IoT Security Handbook

As we increasingly integrate more devices in our lives, the potential effect of security breaches is huge!

Table of Contents

How Arm Is Helping to Secure a Trillion Connected Devices

At Arm we place importance on approaching security from the ground up. We achieve this by not only considering the protection you need to put in place, but also your recovery from the consequences of a breach.

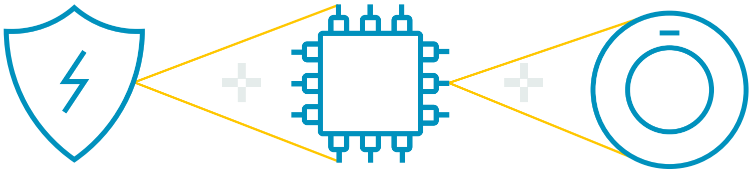
To truly enable systems built on trust, security cannot be considered a separate component, or as an afterthought to the rest of a system. It must be embedded in every element and process that exists in your Internet of Things (IoT) deployment.

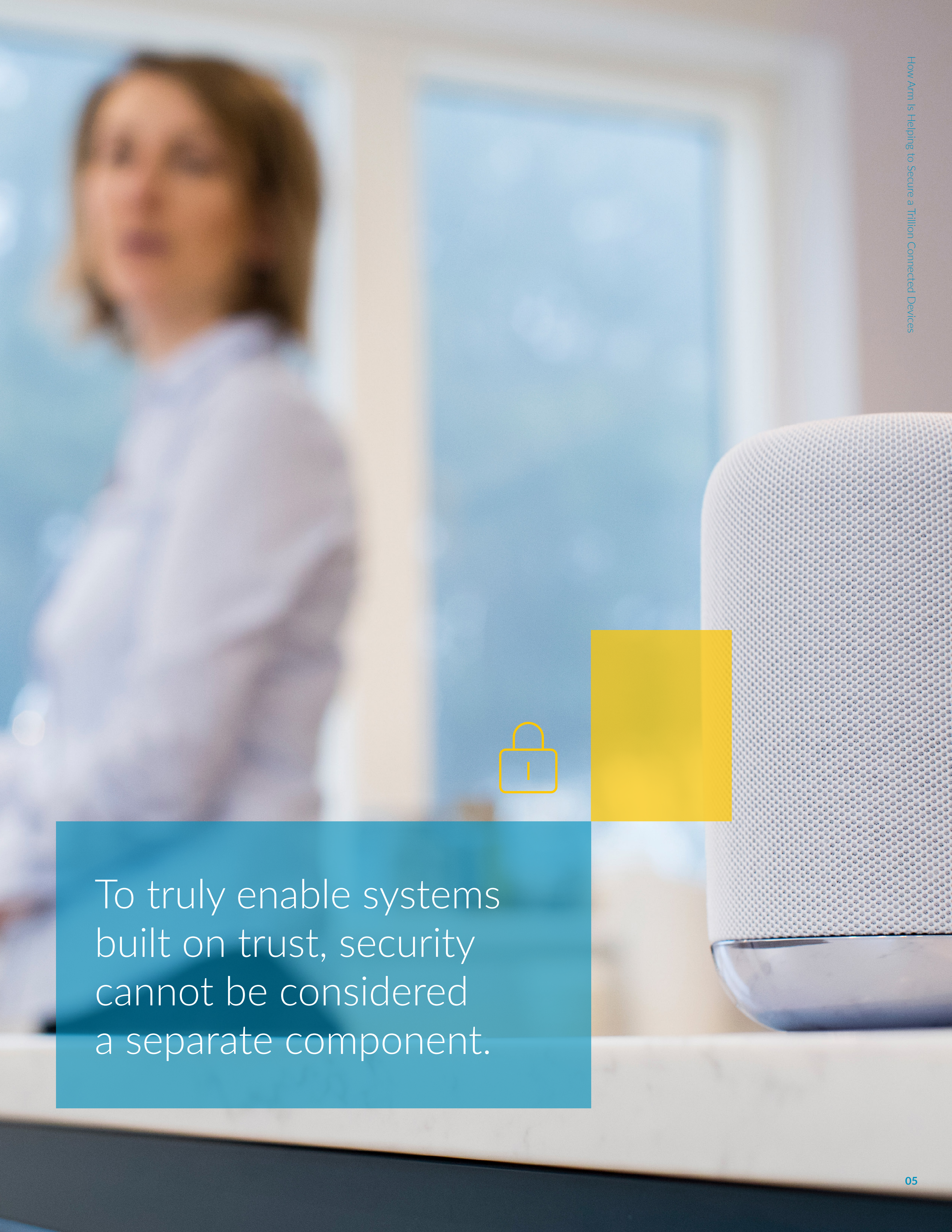
Companies who are creating IoT solutions often find themselves navigating a complex landscape of security standards, technologies and processes – without the in-house expertize required to help it make sense. Arm has a vision for security, and to help make it a reality, we launched a number of programs, services and IP products, to help companies who need to deploy network-wide security as part of their everyday business.

