Six Steps to Develop Secure and Connected IoT Devices

By 2035, it's estimated there will be one trillion Internet of Things (IoT) devices running an array of sophisticated connected applications, including machine learning at the edge. This intelligent network needs to be built on a foundation of IoT-device security with defense-in-depth at its core, as the IoT will not scale if it can't be trusted.

1. Start from a common security foundation

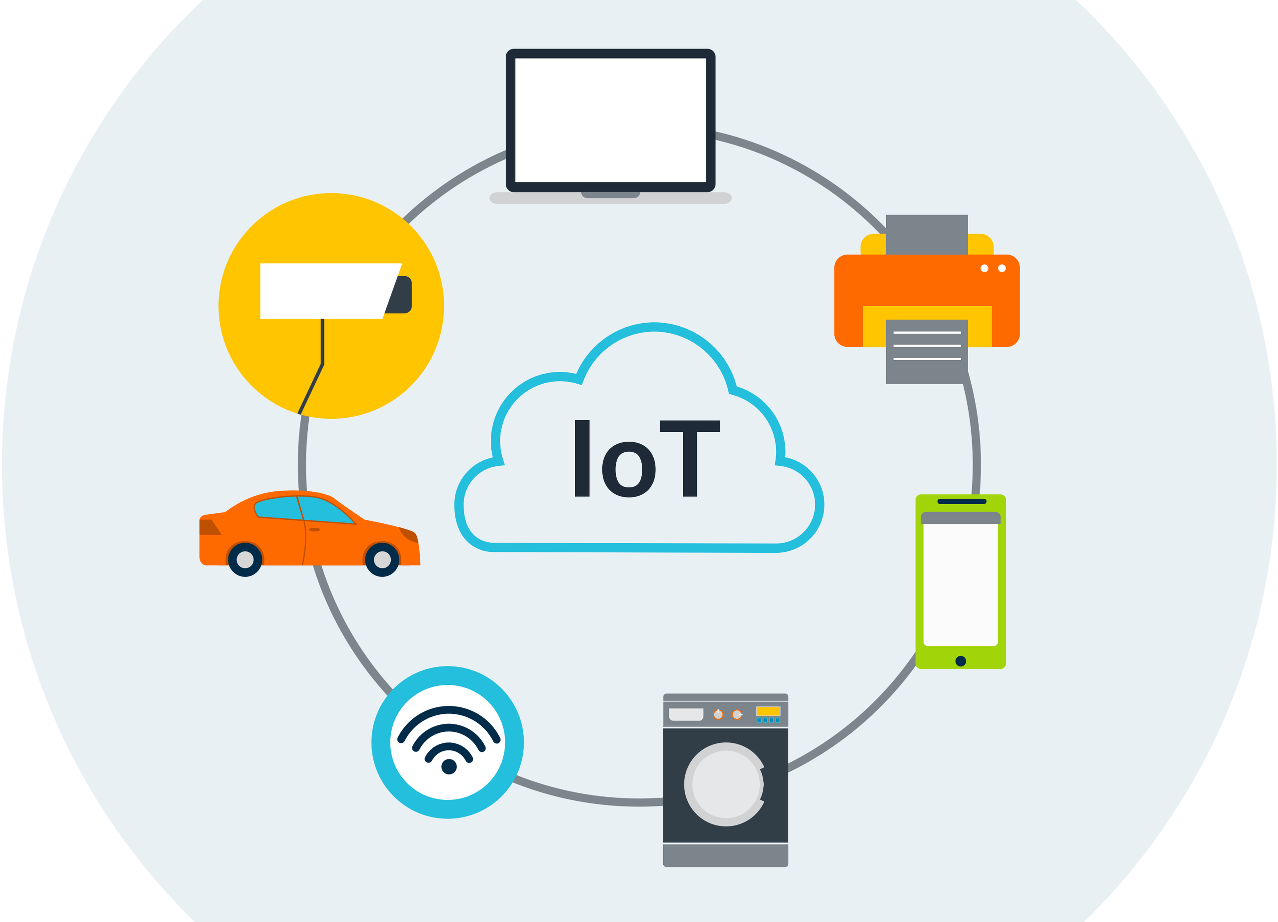
The IoT will be made up of devices with a variety of performance characteristics and price points. It presents a challenge in achieving a consistent level of security because product developers will have different business motivations and expertise. **The Arm Platform Security Architecture (PSA)** is a great starting point for achieving a secure-by-design product.

