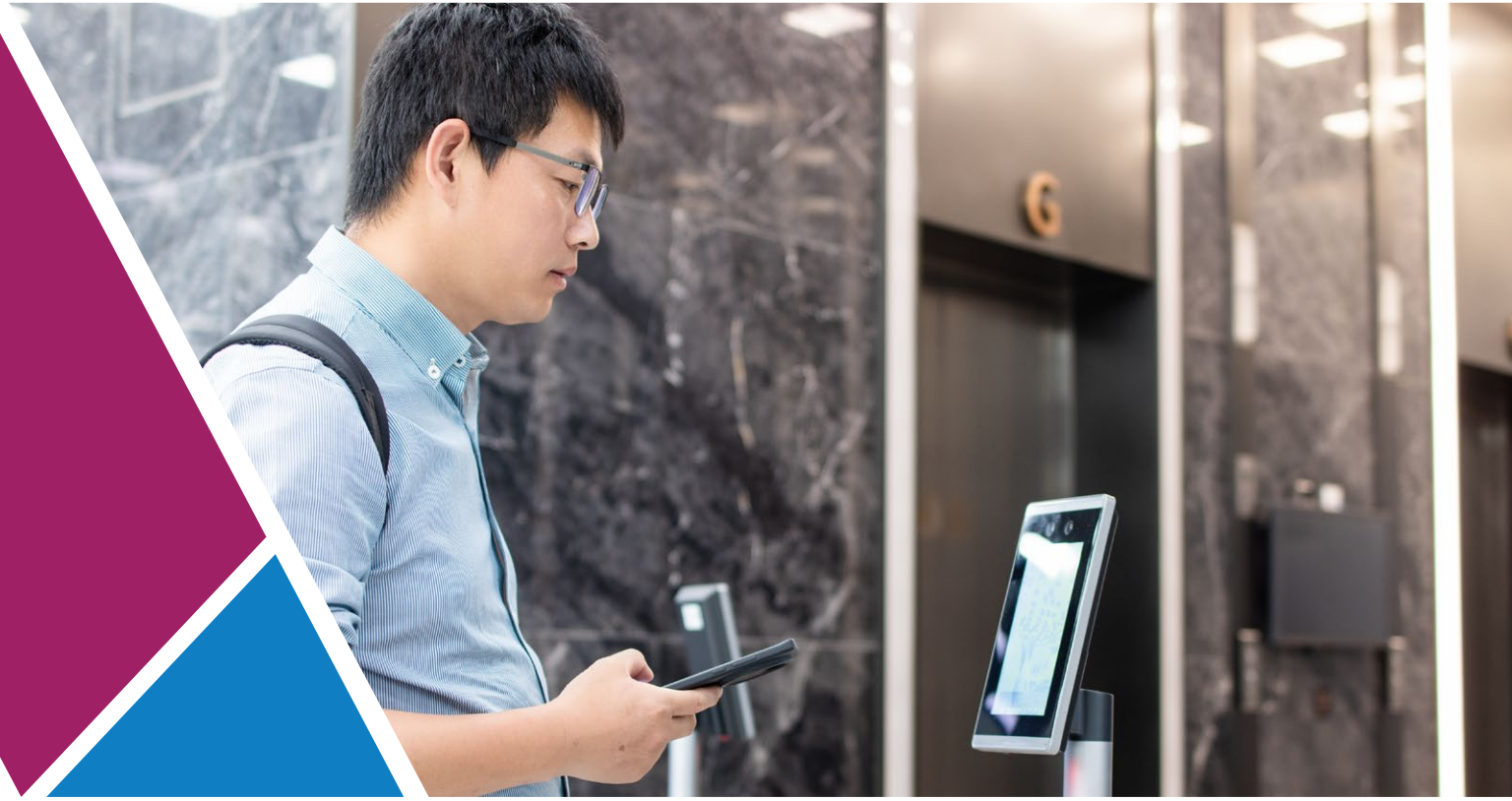
2026 Biometric Physical Access Control Market Report & Buyer's Guide

by Biometric Update and Goode Intelligence



BIOMETRIC UPDATE.COM

GOODE INTELLIGENCE
YOUR PARTNER FOR BUSINESS RESEARCH & ANALYSIS

Biometric Physical Access Control Market Report & Buyer's Guide

Biometric physical access control plays a critical role in securing facilities, infrastructure and restricted environments to protect organizations from physical and cyber threats. To help demystify this market, Biometric Update and Goode Intelligence have partnered on a report addressing the forces and changes shaping this growing segment.

Physical access control determines whether a person is authorized to enter a building or secure area. Automated systems include electronic doors, turnstiles and gates, along with cameras or scanners that capture credentials to authenticate identity and confirm authorization.

Organizations deploy biometric physical access control to increase identity assurance and security, improve convenience, meet regulatory and audit requirements, or achieve a combination of these benefits. Rising identity fraud, theft and regulation are expanding adoption beyond traditional government and critical infrastructure use cases into enterprise, healthcare, education and commercial environments.