Understanding Potential Vulnerabilities

The first stage in designing security is understanding the environment surrounding a device or service, and what the potential threats could be. Arm identifies four main categories of potential vulnerabilities: communication, lifecycle, software and physical (also known as silicon). The risk of each of these happening will largely depend on your application, how it's being used and the potential value of your data.

IoT security should be embedded in every element and process of your IoT deployment.





To truly enable systems built on trust, security cannot be considered a separate component.

A Handy Starting Point

The Platform Security Architecture (PSA) is the framework for securing a trillion connected devices. Backed widely by Arm's partners and industry leaders, it's a four-stage process for making IoT security easier and quicker to implement. PSA suggests common principles for security design and provides a holistic set of resources for the requirements analysis, architecture and implementation phases of device design. PSA Certified provides multi-level, independent testing of IoT devices built on PSA principles.

Platform Security Architecture

A framework for securing a trillion connected devices

Analyze
Threat models & security analyses

Architect
Hardware & firmware architect specifications

Implement
Firmware source code

Certify
Independently tested

Arm aims to demystify threat modelling by providing a variety of examples that you can download for free.

If you're looking for help or advice for analyzing vulnerabilities in a system or product, the right place to start is with threat modelling. Threat Model and Security Analyses (TMSA) documentation is specifically designed to derive security requirements. If you've never considered threat modelling before, this can seem like a daunting process. Arm aims to demystify threat modelling by providing a variety of examples that you can download for free, as part of the Platform Security Architecture.
Once you've completed your threat modelling, you will be equipped with all the information you need to specify a more secure device. This will enable you to make the right choices when selecting counter-measures to protect from vulnerabilities.

PSA is the start of a longer-term effort by Arm and the ecosystem to raise the bar on IoT security. Whether you design chips, buy them, or deploy devices into the field, PSA will provide a foundational security framework for future systems.

Access PSA threat models, architectural specifications and other resources at www.arm.com/psa-resources

Layers and Lifecycles

Security does not stop at the system-on-chip (SoC) level or when a device rolls off the production line. Good security is implemented through layers of hardware and software, considering both the individual device and complete systems in which it functions, including cloud connectivity, data analytics and control components. Mitigations need to be maintained against a constantly changing landscape – as new threats emerge and while devices are built, deployed and retired.

Let's consider a typical IoT deployment, which includes a hardware device running firmware, connected to a network and communicating with a service, commonly deployed in a private or public cloud. All the following aspects must be addressed, to assure security of the IoT system, and PSA helps define and implement these aspects, outlined below.

Usage Lifecycle of an IoT Device

1. The device may contain sensitive data and must be protected from vulnerabilities (including both physical and remote software threats) to ensure data confidentiality, trust and validity.

2. To secure internet connectivity, a device must be provided with a unique identity with keys and certificates that are used to attest and authenticate itself with backend services. Additionally, they provide integrity and confidentiality of the end-to-end communications and information exchanged. It's also advantageous to have the capability to remotely manage these security credentials, so that new trusted networks and services can be used.

3. Over time, vulnerabilities will be found in the device firmware, therefore, you will need the ability to create and push new firmware updates to the device over-the-air. When the firmware is updated, it's important that the device can check that the update is from a valid source.

4. Once the device reaches its end-of-life, or is passed to a new owner, it is important to have the ability to erase all the sensitive data it contains and block its access to previously-approved network applications.

