Secure Vault™ is an industry-leading suite of state-of-the-art security features that address escalating Internet of Things (IoT) threats, greatly reducing the risk of IoT ecosystem security breaches and the compromise of intellectual property or revenue loss from counterfeiting. Specifically, Secure Vault technology:

- Protects against scalable local and remote software attacks
- Defends against local hardware attacks, which – although historically less common than software attacks – are on the rise due to the surge of affordable and easily accessible tools
- Passes testing from independent, third-party laboratories that attempt to infringe security functions for a specified amount of time with sophisticated equipment

Key Features of Secure Vault

Secure Key Management

A Physically Unclonable Function (PUF) to generate a unique digital fingerprint value every time the chip is booted.

Anti-Rollback Prevention

The Secure Boot has the capability to prevent roll-back attacks where cyber criminals try to force the MCU to a previous version with a known vulnerability.

Anti-Tamper

Tamper Protection is a very effective way to prevent a hacker from performing sophisticated local attacks. In addition to tamper based on external switches, we offer tamper based on frequency, temperature, voltage and EMF.

Secure Debug with Lock/Unlock

Devices have been able to lock debug ports for some time, resulting in a manufacturer being unable to troubleshoot the device if it ever fails. With Secure Debug, we've fixed that problem.

Secure Link

Our communication products are often connected on a PCB via a serial interface to a host MCU. Secure Link provides a means of encrypting this interface with a key exchange per session with new keys on each power cycle.

Secure Boot with RTSL

The Root of Trust Secure Loader, a multi-stage bootloader with authentication, checks at each stage with our Immutable Hardware Root of Trust, a separate Secure Engine security subsystem with its own ROM, Flash and RAM.

Secure Attestation

One of the greatest benefits of Secure Vault is that it can provide a "Secure Identity," and with that identity, you can perform a Secure Attestation at any time during the life of the product.

Differential Power Analysis (DPA) Countermeasures

DPA is a black box attack called side-channel attacks, a way to mathematically study stray emissions from the chip and derive the secret keys used during cryptography.

True Random Number Generator (TRNG)

Secure Vault TRNGs meet the most stringent security requirements, including NIST SP 800-90A/B and newer C requirements.