Written by Marco Attard
19 December 2014

According to Gartner the Internet of Things (IoT) will drive the device and user relationship requirements of 20% of identity and access management (IAM) implementation by 2016, bringing new concepts in identity management.

"IAM, as defined today, will bifurcate, with identity management assuming a broader entity relationship management role and access management assuming a broader relationship execution role that replaces or supplements authentication policy and authorization enforcement," the analyst says. "Traditional authentication and authorization for user identities will continue to include devices and services, but will also incorporate expanded machine-to-machine (M2M) communications requirements into expanding digital business moments. Embedded software and systems will make extensive use of the new and expanded IAM architecture to handle the scale and ubiquity requirements the IoT will demand."

In other related predictions, Gartner says enterprise mobility management integration will be a "critical" IAM requirement for 40% of customers-- up from 5% today-- as organisations demand consistent, convenient and secure access to enterprise and 3rd party applications across a wide array of devices. As such, IAM and EMM will both become security requirements, protecting from threats that have overcome traditional IAM and EMM controls when used in isolation.

Further in the future, 60% of organisations will implement social identity proofing by 2020, allowing consumers to access risk-appropriate application via social or other 3rd party identities-- a bring your own identity (BYOI) approach to security, if you will. Being low-cost, such a means of security would be particularly useful for SMBs, eliminating the need for in-house identity-proofing processes.

For the same period Gartner forecasts biometric technologies (such as face recognition via a

user-facing camera, voice recognition via a microphone, keystroke and gesture dynamics via multitouchscreens and handling dynamics) will replace passwords and fingerprints in endpoint device access across 80% of the market by 2020. Such technologies are already built into many mobile devices, and can be simply implemented via endpoint OS update.

"Embedded fingerprint authentication does not improve user experience for everyone," the analyst concludes. "Furthermore, given the low trust that these methods afford, we expect to see increasing dissatisfaction as people's devices are compromised over the next few years. The same kind of biometric modes that organizations may soon adopt for authentication from the device will be preferred for authentication to the device in the midterm."

Go Gartner Predicts 2015: Identity and Access Management