How Can Arm Products and Services Help to Secure the IoT?

A Foundational Approach

Arm provides tailored solutions for jump starting secure PSA ready SoC designs. Matched against the main IoT application classes (constrained, mainstream and rich), they map out the necessary hardware, software and tools for each set of requirements. Security is taken into account from the system architecture definition. It is pre-built into the subsystems, using the PSA principles and integrating security IP like firewalls, Secure Enclave and TrustZone technology.

Security Technology

Arm has a number of technologies and IP products for designers building a SoC that requires an extra level of security robustness. These security technologies target each type of threat.

Arm TrustZone technology has been offering foundational security since 2004, and has a rich heritage in securing mobile devices. Arm TrustZone provides robust hardware-enforced software isolation in CPUs and systems, enabling a secure Root of Trust (RoT). The family of TrustZone technologies is supported by any Arm Cortex-A and the latest Cortex-M23, Cortex-M33 and Cortex-M35P processors. Whether it's the smallest of microcontrollers or high-performance applications processors, developers can achieve isolation to help protect embedded and IoT devices from software vulnerabilities.

If you're looking to protect against communication and lifecycle vulnerabilities, the Arm CryptoIsland and Arm CryptoCell families support Roots of Trust (RoT), security services, lifecycle management, key management and cryptographic acceleration. These cryptographic and security functions are critical to countering a wide range of security threats.

Arm TrustZone provides robust hardware-enforced software isolation in CPUs and systems, enabling a secure root of trust.

Silicon Level Protection

Silicon vulnerabilities and physical security threats are becoming more and more prevalent, due to the availability of tools and knowledge. To help counter this threat, Arm introduced an enhanced family of IP. The family includes the Arm Cortex-M35P processor, which offers a robust, high-performance processor with anti-tamper capabilities.

Physical security threats are becoming more prevalent, due to the availability of tools and knowledge.

The family also includes enhanced IP from the Arm CryptoCell and Arm CryptoIsland families offering protection against side-channel attacks.

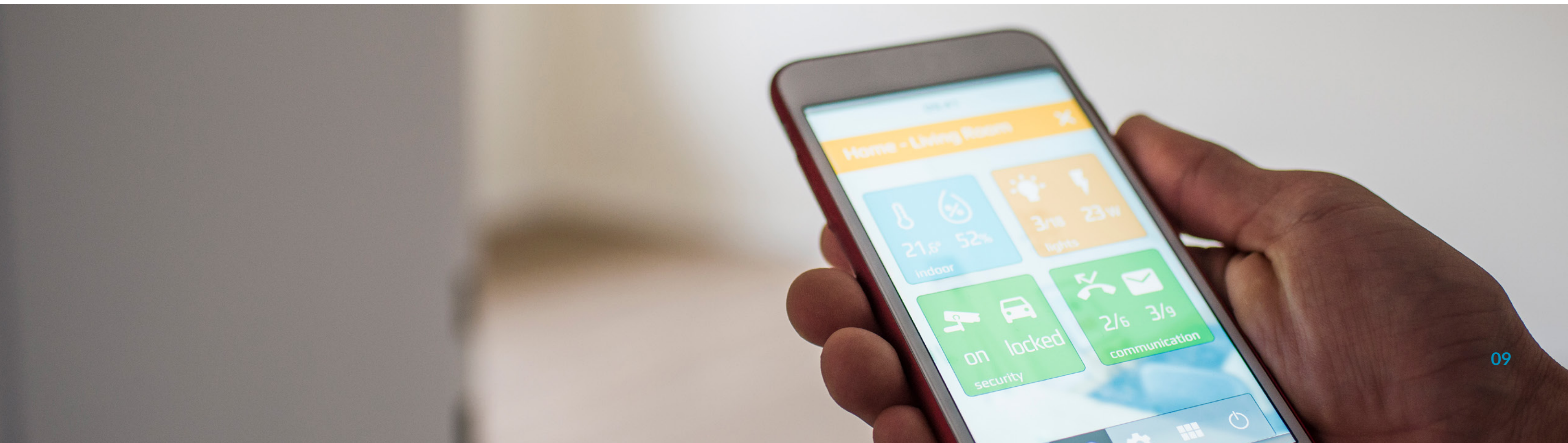
Secure Software Development

The reality of IoT will see over one trillion connected devices all using different hardware, with a variety of different standards and protocols. This means that deploying secure software will be both time-consuming and challenging. How can we ensure that software development is as easy as possible? The challenges of coding, testing and maintaining highly secure software are more easily tackled using Arm software development tools.