Biometric physical access control systems use fingerprints, irises, facial recognition, or emerging modalities such as contactless palm biometrics, either alone or combined with other authentication factors.

This Biometric Update / Goode Intelligence report explains the key concepts in biometric physical access control, presenting commercially available technologies organizations can deploy today, and guiding them in selecting a provider.

The study also investigates the market for biometric physical access control hardware and software, including adoption examples, sector and application analysis, and three-year forecasts for transactions and revenue.

About Biometric Update and Goode Intelligence

This study has been created by a partnership bringing together Biometric Update and Goode Intelligence to produce analytical market reports stakeholders can use to make informed strategy, product and technology procurement choices.

Reports produced by the partnership are based on analysis of recent transactions and trends in the biometrics market, reviews of the regulatory, standards-development and competitive landscapes, and feedback from key insiders in each given area of focus.

Biometric Update is the world's leading source for daily news, opinion and insight into biometrics and digital identity.

Goode Intelligence is the world's leading independent biometrics market analyst and consulting firm, providing quality advice to global decision makers in business and technology.

Executive Summary

Organizations use access control to ensure that only people authorized to enter a particular area or resource are able to do so, typically but not exclusively for safety and security reasons. Access control is therefore a decision based on authorization, which bestows privileges on a given individual or set of individuals.

In enterprise contexts where access privileges are shared by and amongst large numbers of people, automated access control systems require an electronic credential to establish authorization. This historically has often meant devices like physical employee badges or ID cards. But these physical credentials can be stolen or spoofed, undermining their security value. Biometrics are therefore increasingly adopted in physical access control systems to authenticate the individual seeking access based on the inherence factor (often described as "something you are").

Biometrics can be added to existing physical access control systems or deployed as part of complete end-to-end systems.

The Biometric Physical Access Control (BPAC) market, therefore, is served by a combination of vendors selling biometrics components for integration with existing systems and access control providers offering complete solutions.

The market is somewhat mature, as the widespread introduction of biometrics in physical access control was spearheaded by critical infrastructure sites and airports in the early 2000s. The market is still evolving, however, as new technologies make the deployment choices facing organizations increasingly complex.

Biometric physical access control systems can improve the security, regulatory compliance and operational efficiency of organizations in a wide range of sectors, but success is conditional on selecting the appropriate technology and careful deployment.

Terms and Definitions

Authentication
The process of verifying a person's identity before granting them access to a site, system or service. Whereas identity verification matches a person with proof that they are who they say they are (for example, an ID), authentication confirms a claim to a previously established identity, and in this case that a person has been granted permission for access.

Biometric
A unique and measurable physical characteristic, such as a fingerprint, facial geometry, or palm vein pattern. In biometric physical access control systems, biometrics work like keys.

Biometric Physical Access Control (BPAC)
Limiting access to a physical space or resource through the use of biometrics such fingerprints or facial scans. Also sometimes rendered as BIOPAC.

BIPA
The state Illinois' Biometric Information Privacy Act, which sets strict rules on the collection and use of biometrics.

Compliance
Demonstrably following laws, rules and regulations, or standards applied in a given jurisdiction.

Credential
In the context of physical access control, the credential is the thing (token) used to authenticate the person requesting access. These credentials can come in many forms, including physical items like cards and fobs, wearables like wristbands, or digital formats like mobile credentials. A biometric is considered an access control credential.

Data Protection Impact Assessment (DPIA)
A formal assessment of how proposed data processing activities will affect the protection of personal data. It should include statements of purpose, proportionality and risks.

Facial Recognition
Machine learning technology that analyzes face biometrics and matches them against a database of images, in order to find a match.

GDPR
The European Union's General Data Protection Regulation is its primary data privacy and security law.

'Greenfield Site'
A UK term referring to a development project not subject to constraints imposed by prior work.

Identity Management
The processes, protocols and systems for the administration of individual identities within a system or organization.

Liveness Detection
Machine learning technology designed to ensure someone requesting access is a real, living and present human, and not a fraud. Face liveness detection may analyze things like blink patterns, skin tone, shadows, glare and visual noise. Other liveness technologies measure indicators like voice cadence or blood flow.

Logical Access
An automated system that controls access to computer system resources such as workstations, applications or databases.

Modality
The type of biometric leveraged for a particular use case. Biometric modalities include face, fingerprint, palm, iris, gait, vein pattern, DNA and more. Multimodal systems use more than one biometric.

NIST
The U.S. National Institute of Standards and Technology.

Personally Identifiable Information (PII)
Any data that can be used to distinguish or trace an individual's identity, and thus has special legal protections. Biometrics are a type of PII.

Physical Access Control Systems (PACS)
Security that controls who enters or accesses a physical space or resource.

Spoof
A falsified or fake biometric used to try and fool a BPACS; for instance, a silicon fingerprint.

'Tailgating'
When an unauthorized person follows an authorized person to gain access to a restricted space.

