Threat Manager and Log Manager protects the primary datacenter, remote offices, as well as Amazon Web Services (AWS) deployments. Once implemented, the solution's positive results were seen almost immediately. Their choices have translated into practical results within the Sunrise Identity environment. External vulnerabilities have been identified and remedied through vulnerability scanning. Specific attack vectors identified through Alert Logic's Threat Manager have been subsequently closed off in the firewall. Searching log events with Alert Logic's Log Manager helps eliminate false positives and determine if certain attacks have been successful. They even use Log Manager to trouble shoot certain Active Directory issues such as the source of user lockout problems. Another reason they use Alert Logic is for aggregating data into one view. "This is an ongoing time-saver and we've seen a substantially high ROI since first purchasing the solution in 2009," said Stahr.

WORKING SMARTER

Sunrise Identity believes in working smarter. The advice Stahr gives to anyone looking for security solutions is to buy something that requires as little onsite setup as possible. Virtual appliances or plug and play, vendor managed hardware is the key. Avoid solutions that require local hardware/software management and never roll your own. Buy something with a quick log search. Even the lowest tier of events/seconds produces millions of records per day. Finding a needle in a haystack is difficult enough, you don't want to wait for hours to find your query was too specific or too broad. "We strive to work smarter and we've found that Alert Logic helps us do that," said Stahr.

ABOUT ALERT LOGIC

Alert Logic, the leader in security and compliance solutions for the cloud, provides Security-as-a-Service for on-premises, cloud, and hybrid infrastructures, delivering deep security insight and continuous protection for customers at a lower cost than traditional security solutions. Fully managed by a team of experts, the Alert Logic Security-as-a-Service solution provides network, system and web application protection immediately, wherever your IT infrastructure resides. Alert Logic partners with the leading cloud platforms and hosting providers to protect over 3,000 organizations worldwide. Built for cloud scale, our patented platform stores petabytes of data, analyses over 400 million events and identifies over 50,000 security incidents each month, which are managed by our 24×7 Security Operations Center. Alert Logic, founded in 2002, is headquartered in Houston, Texas, with offices in Seattle, Dallas, Cardiff, Belfast and London. For more information, please visit www.alertlogic.com.

ALERT LOGIC®