IDEMIA

Where does biometric access control system matter most?

When it comes to strengthening access control, biometric authentication is the most reliable option. It bolsters security, creates next-level convenience and most importantly, can adapt to a wide range of use cases.

# ACCESS CONTROL

POSTED ON 12.03.21

Whether used to protect high security locations such as a military briefing room, the control center of a nuclear plant or the air traffic control tower of a busy international airport, or common everyday environments such as a hospital's database or proprietary documents in any number of corporate offices, biometrics prevents security breaches and ensures proper operation.

Regulations and the need for biometric authentication

While biometric access control systems clearly stand out as the go-to technology to ensure top-of-class security in many sectors, in many countries their use is strictly regulated. Companies must prove to regulatory bodies that they have just cause to integrate biometrics into their access control systems and that they are **doing it properly**—and this is a very good thing. In Europe, the GDPR regulation, enforced in each country by the local Data Privacy Authority, requires companies to **justify the need** for biometric systems and guarantee the **safety and privacy** of stored data. Other countries use similar regulations or are considering to.

Identity management: false acceptance vs. false rejection

Once a company has duly completed the evaluation to install a biometric authentication system, they need to **decide on the level of security** they want to achieve.

When identity management stakes are particularly high (in the case of a nuclear plant or an air traffic control tower), decision makers tend to opt for a lower rate of false acceptance to ensure that an unauthorized third party can never accidentally be granted access. Concretely speaking, an authorized person may need to scan their biometric data a second time before positively verifying their identity—a brief inconvenience that is accepted given the potential risks. This is where the algorithm strength comes into play: high performing solutions take into account the stakes of each situation and help **strike the right balance**.

Access control systems for extreme conditions

The need to strengthen access control and identity management is not limited to temperature-controlled buildings. Sensitive operational sites can also be outdoors, such as industrial plants, mines or seaports. In order to protect these sensitive assets, the best suited biometric authentication devices are **specifically ruggedized to cope with these harsh environments and weather conditions**. They can operate reliably despite snow, rain, dust, salt mist. They are also protected against impact damage and resistant to vandalism.

The ever-present need to protect critical facilities, data, innovation and proprietary information will continue to **drive biometric technology adoption forward, indoors and outdoors**. Whether it’s biometrics in healthcare, biometrics in banking, or in any number of industrial sectors, biometric access control systems have already proven their worth and are essential to protect sensitive sites.