INTRODUCTION

Boundary offers a smart intruder alarm, built to UK & European standards, which can be remotely monitored with a smartphone. The product can be adapted to suit individual needs, from the number of sensors required to installation options.

Supporting integration with other products in the home, including Amazon Echo, Google Home, and smart home systems, Boundary acts as the central hub to home security. The solution’s cutting-edge technology supports a simple, clear, process of three tiers of monitoring. It includes self-monitoring via a user-friendly app and a keyholder response which will immediately alert a list contacts, including local police.

THE PROBLEM—MEETING TOUGH INDUSTRY REQUIREMENTS FOR HOME SECURITY

Home security is a rigorously structured and legislated industry. Boundary strictly complies to accepted industry standards (for example, BS EN 50131 for intruder alarm systems), and specifically required a solution that would comply to the IoT Security Foundation’s Compliance Framework for Best Practices. This includes a robust set of security capabilities for Boundary’s alarm product, including:

+ Key and Certificate Management, for protecting devices in the home
+ Secure Over-the-Air (OTA) firmware updates for high reliability
+ Secure Payload Verification for verifying the integrity of critical home safety functions
THE EmSPARK™ SOLUTION

Boundary selected Sequitur’s EmSPARK™ Security Suite to deliver a product fully capable of meeting the high expectations of home security solutions.

+ Throughout their lifecycles, the system’s devices use different keys and certificates, used for boot, firmware updates and Transport Layer Security (TLS) based connections to IoT cloud platforms. EmSPARK™ delivered robust key and certificate management tools to easily achieve this variety of security goals. Management functions include loading, deleting, updating, revoking and verifying keys and certificates.

+ Updating a device’s firmware and applications securely is a critical requirement and one where risk of firmware compromise is high. Incoming firmware payloads need to be authenticated to prevent corruption and compromise. EmSPARK™ provided key and certificate-based payload authentication mechanisms to ensure secure updates.

+ An end-to-end secure boot, update and failure recovery process was implemented to protect the product’s firmware integrity in manufacturing and deployment.

+ To accelerate time-to-market, Boundary—and design partner ARS—used the Microchip SAMA5D27 System-on-Module (SOM), which is supported by the EmSPARK™ Security Suite.

Learn More

- Learn More: Microchip SAMA5D27 SOM1-EK1
- Learn More: ARS Embedded Systems
- Learn More: IoT Security Foundation