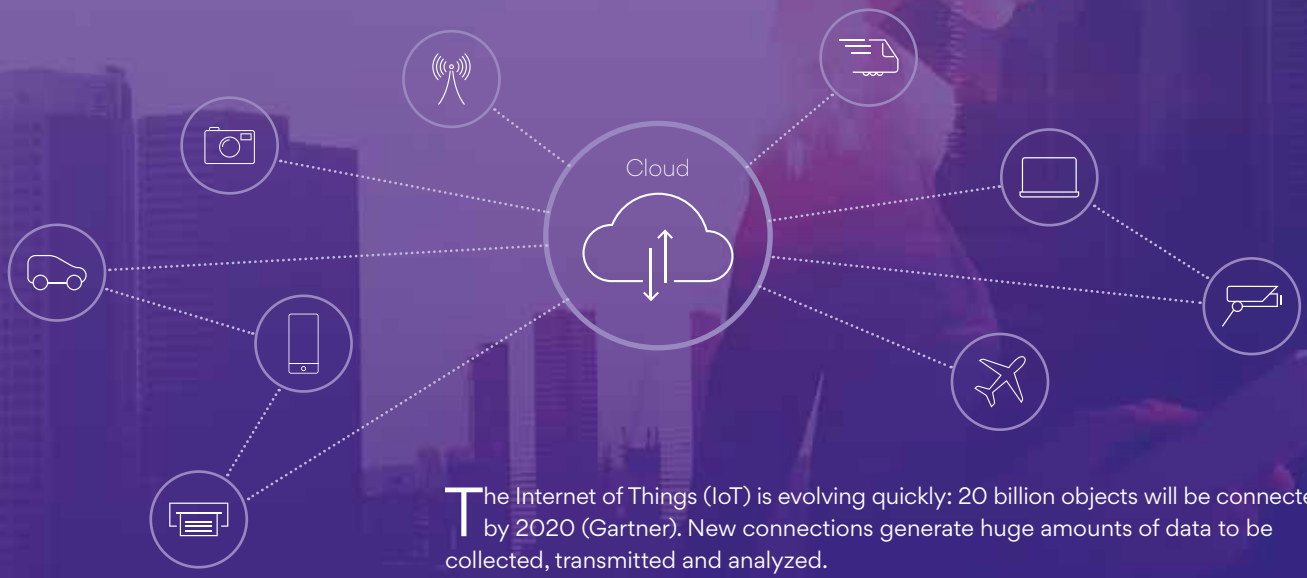
IoT HRiVE™

Managing the entire security chain of non-cellular communications

Connected Objects

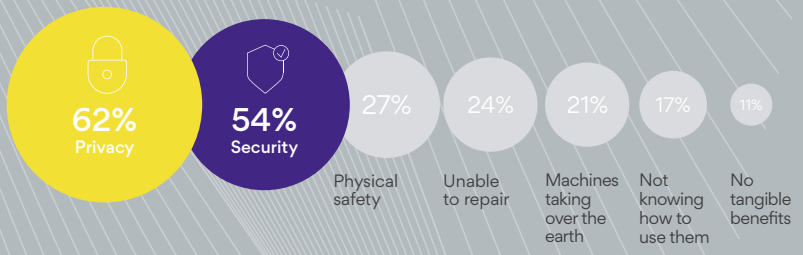


The Internet of Things (IoT) is evolving quickly: 20 billion objects will be connected by 2020 (Gartner). New connections generate huge amounts of data to be collected, transmitted and analyzed.

Internet of Things creates new business opportunities and new services for all market participants. But multiplying connections between objects and the cyber world also means multiplying risks.

Indeed, a Gartner study says that more than 25 percent of all attacks targeting companies will be made by taking advantage of connected objects. IoT is mainly seen as a source of innovation and progress, but also of concern: 62% of the responders of a global survey are worried about privacy, and 54% about security.

What would concern you about a world of connected IoT devices ?



Mobile Ecosystem Forum survey, 2016

Security in IoT requires trusted information

3 PILLARS OF TRUST

Authenticity

Trusted / genuine object with mutual authentication

Integrity

Information not modified or corrupted during transmission

Confidentiality

Encryption / decryption of sensitive information

With **IoThrive™** IDEMIA offers an end-to-end solution, for non-cellular connectivity, composed of secure elements and cloud services to manage the entire security chain in the Internet of Things.

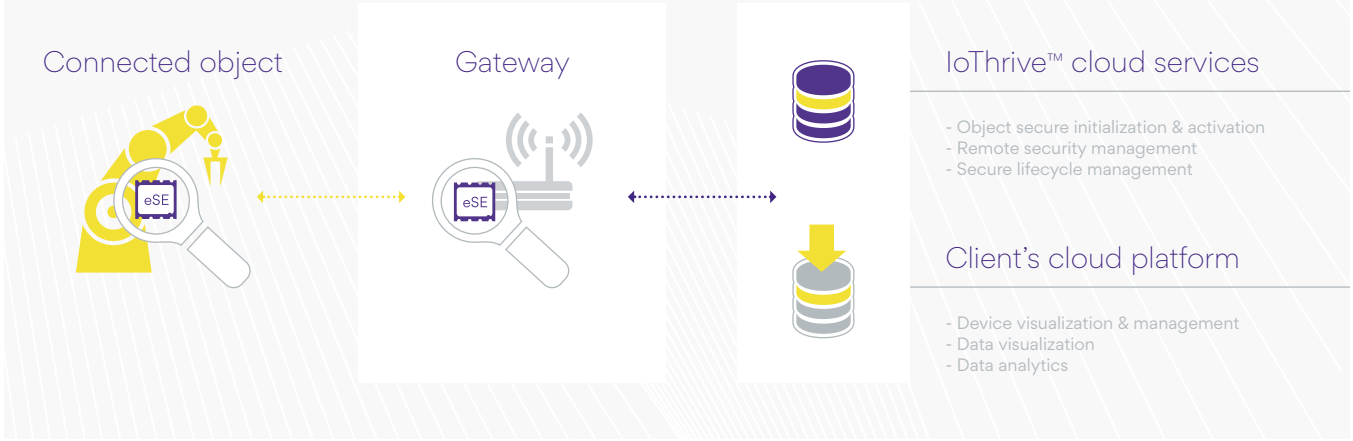
IDEMIA

Secure data flow from a connected object's digital identity to trusted cloud services

END-TO-END SECURITY

COLLECT & TRANSMIT DATA

ANALYZE DATA



By 2025,
non-cellular connections will represent more than
70%
of IoT connections

IoThrive™ is able to manage trusted identities for connected objects in any non-cellular low power network - long range (LPWAN) or short range - for industrial and consumer markets:

INDUSTRIAL		CONSUMER
Security	Energy	Connected vehicles
Healthcare	Metering	Smart Home
Farming	Manufacturing	Consumer Electronics

IoThrive™ Key benefits

- End-to-end solution for security from the connected object to the cloud
- Enabling secure data exchange only between authorized devices using low power networks
- Flexibility to adapt to the requested level of security and customer needs
- Preserving the intellectual property and brand protection
- Simplifying secure enrollment and lifecycle management of objects

IDEMIA

Join us on

www.idemia.com