The Arm Keil Microcontroller Development Kit (Keil MDK) offers everything a developer needs to program a device, with support for over 6000 Arm-based microcontrollers. This includes a number of open-source CMSIS packs, which provide reusable code that works across different devices. Arm MDK also offers support for Trusted Firmware-M (a key component of the Platform Security Architecture) which allows you to create secure IoT software fast.

When coding for security using Armv8-M processors, developers can easily reduce the attack surface exposure by using CMSIS- ZONE with TrustZone and/or memory protection units (MPU). CMSIS Zone simplifies Arm TrustZone for Armv8-M partitioning, offering a quicker route to secure and non-secure domains.

In the event of code maintenance after a device has been deployed, developers can use our secure debug capabilities that only allows verified sources access to authorized secure areas for debug, using debug over functional interface and certificate-based authentication. Secure debug is made possible using a combination of Arm security IP, Arm CoreSight SDC-600 Secure Debug Channel and Arm debug adapters.



Managing Secure identity

Identity must be a key aspect of all IoT devices and it is one of the fundamental PSA security principles. Arm Kigen family offers SIM grade identity for cellular IoT devices. This allows mobile carriers to reply, host and assure the device's unique identity and its associated network attestation credentials.

The Arm Kigen product family offers the lowest footprint and standards-based secure Kigen SIM OS for devices. It also offers a security-accredited Remote SIM Provisioning service to manage SIMs through the lifecycle of these devices. The flexibility of implementing Kigen SIM OS in different form factors (SIM, eSIM, iSIM) will unlock the potential of cellular IoT across 2/3/4/5G, NB-IoT, Cat-M and others enabling scale and security.

Connecting from Device to Cloud

From cryptographic libraries on the device, through to secure firmware updates in the cloud, the Arm Pelion IoT Platform offers the security-specific building blocks you need to create, deploy and manage devices securely, from end-to-end.

Mbed TLS

IoT devices usually contain sensitive application data, and device keys are used to communicate with the cloud services or to verify firmware signature when updated over-the-air. The Mbed TLS library provides a set of software cryptographic components that allow developers to secure communications.

Pelion Device Management

Pelion Device Management secures all stages of the device lifecycle, from manufacturing through to end-of-life. It offers a service specifically designed for fail-safe, secure delivery of firmware over-the-air (FOTA), which is the only efficient way to distribute and install required software. Pelion Device Management also solves another critical challenge of IoT security: strict management around who can access devices and data.

