Case Study

Securonix Selected SafeLogic to Integrate Fully Validated FIPS 140-2 Encryption

SafeLogic

SECURONIX

The Background

Securonix is the industry's first purpose built security intelligence platform that connects and transforms all areas of security management through advanced analytics and actionable intelligence. They provide the industry's first signature-less Behavior Based Threat Detection technology as well as the industry's first risk based access outlier detection technology and fuzzy logic based identity correlation engine. In other words, Securonix is extremely good at locating potential threats and enabling security teams to take action.

Securonix works through identity context, behavior risk analysis, enterprise application level monitoring, data driven link analysis and visualization to mine, enrich, and transform event information through advanced analytics to continuously identify the highest risk users, systems, accounts, and activity for immediate action in real time.

The Challenge

Securonix relies upon data to determine potential anomalies. Tons of data, in fact. Billions of events every day, each with their own unique context, provide Securonix platforms with the necessary insight to identify disruptions. The massive amount of processed information fuel the engine, allowing Securonix to detect mismatches in identity, access, behavior, location, device, or a combination of factors.

Of course, the Securonix platform must be entirely secure. Consider how dangerous it would be to grant access to the entire database to the wrong individual. Imagine the havoc that would be created by a malicious entity with knowledge of each data point and their typical correlation. If that is manifested with spoofed access and unauthorized viewing of internal corporate information, it may cost a company millions, if not billions, by sacrificing their competitive advantage. In the case of a federal agency, if a government operative is identified by cross-referencing their device and location, or a planned military action is exposed, the cost may be calculated in lives.

In addition, Securonix leverages a unique methodology to insure the privacy of their clients' end users. During day-to-day monitoring, individual data is anonymized. This step is seemingly simple, but actually carries a particularly delicate significance. It insures the privacy of the users and shields the security team from scrutiny, as they assess each potential threat on individual, anonymous, data-driven parameters. Whether it is the night janitor or the CEO, the end user's behavior must be evaluated without prejudice.

Because the Securonix platform can identify behavioral patterns of disgruntled employees, authorized but malicious users, and potential flight risks, there are contextual cues that are inherently important to the proper identification of threats. Bluntly, there cannot be sirens and flashing lights every time a user gets flagged for further inspection. These matters must be handled with discretion, so Securonix insures the anonymity of end users up to the point of consensus on the client's security team for the need to escalate. Only at this point is the user unmasked. This feature reinforces the importance of validation encryption for both internal and external needs in the platform.

Securonix Needed Validated Crypto

The demographic that licenses the Securonix product is extremely focused on security and demands the credibility and peace of mind that can only be provided by laboratory tested, NIST validated cryptography. SafeLogic's CryptoComply module and RapidCert service accelerated this process and provided the elusive FIPS 140-2 checkmark in a fraction of the anticipated timeline.

CryptoComply Met Mandate

Securonix engineers faced an impossible task - answering COO Chris Bell's call for FIPS 140-2 validation in the near future, while still meeting all other roadmap goals. The ease of CryptoComply's drop-in architecture allowed the team to integrate quickly and get back to their core tasks while RapidCert handled the rest.

SafeLogic

The Challenge (continued)

These high stakes and dire consequences for compromised data in highly sensitive deployments led Securonix COO Chris Bell to seek fully validated FIPS 140-2 encryption.

“The Securonix platform and database must be completely locked down and encrypted to the highest standard,” said Bell. “Our priorities are clear – customer data integrity comes first, and we needed to hit NIST’s benchmarks to demonstrate our commitment.”

By carrying a CMVP certificate, showing satisfaction of NIST’s FIPS 140-2 standards, Securonix would maintain its brand integrity and boast a competitive differentiator that was beyond reproach. But how would this team of security specialists allocate the resources needed to complete the initiative?

The Solution

Securonix benefited immediately from SafeLogic’s expertise in validated encryption. With the help of SafeLogic’s technical team, Securonix engineers easily integrated the CryptoComply module into their solution. CryptoComply has been fully tested and validated by NIST to FIPS 140-2 standards, so Securonix was able to immediately leverage SafeLogic’s documented compliant encryption. Other open source and proprietary encryption modules have been validated through the CMVP, but only SafeLogic’s support contract guarantees that client integrations will maintain compliance for FIPS 140-2 standards.

For the next phase, Securonix exercised their option for RapidCert, SafeLogic’s unique certification offering. It is the only turnkey validation process in the industry. By using RapidCert, Securonix did not need to contract with any experts or consultants. They didn’t need to hire any additional developers or specialists. They did not assign any of their valuable engineers to the effort. They didn’t have project managers, overhead, or really even any stress. SafeLogic handled the entire testing and validation process from end to end. Even better, it was at a fixed cost for Securonix and was nearly 12 months faster than originally estimated by consultant bids.

“Our experience with SafeLogic has been beyond expectations,” said Bell. “We saved a ridiculous amount of time, while avoiding stress and cutting both hard and soft costs! We didn’t have to compromise on anything and are now the proud owners of FIPS 140-2 certificate number 2094.”

Chris Bell
COO. Securonix

> **“We saved a ridiculous amount of time, while avoiding stress and cutting both hard and soft costs!”**

SECURONIX

About Securonix

Securonix is working to radically transform all areas of data security with actionable security intelligence. Their purpose-built advanced security analytics technology mines, enriches, analyzes, scores and visualizes customer data into actionable intelligence on the highest risk threats from within and outside their environment.

SafeLogic

About SafeLogic

SafeLogic Inc. was established in 2012 to reduce the time and complexity of integrating and validating world class encryption. Spun out from Apex Assurance Group, which has provided FIPS 140 consulting services to top companies for nearly a decade, SafeLogic delivers innovative security, encryption, and FIPS validation to applications for mobile, wearable, server, appliance, and constrained device environments.

SafeLogic is privately held and is headquartered in Palo Alto, CA.

SafeLogic Inc.
530 Lytton Ave, Suite 200
Palo Alto, CA 94301
(844) 4-ENCRYPTION
@SafeLogic
info@SafeLogic.com
www.SafeLogic.com

You needed SafeLogic six months ago.