Case Study

Vectra Networks Chose SafeLogic's FIPS 140-2 Encryption to Accelerate Federal Sales

SafeLogic

VECTRA®

The Background

Cyber attacks and data breaches have become all too common today and IT security teams are scrambling to find ways to stop them. Vectra Networks was launched to fill this void, offering automated, real-time detection of active cyber attacks.

Today's sophisticated cyber attackers easily evade perimeter security systems – firewalls, malware sandboxes and IDS/IPS – and infect host devices inside networks. Vectra closes this security gap by detecting the behavior of attackers who attempt to spy, spread and steal. Leveraging a unique combination of data science, machine learning and behavioral analysis, Vectra detects threats in all critical phases of an attack – command and control, botnet monetization, internal recon, lateral movement and data exfiltration.

Vectra consolidates and scores detected threats, maps them to the hosts under attack, and prioritizes the ones that pose the highest risk. This enables security teams to respond to threats with unprecedented speed, accuracy and efficiency.

The Challenge

While Vectra grew its customer base in private sector verticals such as utilities, media and higher education, it was simultaneously focused on tackling the federal market. When it comes to purchasing power and demand from departments and their agencies, the U.S. government is the world's largest and most influential cyber security customer.

To reach its goal of earning federal business, Vectra partnered with AS Global, a leading systems integrator that specializes in federal markets. However, one hurdle remained for Vectra – NIST certification.

"FIPS 140-2 validation is required for encryption in software solutions that are procured, deployed and utilized by the U.S. government," said Jason Kehl, vice president of engineering at Vectra Networks. "Despite our strong commitment to FIPS 140-2 encryption, we had concerns about the time and effort that the validation process would involve."

Vectra Needed FIPS 140-2 Quickly

Vectra Networks partnered with AS Global to open doors and create opportunities for sales in the public sector. However, without FIPS 140-2 validated encryption, Vectra could not qualify for U.S. Federal deployments. Every day that passed without the mandatory cryptographic certification was a day that government agencies might select a competing solution. This was the final hurdle and time was of the essence.

RapidCert Delivered

SafeLogic's product line of CryptoComply encryption modules are designed for simple and fast installation. The drop-in architecture allowed the Vectra Networks team to integrate quickly and get back to their core tasks.

Meanwhile, the SafeLogic team handled the RapidCert process. This resulted in a full FIPS 140-2 Level 1 validation within weeks of signing a contract, accelerating Vectra's federal sales timeline and requiring zero additional effort from Vectra. SafeLogic handled all of the documentation, testing and coordination, from start to finish.

The Solution

Vectra selected SafeLogic to provide both the cryptographic libraries and FIPS 140-2 validation services for their flagship product. With SafeLogic's help, the process took only a few hours of effort from the Vectra team and the validation was complete after less than three months of waiting.

"By achieving FIPS 140-2 validation, Vectra has opened the doors to federal procurement officers," said Kehl. "Even better, we did it with SafeLogic's encryption modules, which enabled to us to reduce the time, cost and complexity of validating our solution for federal markets. Needless to say, the Vectra team is very pleased."

Vectra licensed SafeLogic's CryptoComply module, which contains the algorithms needed to encrypt all data. It also includes RapidCert, the unique process in which SafeLogic's team handles all the testing, coordination and paperwork to compress a typically 12-18 month timeline.

Vectra's validation was posted on September 17, 2015 and displays tested operating environments that include SUSE Linux Enterprise 11 SP2, CentOS 6.3, and Red Hat Enterprise Linux 6.3.

"By achieving FIPS 140-2 validation, Vectra has opened the doors to federal procurement officers. Even better, we did it with SafeLogic's encryption modules, which enabled to us to reduce the time, cost and complexity of validating our solution for federal markets."

Jason Kehl
VP of Engineering at Vectra Networks

VECTRA®

About Vectra Networks

Vectra Networks is the leader in real-time detection of in-progress cyber attacks. The company's automated threat-management solution continuously monitors internal network traffic to pinpoint cyber attacks as they happen. It then automatically correlates threats against hosts that are under attack and provides unique context about what attackers are doing so organizations can quickly prevent or mitigate loss. Vectra prioritizes attacks that pose the greatest business risk, enabling organizations to make rapid decisions on where to focus time and resources. Vector's headquarters are in San Jose, California, and it has European operations in Zurich, Switzerland.

SafeLogic

About SafeLogic

SafeLogic's product line is focused on standards-based cryptographic engines designed for use in mobile, Cloud, server, wearable, IoT, workstation, and appliance environments. SafeLogic modules include RapidCert, the industry's only FIPS 140-2 validation service that provides a certificate in the customer's name, while drastically accelerating the timeline, requiring no additional engineering effort, zero interaction with testing labs, and at a fixed cost.

SafeLogic was established in 2012, is privately held, and is headquartered in Palo Alto, California.

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.