STERNUM

USE CASE

Reducing Customer Security Liability with Limited Overhead

Main challenge

Finding an embedded security solution to reduce security liability with as little overhead as possible

Sternum solution(s) chosen

- Embedded Integrity Verification (EIV™) security technology for IoT

COMPANY TYPE

International Manufacturer of Vision Systems, Software, and Sensors

INDUSTRY

Manufacturing Automation

DEVICE TYPE

Machine Vision System

LIFECYCLE STAGE

Production

BACKGROUND

A manufacturer of machine vision systems used in a host of applications in automated manufacturing to inspect and identify parts, detect defects, verify product assembly, and guide assembly robots was looking for a product security solution for one of their vision systems. This particular vision system is used to identify defective or deficient products in an assembly line in real time in order to remove the defective products. It is part of a greater system comprising many moving parts that work together to identify and remove the deficient products. Therefore it is imperative that there is no delay in the performance of the vision system, otherwise the performance of the greater system will be affected. This Company also understood that to remain the leader in the industry, it has to pay attention to product security as it is of great concern both to its customers and to IoT regulators. Implementing a runtime protection solution would allow them to differentiate themselves from the competition, ensure regulatory concerns, and broaden assurance with their customers.

THE CHALLENGE

Embedding Security with Minimal Overhead

This Company was concerned about security as the industrial control and critical manufacturing industries are increasingly falling victim to cyberattacks. Strengthening their security posture and ensuring secure-by-design principles, while keeping their extremely sensitive devices unburdened from any performance impact was a challenge. The acceptable solution needed to keep chip performance impact below <4 %, thus options were limited.

SOLUTIONS

Results in Real Time

Demonstrate a forward-leaning approach to security that keeps customers confident their purchase will be forward-compliant, as IoT regulations are moving fast, especially in the EU. Meet strict performance requirements to keep their systems moving in real-time. Sternum's agentless end-point protection and response solution provides auto-mitigation of zero-day threats throughout the product lifecycle. Threats include Memory attacks, integrity of execution flow, command injection, and software supply chain threats.

BUSINESS IMPACT

Liability Reduction

Sternum's security solution was implemented to mitigate the Company's liability. Customer agreements typically stipulate that the supplier bears liability in the event of a security breach. By offering a more cyber-secure device, the Company provides customers with the option to invest in enhanced security, thereby potentially reducing the supplier's liability. If customers opt for the additional security, the supplier's liability may be further diminished.

No Performance Overhead

A POC was conducted to ensure the security and performance of a vision system used in assembly line detection. Over the course of over 800 tests, Sternum was able to demonstrate that they provide runtime protection without hindering the real-time nature of these systems.The biggest question was if Sternum could keep overhead as low as possible, and the Company found it remarkable how little overhead was added. Because the vision systems work in real-time, any additional lag will affect the product and the entire system from working as required.

Faster Time-to-Market

By integrating Sternum's EIV security solution, the Company leverages Sternum's compliance certifications, including the prestigious Diamond rating in UL's Security IoT Device Security Rating system. This rating is aligned with various industry frameworks and regulations such as ETSI TS 103 645, NIST IoT Cybersecurity Capabilities Baseline, EU Cybersecurity Act, among others. This allows the company to accelerate its regulatory approval processes, reducing the time and resources required to bring its future products to market while ensuring robust security standards were met.

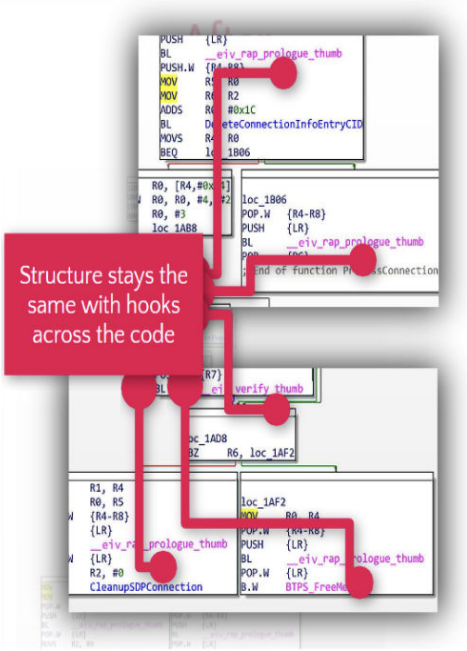
Security as a Market Differentiator

Incorporating Sternum's security solution, the Company bolstered its security posture, a move that has since influenced its go-to-market strategy. This enhanced security strength is now becoming one of their key selling points, allowing the Company to attract new customers seeking robust security measures. By leveraging Sternum's technology, the Company is differentiating itself in the market, showcasing a commitment to cybersecurity that has been resonating with potential clients. This strategic approach not only attracts new customers but also reinforces the Company's position as a leader in providing secure devices.

Sternum Features Used in this Use Case

EIV™ Runtime Protection

(EIV™) runtime protection is part of Sternum's full-stack IoT platform, offering a wide range of on-device security, threat detection, and monitoring capabilities.
Using patented technology, EIV™ leverages binary instrumentation to deploy verification checks across all exploitation paths. This deterministically prevents all code and memory manipulation attempts, including third-party code, assuring system integrity at all times.
Deployed as part of your build, EIV™ seamlessly integrates with all development, testing, and deployment processes, providing agentless in-code security with near-zero overhead and no reliance on external communication.



Learn more about EIV™ >>

Learn more about Sternum Platform >>