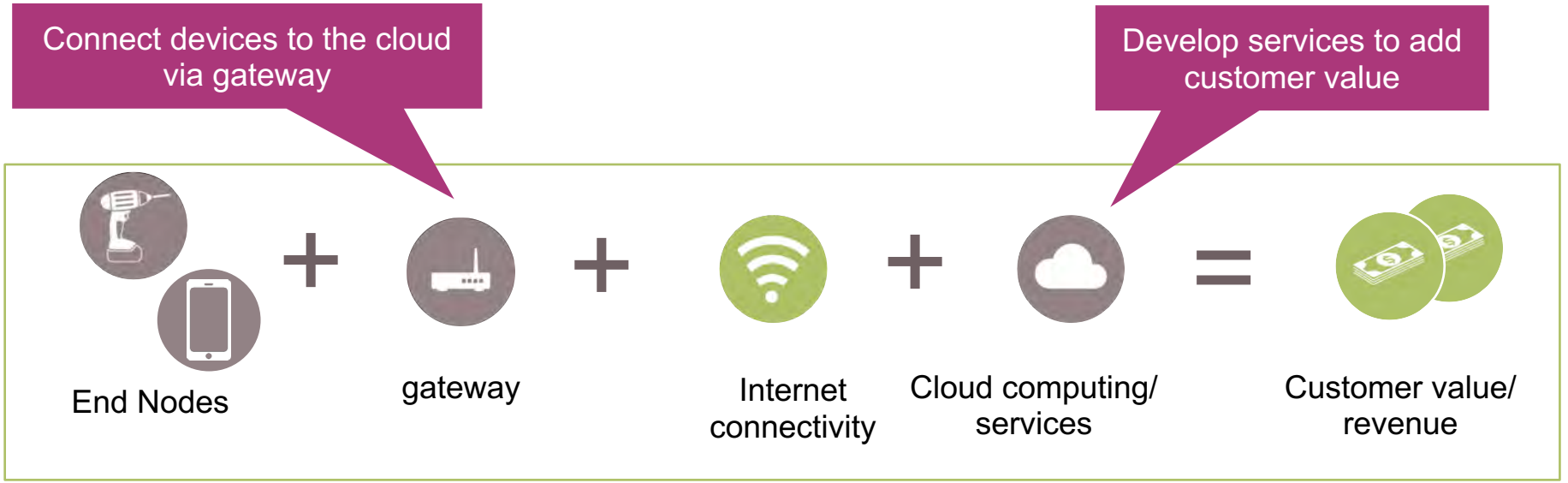
Securing your gateways against attacks

Infineon’s virtual show 2020

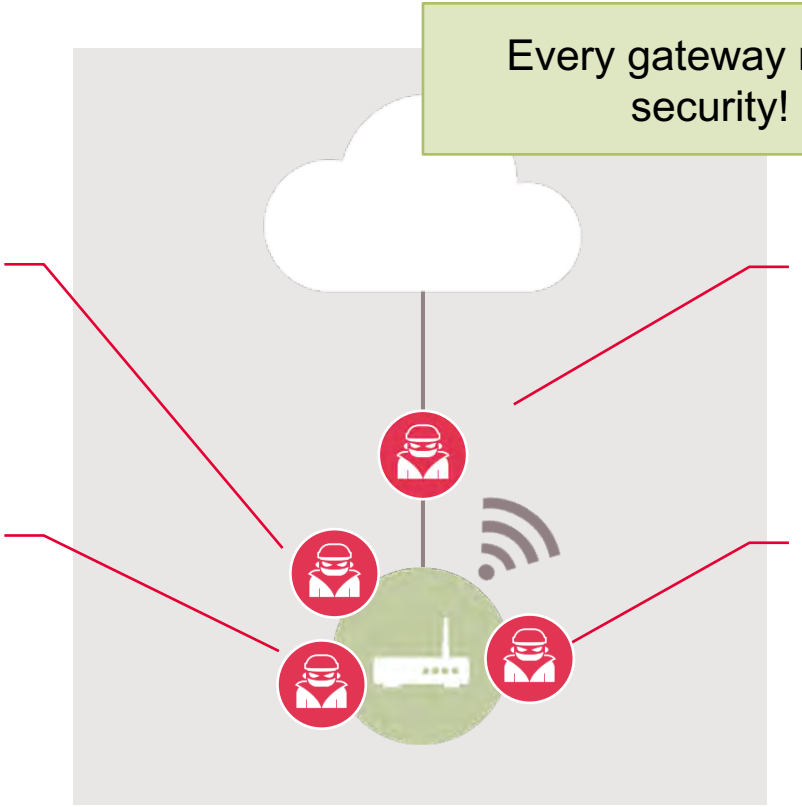
Enterprises face a changing environment



Migration from a device-centric to cloud-based business making your **gateways an attractive target for attacks**

Gateways can be attacked through many ways

Every gateway needs security!