Introduction to Biometric Physical Access Control

Biometric physical access control refers to systems that use biometrics as a key or trigger for access to a specific location. BPACs enable a subject to enter a restricted area with their biometric that represents "something you are." BPACs are deployed in a variety of scenarios, to credential those who are authorized entry and manage the movement and access of those who are not. A biometric can be used in addition to an existing access control credential, a card or a phone, in two-factor mode, or as a stand-alone credential.

Popular biometric modalities for physical access control systems

The choice of what modality to use for BPACs is dependent on a number of criteria including regulation, risk appetite, environmental factors (does it need to work in the dark or challenging conditions), integration factors (will it work with what I currently use), and user experience factors.

Face is increasingly the preferred biometric modality for many physical access control scenarios, given its contactless functionality. Face biometrics fulfill the demand for fully contactless authentication that is very difficult to bypass. Facial scans have notably been used by the National Football League (NFL) for biometric credentialing and access control at select stadiums.

Fingerprint sensors and scanners are now mass market technology, easy and inexpensive to acquire. Fingerprint biometrics became problematic during the COVID-19 pandemic, when concerns about illness transmission pushed a pivot to contactless solutions. However, fingerprints continue to be a common modality for biometric physical access control, with a growing market.

Iris recognition systems capture an image of your eye using infrared light, and apply mathematical pattern-recognition techniques to the random pattern in the iris to create a unique digital code, which is enrolled into a database for storage and subsequent rapid matching. The high amount of data contained in the patterns of the iris muscle makes the iris effective for high-security verification. Iris recognition is deployed for airport screening and other high-security applications.

Emerging modalities: palm, vein, dual solutions

Palm prints, palm and finger vein patterns are also used in some biometric access control systems, but less commonly than face, iris or fingerprint biometrics – for now.

Palm prints can function like larger fingerprints containing more data. They can offer affordable biometric security for high-traffic access points.

Vein matching or vascular biometrics analyzes the patterns of blood vessels under the visible surface of the skin. Like facial scans, palm vein recognition, fingerprint vein matching and other vascular biometric tools provide contactless authentication. This can mean less wear on devices, and fewer issues with surface-level irregularities in skin.

Palm prints are often combined with palm veins for stronger security scenarios, including payments. Amazon tried out palm payments with its Amazon One technology in Whole Foods markets, but recently shut down the project, citing limited customer adoption.

However, combined palm print and palm vein biometrics continue to see deployments, partciularly for payments, as well as patient check-ins for health clinics, and palm authentication for identity verification on blockchain networks. As a multi-biometric system, combined palm print and vein scanners are also used to secure sensitive worksites like data centers and power plants.

For high-risk BPAC deployments, multiple modalities can be combined to provide layered security. For instance, access to a highly restricted area could require both a facial scan and an iris scan, or a voice match and a fingerprint scan.

Physical and logical access control converging

Physical access control remains distinct from logical access control, which governs access to data and computer systems. However, as organizations seek streamlined solutions with minimal friction, and increasingly adopt passwordless options for logical access control, there is growing convergence between the two streams toward systems that integrate both physical and logical access. A single authentication might, for example, allow a doctor access to both a room and a computer system at once. Or a single authentication might unlock both doors and desktops.

Convergence, as it is known, can reduce costs and time associated with managing multiple access control systems.

Integrations for Surveillance, Time & Attendance

The convergence of physical and logical access control enables deeper integrations of security and surveillance capabilities across physical and digital spaces. While a BPAC may monitor who is allowed in based on credentials, it could also connect to a database of known threats.

Biometric physical access control systems can support Time and Attendance systems, to help manage practices around employee scheduling and workforce control. Biometric-based time and attendance systems narrow the margin for human error, and can streamline payroll and operational efficiency by significantly reducing processing time. Applications span use cases from logistics depots to construction sites to moving between office terminals.

Audited and compliant solutions

Increasingly complex access control audit requirements and modern compliance frameworks demand comprehensive documentation. BPACs can also be used to maintain compliance in highly regulated sectors and sensitive scenarios, through blockchain-enabled auditability.

For instance, biometrics can be used to secure access to medical cabinets and secure storage units designed for housing supplies and controlled substances in healthcare settings. Another example is biometric gun safes and cabinets. BPACs can log each access attempt, providing a detailed, easily traceable data trail for audits.

Standards and Testing

Physical access control standards

The access control sector has developed a mature set of operational and technical standards. Some are specific to physical access control, though many include physical access as a consideration or aspect of overall or logical access control.

International standards have been developed by organizations, mainly ISO/IEC. In some cases national standards bodies have supplemented them with additional standards or guidance.

There are also independent or regional level bodies that set standards for access control and adjacent areas like cybersecurity. American test lab Underwriters Laboratories (UL), for example, has established access control standards used throughout North America.

Organizations deploying BPACs should also consult their local data protection and privacy laws early in the process to ensure that they do not expose themselves to regulatory complaints or liability.

ISO/IEC

ISO/IEC 27001 is a technical standard for information security management systems (ISMS). Physical access control is included as one aspect of comprehensive ISMS. Annex A of the 27001 standard lists 93 control measures organizations can put in place to protect physical access. These measures are divided between organizational, people, technological and physical controls. Certification to ISO 27001 is granted through an audit by an accredited body.

