Written by Marco Attard
04 September 2015

According to Gartner by end 2017 20% of enterprises will acquire security services to protect business initiatives using devices and services making part of the Internet of Things (IoT).

“The IoT now penetrates to the edge of the physical world and brings an important new "physical" element to security concerns. This is especially true as billions of things begin transporting data,” the analyst says. “The IoT redefines security by expanding the scope of responsibility into new platforms, services and directions. Moving forward, enterprises should consider reshaping IT or cybersecurity strategies to incorporate known digital business goals and seek participation in digital business strategy and planning.”

The IoT is at a "conspicuous inflection point" for security, since it consists of devices and services designed for specific purposes. IoT devices use data to change the physical state of environments, be it raising temperatures when a sensor determines a room is too cold, or adjusting fluid flow to a patient as per medical records, and as such require "significant" security function governance, management and operations.

In addition securing the IoT is something of a "moving target"-- after all, the term covers a sheer number of possible device technology and service combinations, meaning its security will involve the use of both old and new technologies from all eras.

“Ultimately, the requirements for securing the IoT will be complex, forcing CISOs to use a blend of approaches from mobile and cloud architectures, combined with industrial control, automation and physical security,” Gartner concludes. “However CISOs will find that, even though there may be complexity that is introduced by the scale of the IoT use case, the core principles of data, application, network, systems and hardware security are still applicable.”

Go Gartner Says that the IoT Will Change Cybersecurity Forever