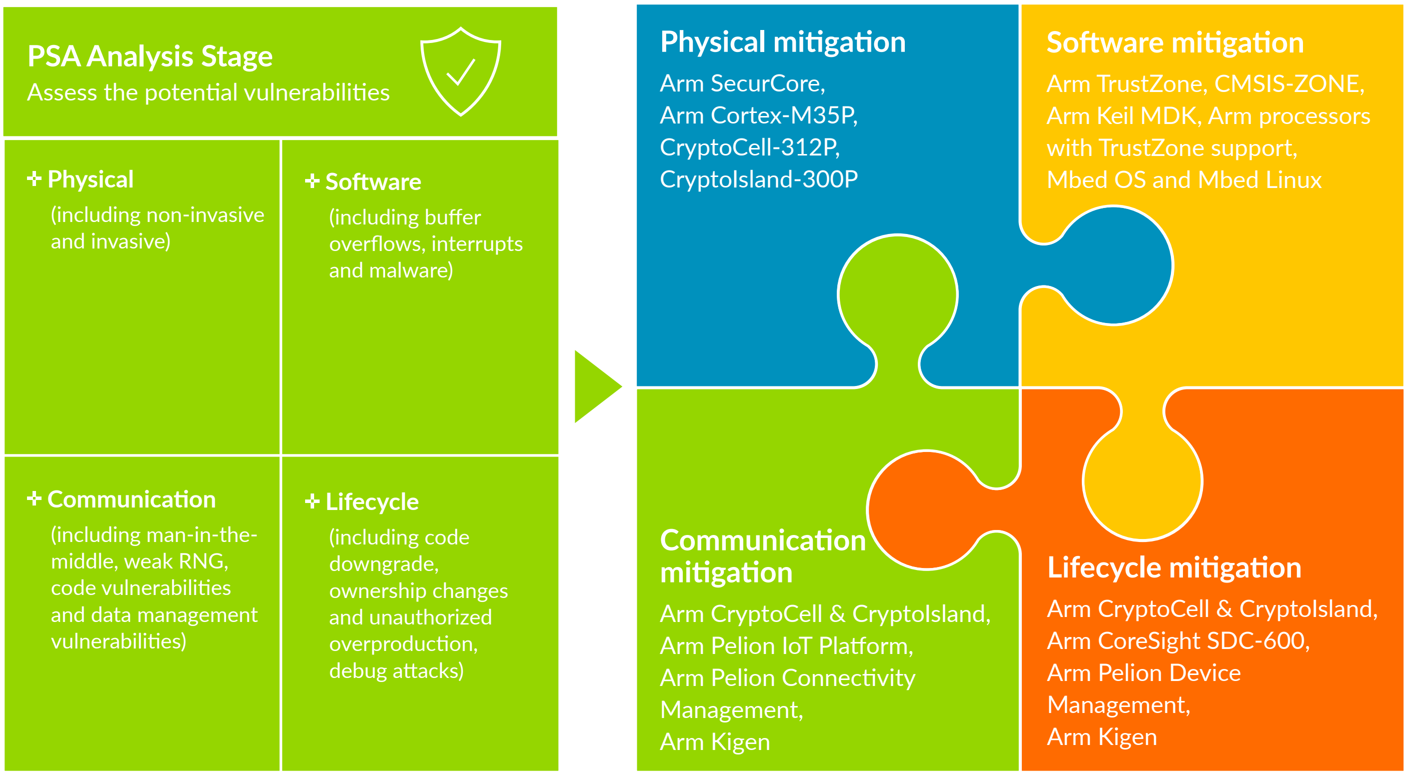
Lowering the Barrier for Cellular Connectivity

Connecting a cellular IoT device comes at a cost, such as complex logistical steps, the hardware Bill of Materials and assembly, as well as physical space. It is a struggle to justify adding cellular connectivity with current technology, especially for (but not limited to) small-footprint, low-cost devices, such as sensors. With the introduction of Arm Kigen iSIM these barriers are removed or lowered by removing the additional steps that are required today. **Kigen iSIM** leverages PSA principles, **CryptoIsland** and **Kigen SIM OS** to enable remotely provision SIMs, within the existing silicon footprint. This is supported by secure hosting by a certified service, such as the Kigen Remote SIM Provisioning service.

Matching the Vulnerability with the Right Mitigation

To enable the internet of things to grow to its full potential, security needs to be considered from initial design with all vulnerabilities being considered from the start. Arm identified four types of vulnerability with specific mitigations for each to enable the design of secure devices.

To discover more about the Arm security solution, visit **arm.com/products/security-on-arm**.



PSA Analysis Stage
Assess the potential vulnerabilities

+ Physical
(including non-invasive and invasive)

+ Software
(including buffer overflows, interrupts and malware)

+ Communication
(including man-in-the-middle, weak RNG, code vulnerabilities and data management vulnerabilities)

+ Lifecycle
(including code downgrade, ownership changes and unauthorized overproduction, debug attacks)

Physical mitigation
Arm SecurCore,
Arm Cortex-M35P,
CryptoCell-312P,
CryptoIsland-300P

Software mitigation
Arm TrustZone, CMSIS-ZONE,
Arm Keil MDK, Arm processors with TrustZone support,
Mbed OS and Mbed Linux

Communication mitigation
Arm CryptoCell & CryptoIsland,
Arm Pelion IoT Platform,
Arm Pelion Connectivity Management,
Arm Kigen

Lifecycle mitigation
Arm CryptoCell & CryptoIsland,
Arm CoreSight SDC-600,
Arm Pelion Device Management,
Arm Kigen