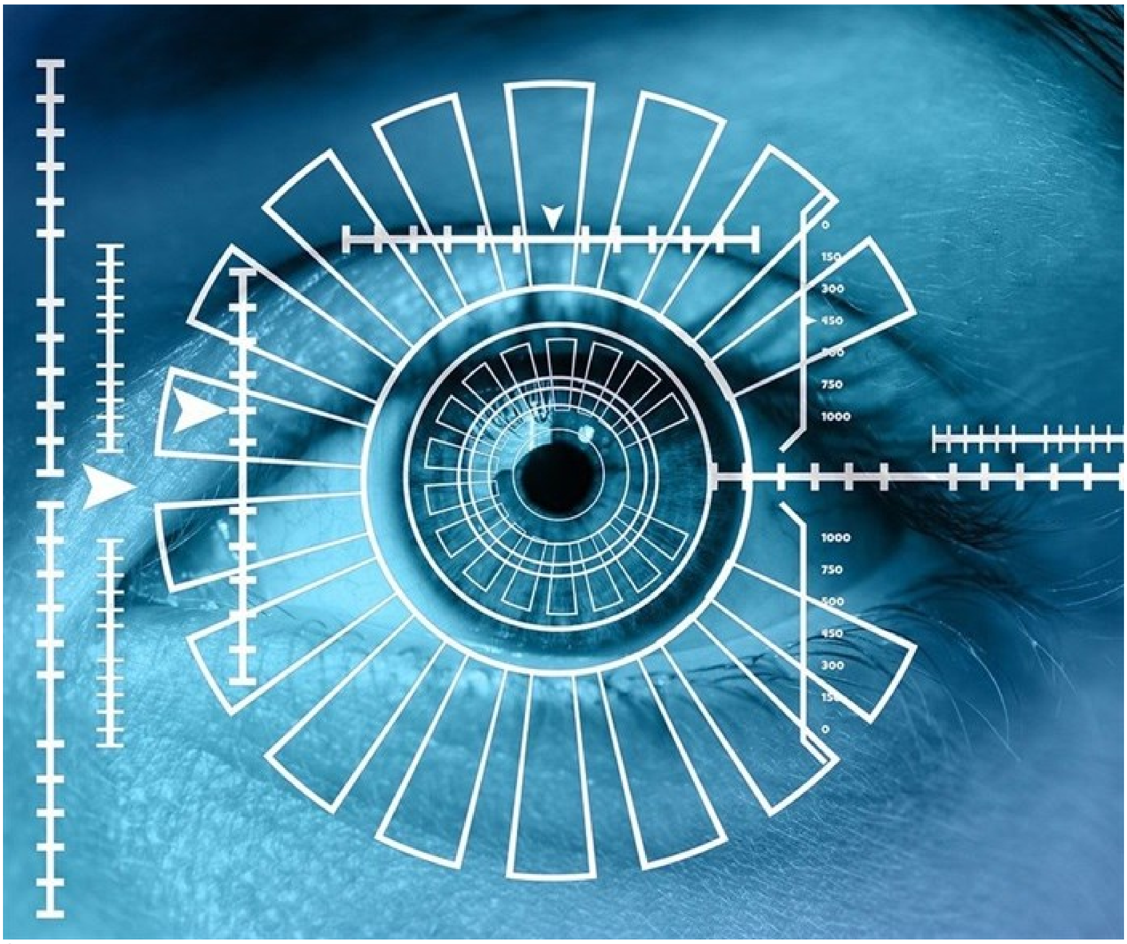
BIZCOMMUNITY

Gartner predicts increased adoption of mobile-centric biometric authentication

By 2022, Gartner predicts that 70% of organisations using biometric authentication for workforce access will implement it via smartphone apps, regardless of the endpoint device being used. In 2018, this figure was fewer than 5%.



Source: pixabay.com

Lower costs and improved user experience/customer experience (UX/CX) are fuelling this increasing interest in biometric authentication.

“Security and risk management leaders responsible for identity and access management (IAM) and fraud prevention continue to seek approaches for identity corroboration that balance trust and accountability against total cost of ownership and UX/CX,” said Ant Allan, research vice president at Gartner.

“Biometric authentication uses biological or behavioural traits unique to each person and offers better UX/CX and accountability than other common methods. Implementing this via smartphone apps provides more consistency in UX/CX and is technically simpler than supporting it directly on a variety of different endpoint devices.”

#BizTrends2019: Digital, data-driven biometrics

Pine Pienaar 15 Jan 2019

Midsize and large organisations looking to implement biometric authentication via smartphone apps must be aware that biometric approaches that can be readily supported on any smartphone are vulnerable to presentation attacks or “spoofing” using photos, videos, voice recordings, and so on. Therefore, presentation attack detection or “liveness testing” is essential.

SaaS-delivered IAM will fulfil most needs

Gartner predicts that, by 2022, 40% of global midsize and larger organisations will use IAM capabilities delivered as software as a service (SaaS) to fulfil most of their needs — up from 5% in 2018.

SaaS-delivered IAM is often deployed to enhance access management software implementations. The ease of implementation and rapid time to value of SaaS-delivered IAM offerings have proved valuable to organisations that favour SaaS adoption and do not consider the operational management of IAM functionality core to their business.

How do biometric identifiers measure up?

Henrik Nilsson 24 Dec 2018

“Based on our client interactions, most SaaS-delivered IAM purchases are for access management and lightweight identity governance and administration functionality, such as single sign-on. These offerings provide excellent connectivity and include solid access management and password management features,” said Abhyuday Data, associate research principal analyst at Gartner.“B2B and B2C are the most established use cases with matured access management capabilities.”

The steady movement of applications to cloud and mobile architectures is also influencing adoption. The combination of functional offerings that are configured, rather than customised, and modern application architectures is causing a substantial portion of the market to adopt SaaS-delivered IAM.

“Organisations looking to use SaaS-delivered IAM should first ensure they have established satisfactory and well-supported traditional IAM software stacks. They then need to consider SaaS-delivered IAM once functional needs are met and the organisational benefits are realised,” concluded Allan.