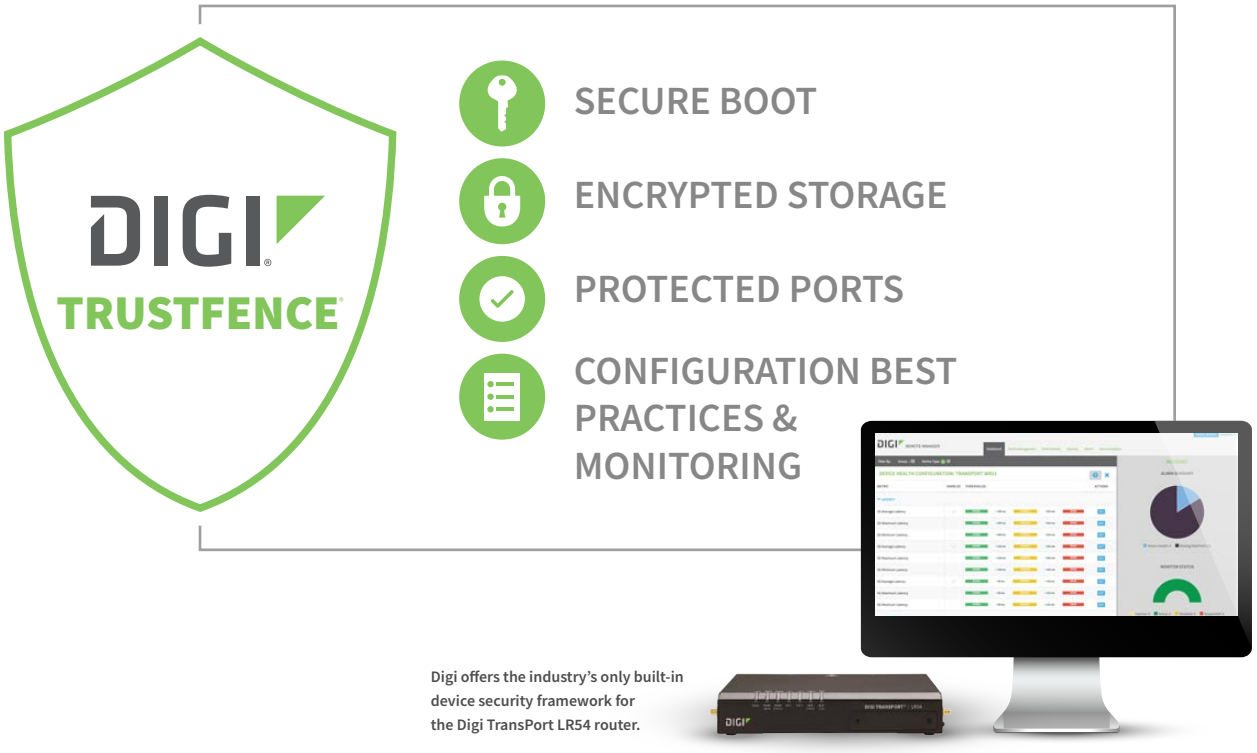
V.3/19

DIGI TRUSTFENCE®

SECURE BY DEFAULT



Digi offers the industry's only built-in device security framework for the Digi TransPort LR54 router.

Enterprise LTE networking – built secure from the ground up

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. With an LTE platform designed for security from the start, you have the assurance that remote network equipment will be a security asset, not a security liability.

Alcom electronics
Singel 3 | B-2550 Kontich | Belgium | Tel. +32 (0)3 458 30 33
info@alcom.be | www.alcom.be
Rivium 1e straat 52 | 2909 LE Capelle aan den IJssel | The Netherlands
Tel. +31 (0)10 288 25 00 | info@alcom.nl | www.alcom.nl
DIGI

Rely on Digi TrustFence to keep remote TransPort LTE equipment secure and up-to-date.

Digi TrustFence is the security framework for the Digi TransPort® LR series of M2M routers. The TrustFence framework requires security to be designed in at the ground floor, resulting in a new security orientation for Digi TransPort LR devices. The built-in security of Digi TrustFence gives you secure connections, authenticated boot, encrypted data storage, secure software updates, and excludes all insecure ingress protocols.

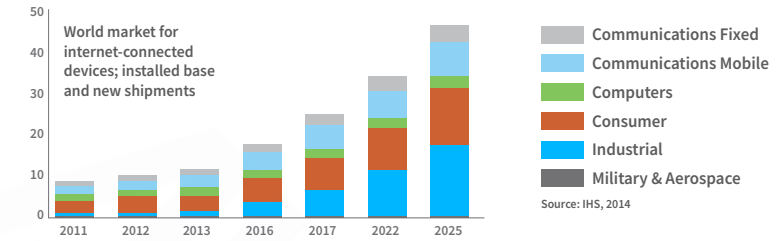
GROWING CONNECTIVITY AND CONCERN FOR DEVICE SECURITY

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.



Digi TrustFence delivers built-in security with a full range of features including:

Secure Boot

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

No Default Password – Prevent hackers from guessing an administrator password to the device.

Authenticated Firmware Upgrade – Only allow firmware that has been authored 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 centralized management of users. This also allows password policies, which can become very complex to be managed separate from the device.

Encrypted Storage

Local file system encryption keeps internal data safe. Digi's cryptographically secure pseudo-random number generator (CSPRNG) is dedicated hardware for random source generator that is unpredictable, 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 and the JTAG port is secured.

Configuration Best Practices and Monitoring

Good security requires people, process and technology. Digi delivers end-user guidelines to properly secure a device and have confidence that it stays secure. Our guidelines include hardening documentation and policy guidelines along with on-going monitoring, alerts and notifications.

For more information about Digi TrustFence, visit www.digi.com/security

www.digi.com

91003526
A2/817