43%
PROCESSING
OF FACE
RECOGNITION
S1 = 528,08; S2 = 833,22; S3 = 044,47
S4 = 922,76; S5 = 334,09; S6 = 432,78
S7 = 099,65; S8 = 209,25; S0 = 168,45
S1 = 528,08; S2 = 833,22; S0 = 168,45
S3 = 044,47; S4 = 922,76; S5 = 387,49
S7 = 099,65; S8 = 209,25; S0 = 449,90
S1 = 528,08; S2 = 833,22; S3 = 044,47
S4 = 922,76; S5 = 334,09; S6 = 432,78
S7 = 099,65; S8 = 209,25; S1 = 528,08
S2 = 833,22; S0 = 168,45; S3 = 044,47
S4 = 922,76; S5 = 387,49; S7 = 099,65
S8 = 209,25; S0 = 449,90; S0 = 168,45

Will Biometrics Replace Passwords?

Devolutions

BY THE YEAR 2022, THE BIOMETRIC INDUSTRY IS EXPECTED TO REACH $32.73 BILLION WORLDWIDE.

Over the last couple of decades, and especially in the last few years, the use of biometrics as part of identification and access control has been surging. In fact, by the year 2022, the biometric industry is expected to reach $32.73 billion worldwide.

Given that the role of biometrics is only going to get bigger in the future, we thought it would be helpful to provide a summary of what biometrics are, and highlight some of its pros and cons.

About Biometrics

Biometrics refer to a process in which an individual's **unique physical traits** are captured, scanned and recorded by an electronic system in order to authenticate identity and grant access to physical spaces, software, devices, and so on. There are many different types of biometrics. The best known are **face, fingerprint, iris, palm and voice**.

Top 3 Pros

- **HARD TO FAKE** Like Minority Report demonstrated, it's hard to fake an iris scan!
- **CONVENIENT** Giving new employees and visitors unique, strong passwords can be time-consuming, and they can forget them — or worse, store them in an unsafe manner (sticky notes, spreadsheets, etc). With biometrics, all that organization needs to do is register a bio of the person and everything is set. There's nothing to remember and nothing to forget!
- **EASY TO USE** Putting your hand on a screen, staring at a lens, or saying your name is fast and easy.

Top 3 Cons

- **PRIVACY** Not everyone is comfortable with the idea of sharing their biometric information — and there is reason for caution. For example, in 2015, 5.6 million federal employees in the US government had their fingerprint scans **stolen in a hack**.
- **HIGH COST** Implementing biometric readers on devices and installing systems is relatively expensive compared to using passwords. Of course, once everything is set up then (as noted above) it's **fast and easy**. But getting there isn't cheap.
- **LACK OF ACCURACY** Biometrics are not flawless. Some problems include partially capturing data, rejecting authentic users, and most troubling of all: false acceptances.

The Road Ahead

Biometrics are here to stay. However, there's still **a lot of work to do**. To get mass adoption, they need to be less expensive to install and operate, more secure, and more accurate. Even though biometrics grow in popularity, passwords are also here to stay. I don't see the day when we are going to log on a distant server on Linux with a simple retina scan. While end users might prefer biometrics, IT pros and sysadmins need to keep using strong and secure passwords for their daily tasks.

So, what's your opinion? Does your organization use biometrics, and if so, has the experience been positive or negative (or a mix of both)? And what do you think about the future of biometrics? Please share your views below.