2. Think about your IoT business model

The current "design, ship, analyze, and pivot" product-delivery model works best when manufacturers are able to apply post-shipment device deployment security fixes (e.g. in smartphones). This ability to update needs to be built into the design process from the start. Moving forward, the ability to deal with security threats will evolve as artificial intelligence enables more advanced threat detection. This will change IoT business models to "design for security, ship, analyze, and self-heal or quarantine."

3. Take a multilayer approach to security

Any security implementation needs to fit the use case in mind, which is why it's important to consider the threats your device may face. Once you've created a threat model for your application, you can deploy a multilayer approach to security that protects your IoT solution. Consider multiple vulnerabilities and deploy the right counter-measures, including (but not limited to) isolated security domains, cryptography, secure over-the-air updates, and transport layer security for secure communications.

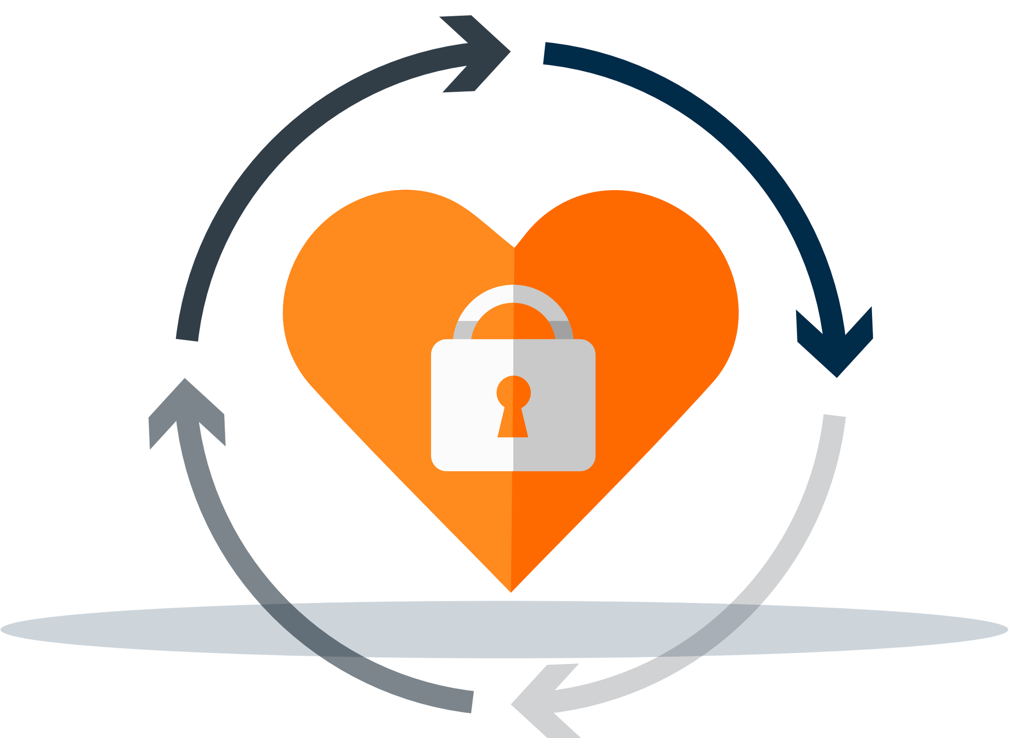


4. Use a secure RTOS purpose-built for IoT devices

Today's increasingly complex IoT applications use an open source operating system created specifically for IoT devices. An embedded operating system should offer a comprehensive suite of security and connectivity elements.

5. Run detection at the edge

A secure IoT system requires detection capabilities at the edge. Your edge nodes should feature sensors that monitor unusual behavior and include live firmware execution, tracing and performance counters to capture code and data-access patterns.



6. Make security central to device updates

You need to think about lifetime security of your device. With this in mind, it is critical that you can deliver authenticated and validated firmware securely over any network infrastructure, no matter which connectivity protocol your device is running. These are essential capabilities for a network of highly secure IoT devices.

Arm is committed to solving tomorrow's IoT device-security challenges through innovative, security-first product design. Learn more about how Arm approaches security and its security solutions to enable a connected, highly secure one trillion IoT device future.