Cryptographic key attacks

e.g. steal or manipulate secrets

Device integrity attacks

e.g. change device's configuration, malware

Communication attacks

e.g. eavesdropping, man-in-the-middle

Device identity attacks

e.g. generate fake devices

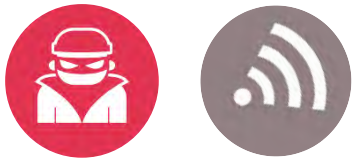
Why is protection against physical attacks so important? …they are often used to discover new connectivity attacks

Attacker gets **physical access** to a device

Buy a targeted gateway on the Internet

Attacker performs physical attacks to **identify vulnerabilities**

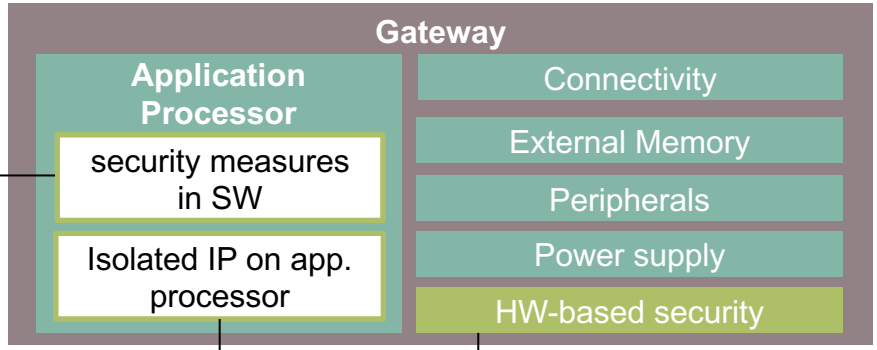
- De-solder & read out flash memory to analyze SW
- Tampering of µC to identify sensitive information or cause unintended behavior



Attacker implements and performs **remote attack**

The attacker combines the know-how gained from physical attacks with other attack vectors to create a new attack

Implementing attack countermeasures on gateway



	Software	Isolated Security IP (HSM)	HW-based security
Software attacks	⚠	🔒	🔒
Micro-architectural attacks	⚠	🔒	🔒
Physical attacks	⚠	⚠	🔒

Strong security solution built on security certified HW

OPTIGA™ TPM is a standardized and turnkey solution

The OPTIGA™ TPM is best described in two pieces

Hardware Security Module (HSM)

Credential storage

Cryptographic operations

+

Security Functions

- Platform Integrity Measurement
- Key Sealing
- Enhanced authorization

100+ functions

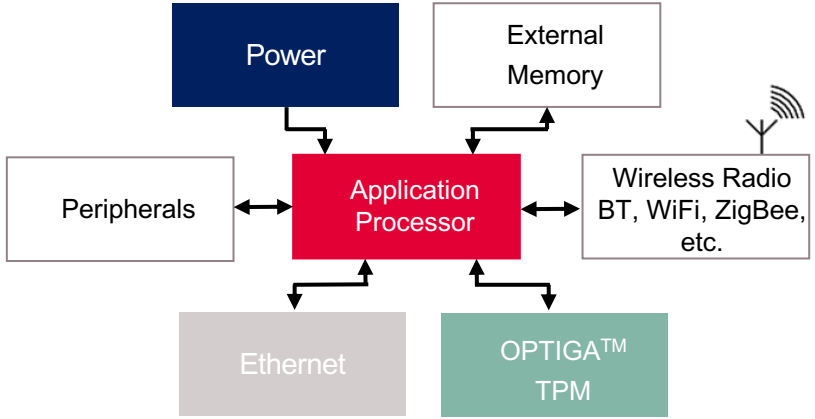
Key benefits

OPTIGA™ TPM

- Provide **certified hardware-based roots of trust** for the gateway
- Assurance on **platform integrity**
- Cryptographic **key generation and storage**
- Cryptographic **anti-counterfeiting**
- Good **entropy source**
- **Easy integration** with many OS, PKI software libraries and etc

Main security use cases

- OEM device Identity
- OEM counterfeit protection
- Secured zero touch provisioning
- Securing secrets
- Secured communication
- Protection of IP
- Device health check
- Entropy generation

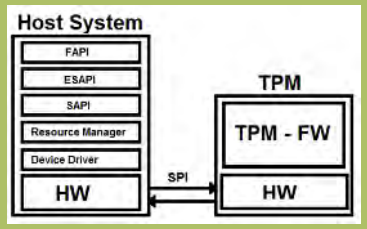


Infineon offers beyond the products delivering complete solutions for gateway

Hardware

TPM Iridium board on Raspberry Pi®

Software



TPM2.0 SW Stack

Cloud Platform

AWS Greengrass

Microsoft Azure

Appnote, Github, Whitepaper

Your personal key takeaways

Strong security is required for gateways today

Infineon provides scalable, strong, easy to use security solutions

Infineon is the ideal partner for network equipment security

Part of your life. Part of tomorrow.