UL

UL 294 is a standard for end-to-end access control system integrity, which recognizes a range of levels of security and defines testing and certification requirements.

SIA

The Security Industry Association (SIA) has developed several standards related to physical access control, including for PVC access control cards and a "protocol for the 26-BIT Wiegand Reader Interface."

The SIA's BIO-01-1993.02 defines biometric terminology, but does not set technical requirements. The SIA TVAC-01-2001.04 standard specifies an interface protocol for communications between CCTV and access control subsystems.

Most important among the SIA's standards from a biometric physical access control perspective may be the Open Supervised Device Protocol (OSDP). OSDP is an interoperability standard for security and access control systems. OSDP v2.2.2 was released in October 2024.

Key biometrics, identity and security standards standards

The ISO/IEC 30107 standard for biometric presentation attack detection (PAD) provides important assurance of the security of the system against spoof attacks. It provides criteria for compliance testing, which is performed by accredited biometrics laboratories.

NIST SP 800-53 provides guidance for "Security and Privacy Controls for Information Systems and Organizations."

Section PE-2 provides guidance on physical access authorizations, including the advice that "(f)or gaining access to facilities using automated mechanisms, organizations may use PIV cards, key cards, PINs, and biometrics."

Section PE-3 specifically addresses physical access control, and includes "biometric readers" among the physical access devices appropriate for enforcing controls.

SOC 2 is a standard for secure data management. Within the standard, Common Criteria (CC) 6.1 requires that the security system identifies and authenticates users and CC6.4 stipulates that physical access to facilities and protected information assets must be restricted to authorized personnel. Certification to the SOC 2 framework is performed by accredited auditing firms.

Privacy and data protection regulations

Biometric physical access control involves the use of personal information by definition. It must therefore comply with the data privacy and protection laws and regulations of the jurisdiction in which it is taking place.

The European Union's General Data Protection Regulation (GDPR) sets requirements for the use of "special category data," which includes biometrics. Organizations must have a legal basis for processing the data, complete a data protection impact assessment (DPIA) and follow limitations regarding how the data can be used and how long it can be stored for.

GDPR also states that organizations should implement biometric liveness protection to prevent fraud (article 32), codifying a best practice.

GDPR is generally considered the most stringent data protection regulation that international organizations must

be aware of, and GDPR compliance also ensures compliance with the regulatory obligations for operating in many other jurisdictions.

UK GDPR very closely follows the EU version.

In the United States, data protection rules differ from state to state. Illinois' Biometric Information Privacy Act (BIPA) stipulates that written, informed consent must be collected from any individual prior to capturing their biometric data. Informed consent includes a shared schedule for data retention and a publicly available data retention policy.

Illinois' BIPA grants a right of private action to plaintiffs, and has resulted in numerous lawsuits against organizations using biometric physical access control.

Other states have adopted or are considering similar regulations, including Texas, Washington and Missouri, and others have more general data protection regulations that should be considered when implementing biometric systems for access control.

They generally require organizations to collect consent from individuals before capturing their biometrics.

Commercial establishments like retailers may also be subject to municipal regulations regarding public biometrics use in places like Portland, Oregon and New York City.

Businesses operating biometric physical access control systems should therefore take care and consider consulting a compliance professional to ensure they do not expose themselves to liability under local regulations.

Whether at the national or sub-national (state or provincial) level, data protection laws that could impact physical access control systems, the use of biometric data or both are in place in most jurisdictions around the world. It is therefore important to clearly understand local data protection and privacy laws before deploying biometric physical access control systems.

Bespoke and integrator testing

Several businesses operating consulting or security system integration services also provide testing for biometric physical access control systems.

Biometrics laboratories like BixeLab and Ingenium Biometric Laboratories carry out testing and validation services for BPACS.

Industry publication IPVM carries out vendor comparisons and technology evaluations for its own research reports.

Integrators like Anixter carry out operational performance testing for clients to help them select technologies, including for BPACS.

Biometric Physical Access Control Market Analysis

This section investigates key drivers for adoption, important sectors, and applications for the adoption of biometric physical access control, and adoption examples around the world.

Key Drivers

The four key drivers for biometric physical access control are:

1. Security
2. Convenience
3. Cost savings
4. Tighter integration with other physical security applications

Security

Biometrics used for physical access control provides an additional layer of security. You know who is entering your building versus authenticating a card or someone knowing a PIN. Biometrics can be used as part of a two-factor authentication (2FA) solution with a card, what you are and what you have, or standalone – you are the key. Certain biometric modalities, face in particular, when used in a physical access control system can be used to detect and prevent tailgating.

Convenience

Biometric physical access control enables a convenient user experience. You always carry your biometric with you and walking through a gate or opening a door without having to find an access control token (card, fob, or mobile), offers more convenience over other physical access control solutions.

