# DIGI TRUSTFENCE®
# SECURE BY DEFAULT

**DIGI TRUSTFENCE®**

🔑 **SECURE BOOT**

🔒 **ENCRYPTED STORAGE**

✓ **PROTECTED PORTS**

☰ **CONFIGURATION BEST PRACTICES & MONITORING**

**Digi TrustFence, the industry's only built-in device security framework, is designed to protect Digi cellular routers, gateways and embedded solutions from intrusion.**

## Powerful Security for Your Connected Devices

Security is a critical concern for engineers and architects designing networks to support the growing number of connected IoT devices. Evolving technology and the sheer scale of connected devices expose operators to significant new security risks and engineering challenges. Worrying about the vulnerability of remote or customer-premise LTE equipment shouldn't be one of those challenges.

Digi TrustFence® provides a tested and documented security framework designed to minimize or eliminate threat vectors. When you deploy connected Digi products with Digi TrustFence built in, you have the assurance that remote network equipment and edge devices will be security assets, not liabilities.

Whether you build IoT products or deploy plug-and-play Digi cellular solutions, TrustFence has your back.

**DIGI**

# Rely on Digi TrustFence to keep remote equipment secure and up-to-date

Digi TrustFence is the security framework for Digi connected solutions. TrustFence provides "defense in depth" security, resulting in robust, multi-layer defense to thwart existing and future threats.

The built-in security of Digi TrustFence gives you secure connections, authenticated boot, encrypted data storage and secure software updates, and excludes all insecure ingress protocols.
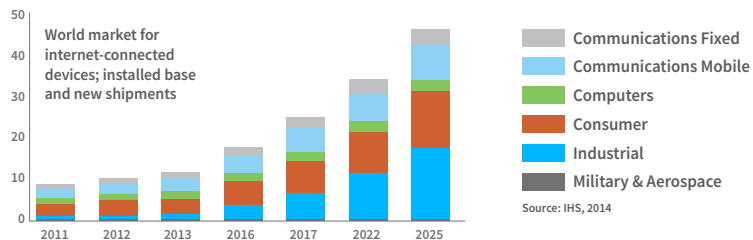
## Growing Connectivity and Concern for Device Security

# 70%

of IoT devices are vulnerable to attack

Source: HP Security Research

**Non-consumer sectors will account for the majority of connected devices by 2025.**

World market for internet-connected devices; installed base and new shipments

Communications Fixed
Communications Mobile
Computers
Consumer
Industrial
Military & Aerospace

Source: IHS, 2014

2011 2012 2013 2016 2017 2022 2025

## Built-in security with a full range of features

### SECURE BOOT

Secure Boot is a set of authentication capabilities that ensure only authorized users can access a device and only certified code can run on a device. The following are the key elements of Secure Boot:

- **No Default Password** – Prevent hackers from guessing an administrator password to the device.
- **Authenticated Firmware Upgrade** – Only allow firmware that has been authorized by the manufacturer.
- **External Authentication and Device Identity Management** – With certificate management and secure key storage, each device can be authenticated before it joins your network. This allows management of users. This also allows password policies, eliminating the challenge of managing them separate from the device.

### ENCRYPTED STORAGE

Encryption for sensitive keys and settings keeps internal data safe. Digi's cryptographically secure pseudo-random number generator (CSPRNG) is dedicated hardware for random source generation. This ensures data is encrypted in an unpredictable way, which is a requirement for all security operations.

### PROTECTED PORTS

All internal and external I/O ports are hardened and access controlled to prevent unwanted local intrusion. Digi ensures all ingress and egress protocols are secure.

## CONFIGURATION BEST PRACTICES AND MONITORING

Encryption of sensitive information keeps internal data safe. Additionally, Digi TrustFence includes tamper-proofing and device-integrity monitoring to protect against physical intrusion, as well as enterprise-level data encryption for secure connections.
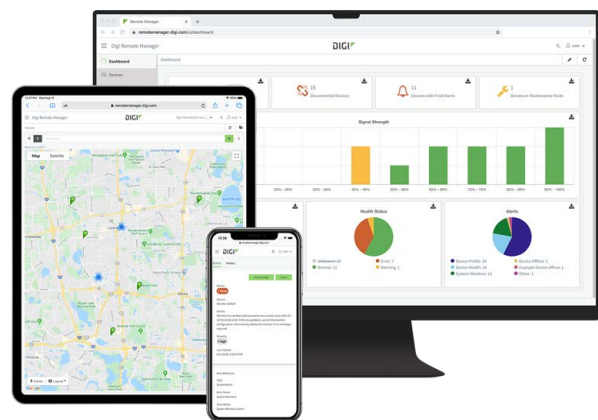
## Digi Remote Manager

With Digi Remote Manager®, you can centrally administer device configurations, update firmware and track operational status of your devices. You can build a device configuration that has no services that are directly attackable on the device. This will significantly reduce your external attack surface on your devices. All management communication will be initiated by the device into Digi RM over a highly secure and authenticated connection.

91003526
B3/920

DIGI