Cost Savings

Biometrics offer potential cost savings when replacing other physical access control solutions, including card-based access control systems. In token-less scenarios, it can reduce maintenance functions, e.g., no card / token to manage and replace. When deployed smartly, it can also lead to reception-less entrances and can replace physical barriers and gates.

Tighter Integration with other Physical Security Applications

The ability for tighter integration with other physical security applications including surveillance and safety especially when face is the modality used. Modern face biometric PACS can detect and prevent tailgating as the camera can be monitoring this activity.

Key Sectors

Key sectors that are leading the way with adoption of biometric physical access control are:

1. Office
2. Residential
3. Government
4. Healthcare
5. Transport
6. Education
7. Technology, including data centers.

Office

Biometrics for physical access control systems is an active area for adoption with examples being seen around the world for both greenfield sites (new builds) and existing office buildings of all sizes.

Newer, AI-powered, biometric physical access control solutions are enabling all sizes of office buildings to be able to deploy the technology. The ability to easily integrate biometrics into existing physical access control systems (PACS) is a major driver for adoption.

It also offers greater potential for hybrid physical / logical access control systems where a biometric can be used to gain access to office buildings and then to sign-in to digital resources.

Residential

As well as adoption for high-end residential property, especially apartments that need to manage multiple residents entering an external door, there is growing availability of inexpensive biometric-enabled door lock equipment that can be purchased from major retailers for under $50 and can be easily integrated by either the home owner or a locksmith.

A significant proportion of activity is aligned with the smart home movement with connected and integrated home devices. For this sector, support for Apple, Google and Amazon home automation solutions is an important consideration.

Government

Governments have been adopting biometrics for physical access control for decades largely to support access to buildings and rooms that require high security and high assurance technology.

This is across most government departments but especially those aligned with higher levels of security including defense and law enforcement.

Typically, they will be deployed in line with government security policy including NIST standards for physical access control, found in SP 800-53 and SP 800-171, and the German KRITIS Umbrella Act (Kritis-Dachgesetz).

For high-security deployments, iris and retina biometrics are popular modalities as these are difficult to copy and offer a high level of accuracy.

Healthcare

Healthcare includes access control for medical centers (hospitals etc.) and also for the pharmaceutical and biotech sectors. A combination of industry regulation, including HIPPA in the U.S., and high-security requirements to control access to medically sensitive areas creates demand for biometric physical access control systems.

Controlled substances are subject to rigorous regulation within healthcare facilities, given their significant potential for abuse, dependence, and adverse outcomes when improperly managed. Institutions are mandated to enforce strict protocols for the storage and handling of these medications, including comprehensive tracking systems to monitor their distribution throughout the facility.

An important factor is hygiene for healthcare facilities and this means that there is a demand for touchless biometric physical access control systems. Modalities including iris and face are popular for healthcare PACS. Healthcare is also an environment where masks, rubber gloves, safety glasses are commonly worn and this has to be taken into account when deploying biometric technology for healthcare physical access control.

Having said that, technology suppliers do offer fingerprint access control solutions specially aimed at environments that wear latex and rubber gloves.

Transport

Biometric physical access control for transportation is not about authenticating travellers but the people that are involved in working in the transportation industry, especially where that is considered to be critical national infrastructure. This includes access control for airport, rail, and marine (sea travel and sea cargo) industries. Additionally, access control for the commercial haulage / logistics industry.

Education

Education organizations, schools, universities and colleges are increasingly turning to biometrics to secure their facilities.

These systems can be integrated with other security tools like CCTV and alarm systems to provide comprehensive security management and a complete audit trail of access events.

They can also be linked to education digital identity where other applications can 'hang' off the biometric including payment in canteens and refractories.

Biometrics can augment or replace token-based (mainly card) access control in education facilities.

Fingerprint and face are popular modalities for education biometric physical access control.

Technology

The protection from unauthorized access to buildings and rooms that house technology is a critical factor. This includes data centers and telecommunications centers. The physical security of data when stored and in transit is a fundamental component of cybersecurity policy.

As biometrics provides a high level of security and assurance for physical access control systems it is an important technology for information security.

High assurance modalities including iris and vein are popular modalities in protecting technology, in addition to fingerprint and face.

In data centers, these biometric systems are typically integrated with other security measures to create a robust, multi-factor authentication (MFA) system.

Biometric Physical Access Control Forecasts

Introduction

Market forecasting is very important in the Goode Intelligence (GI) research and analysis methodology especially when dealing with new or emerging markets and products.

GI has an excellent track record of forecasting in emerging technology areas including correctly predicting the growth of the mobile as an authentication device in 2009, the emergence of biometrics on mobile devices in 2011, and the growth in digital identity in 2015.

Market forecasting is one of the tools that GI uses in predicting the degree of success a new product or service will enjoy in the marketplace. The GI methodology considers areas such as product awareness, distribution, price, fulfilling unmet needs and competitive alternatives.

GI creates forecasts by gathering data from diverse sources like company filings, economic reports, and direct interactions (interviews) with both suppliers and buyers, some of which are bound by NDAs. GI then applies both quantitative methods and qualitative assessments (such as expert opinions) within financial models. These models are designed to estimate future performance by incorporating macroeconomic factors, industry trends, and company-specific details to provide a comprehensive view of expected growth and profitability.

Revenue forecasting at Goode Intelligence (GI) involves collecting data from a variety of sources such as company filings, economic reports, and interviews with suppliers and buyers, often under NDA. This information feeds into financial models that use both quantitative and qualitative methods, including expert opinions, to project future performance. These models consider macroeconomic factors, industry trends, and company-specific details. For revenue projections, GI calculates an average price, taking into account the variability in vendor pricing and potential discounts. The result is a comprehensive estimate of expected revenue growth and profitability for new or emerging products and markets.

We always welcome feedback from readers on the accuracy of the forecasts and are open to reflecting your opinion in future reports.

The forecasts are taken from the Goode Intelligence market analyst and forecast report on biometric physical access control.

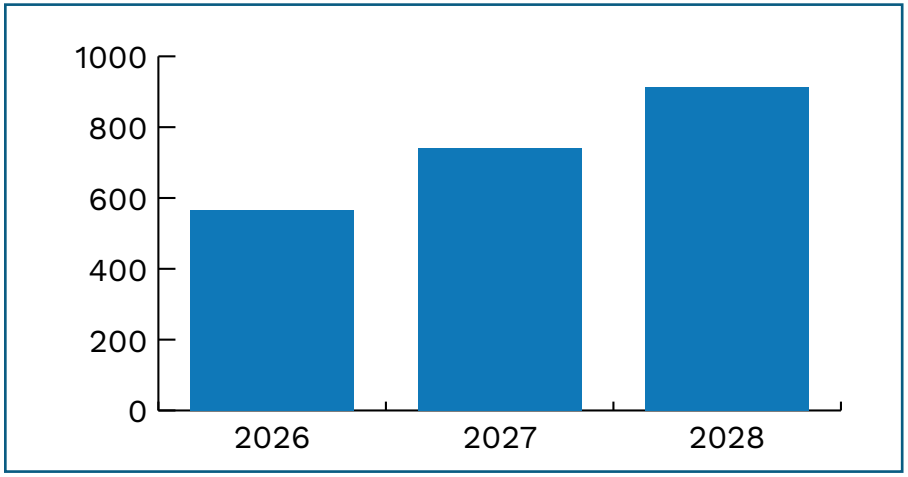
There are three-year forecasts, 2026-2028, covering:

1. Total Biometric Physical Access Control Users
2. Total Biometric Physical Access Control Revenue

Biometric Physical Access Control – Total Users

These forecasts are for total global biometric physical access control users.

Chart 1: Biometric Physical Access Control Forecasts: Total Global Users (m)



Source: Goode Intelligence © 2026

Table 1: Biometric Physical Access Control Forecasts: Total Global Users (m)

	2026	2027	2028
Total	566.66	740.69	913.34

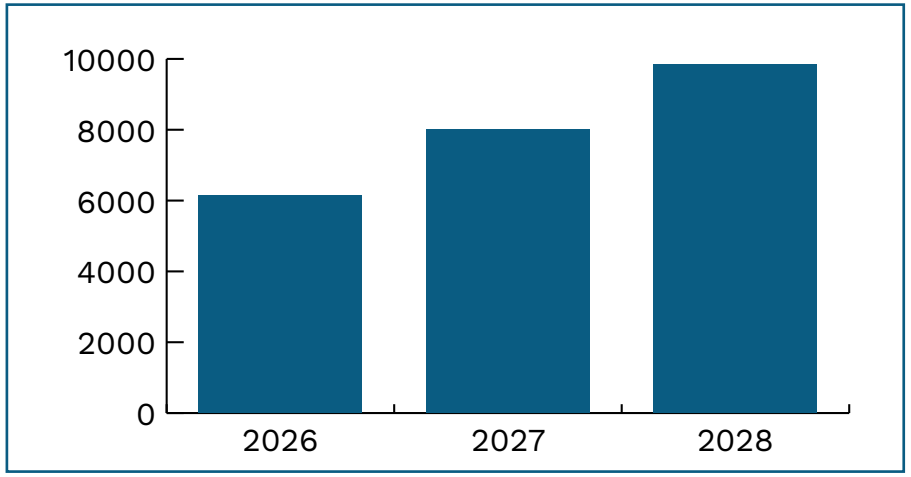
Source: Goode Intelligence © 2026

Total Biometric Physical Access Control Users will exceed 913 million by 2028

Biometric Physical Access Control – Total Revenue

These forecasts are for total biometric physical access control revenue in US Dollar (million).

Chart 2: Biometric Physical Access Control Forecasts: Total Global Revenue (US$m)



Source: Goode Intelligence © 2026

Table 2: Biometric Physical Access Control Forecasts: Total Global Revenue (US$m)

	2026	2027	2028
Total	6133.77	7995.69	9845.07

Source: Goode Intelligence © 2026

Biometric Physical Access Control Revenue will exceed $9.84 billion by 2028

Biometric Physical Access Control Buyer's Guide

This section provides potential buyers of biometric physical access control products and services with a guide to how to assess solutions. It also includes sections on deployment considerations.

The buyer's guide has separate sections for SMB and Enterprise buyers as there can be differences in deployment considerations and buying criteria between the two segments. There will also be overlap between deployment considerations and buying criteria between the two segments.

It is important to note that this guide should not be used as the sole method for assessing biometric physical access control solutions as that is based on an organization's individual and specific requirements that should be included in a comprehensive assessment.

The buyers guide also includes a list of biometric physical access control vendors (suppliers) that are active in the market. For a select number of vendors, there is a profile of the company and their products.

Biometric Physical Access Control Buyer's Guide (SMB)

This section provides potential SMB buyers of biometric physical access control products and services with a guide to how to assess solutions. It also includes sections on deployment considerations.

Deployment Considerations for SMB Buyers

SMB buyers of biometric physical access control should be aware of the following deployment considerations.

System Integration

Ensure compatibility with existing Video Management Systems (VMS), alarms, and HR software.

Support for Legacy Systems

Does the biometric solution easily integrate with existing (legacy) physical access control systems.

Scalability

The system should grow with your business, supporting additional doors or users without complete overhaul.

Authentication Speed

The system must process users quickly to avoid bottlenecks in high-traffic areas, which is crucial for employee productivity.

Multimodal Options

Consider using multiple biometrics (e.g., face + palm) for higher-security areas, or pairing biometrics with smart cards for multi-factor authentication.

Ease of Deployment / Use

Is the solution easy to deploy and easy to use without the need for costly specialist staff?

Visitor Management Support

Can visitors make use of convenient biometric enrolment at home / enroute to streamline their visit?

Balance Security with Affordability

SMBs should prioritize solutions that balance high-level security with affordability, ease of use, and scalability.

Reduced Administrative Overhead

Biometric systems should reduce time spent by staff managing credentials and reissuing lost badges, providing faster ROI.

HR/Payroll System Integration

Many biometric systems can sync with time-and-attendance software, eliminating "buddy punching" and automating payroll.

Choosing a Biometric Physical Access Control Supplier (SMB)

This section provides potential SMB buyers of biometric physical access control products and services with a guide to how to assess solutions.

It is important to note that this guide should not be used as the sole method for assessing biometric physical access control solutions as that is based on an organization's individual and specific requirements that should be included in a comprehensive assessment.

The buyers guide also includes a list of biometric physical access control vendors (suppliers) that are active in the market. For a select number of vendors, there is a profile of the company and their products.

Biometric Update and Goode Intelligence strive to provide accurate information, but we must point out that our list of vendors is not comprehensive. We have selected a representative group of vendors, but we do not guarantee that our list is exhaustive. The analysis is presented on a "best efforts" basis, and we cannot accept any liability for any errors or omissions.

If a vendor considers that we have unreasonably omitted them then there is an opportunity for them to engage with Biometric Update and Goode Intelligence for inclusion in subsequent editions of this report.

What to Look for in a Biometric Physical Access Control Supplier (SMB)

This section provides a guide for SMB buyers on what to look for in a biometric physical access control supplier.

It is important to repeat that this guide should not be used as the sole method for assessing biometric physical access control solutions as that is based on an organization's individual and specific requirements that should be included in a comprehensive assessment.

This report identifies the following baseline criteria for measuring whether a biometric physical access control solution or product is suitable.

1 **Cost:** Does it meet your budget expectations: This is especially important with hardware based deals that include installation, maintenance and replacement fees. If the deal is linked to an identity and access management solution, then does the fee involve a per-user fee.

2 **Technology Type**: Choose the technology and biometric modality based on security needs (e.g., iris for high security, facial for speed/hygiene, fingerprint for cost-effectiveness).

3 **Accuracy and Speed:** The solution should have high accuracy (low false positives and false negatives) and be able to process access requests in all physical conditions including low-light and wet weather. Can the solution deal with peak times, e.g. the start and end of a business day for office use.

4 **Liveness Detection:** Accuracy and Reliability - is it a certified / tested product? The main standard for testing liveness detection are the ISO/IEC 30107-3:2023 standard. This is considered to be "table stakes" when assessing whether a liveness detection solution is effective.

5 **Environmental Factors:** Consider if access control readers work in direct sunlight, high humidity, or extreme temperatures.

6 **Bias:** Ensure the solution has been tested for bias and is fair in its analysis of different types of presented biometric data.

7 **Security:** Does the supplier have physical security and cybersecurity certifications and adhere to guidance / best practice?

8 **Privacy and data protection compliance:** Does it meet EU GDPR and other state legislation related to the collection, storage and use of biometric data?

9 **Scalability:** The system should grow with your business, supporting additional doors or users without complete overhaul.

10 **Backup Solutions:** Ensure the system has fail-safe options like PIN codes or RFID cards if the biometric scanner fails.

11 **Contactless vs. Contact:** Consider contactless options (e.g., facial recognition) for hygiene-conscious environments.

SMB Featured Vendor Profiles & Case Studies

Biometric Update and Goode Intelligence have identified a broad range of vendors providing physical biometric access control technologies for small and medium-sized businesses. These solutions typically combine core technologies such as facial recognition, fingerprint authentication, mobile credentials, cloud-based access management, and standalone or networked door controllers.

The SMB segment is characterized by vendors focused on ease of deployment, cost efficiency, and simplified administration, often delivering cloud-managed platforms through channel partners and security integrators. As smaller organizations increasingly adopt modern physical security systems, it is important that vendors provide scalable solutions that can evolve from a single office deployment to multi-site environments without adding operational complexity.

HID

hidglobal.com
611 Center Ridge Drive, Austin, TX 78753
United States
(800) 237-7769

HID is a recognized leader in physical access control and trusted identity solutions, delivering secure, highly scalable systems that protect people, places, and assets. Its comprehensive portfolio spans credentials, readers, controllers, cloud-enabled platforms, and identity services that seamlessly unify physical and digital security across buildings, campuses, and industries – improving security, compliance, and operational efficiency.

Part of the ASSA ABLOY Group, HID is headquartered in Austin, Texas, with over 4,500 employees and international offices that support more than 100 countries. It boasts one of the access control industry's broadest ecosystems, with a wide network of software partners, system integrators and OEMs developing on top of HID readers, credentials, controllers and cloud platforms.

HID secures every layer of the access control stack, designing its products to offer maximum flexibility and choice for end users. Seos credentials deploy AES-128 with mutual authentication for anti-cloning protection; mobile credentials introduce the ability to revoke credentials remotely; Signo readers use certified secure element hardware to secure cryptographic keys and encrypt communication upstream via OSDP; and further upstream Mercury MP Controllers are subject to rigorous third-party penetration testing to proactively identify and address vulnerabilities before they can be exploited.

HID believes the next generation of physical security is defined less by hardware and more by how identity is managed and delivered. The siloed badge-for-buildings model is fading, and as the industry shifts from static cards to mobile-first credentials, integration must be seamless and flexible. Organizations are accelerating toward converged physical and logical credentials, driven by the need for a single identity that works consistently across doors, networks, and cloud applications. Coexistence by design ensures mobile credentials are deployed alongside physical cards, allowing users to adopt mobile access without disrupting existing workflows or infrastructure.

HID mobile access integrates with existing access control systems through secure APIs, minimizing system changes and avoiding rip-and-replace upgrades. For deployment, credentials can be provisioned through the HID mobile app, added to Apple Wallet or Google Wallet, or embedded via SDK into a HID technology partner's application.

Innovative Technology

innovative-technology.com
sales@innovative-technology.com
Innovative Business Park, Derker Street,
Oldham, OL1 4EQ, UK
+44 161 626 9999

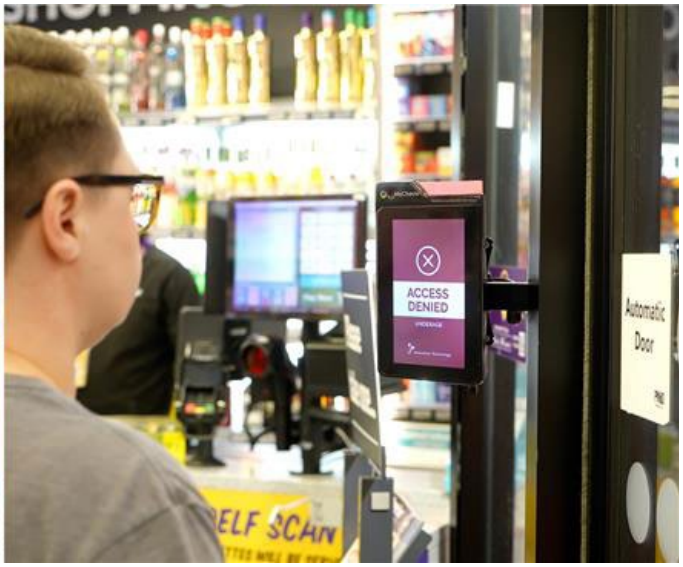
For over 30 years, the UK's Innovative Technology (ITL) has provided pioneering automation technology. With a dedicated biometrics division, the company offers a range of AI-powered age estimation and access verification technology, serving numerous industries across the UK, Europe and the U.S.

A wide range of sectors use ITL's technology to control access to age-restricted areas and products including retail and convenience, beer caves, lottery, gaming, casino, amusement and vending. Verification using 1:1 face matching with passports, ID cards, driving licences, membership cards or entrance tickets can be used by many sectors including AML applications, leisure and airport settings. For 1:N access control, ITL automates secure access control to buildings, safes or restricted areas, reducing the need for cards, fobs, pin codes or keys for any industry.

The MyCheckr hardware device can be mounted on a barrier, door, gate, kiosk, or any access point. The screen and LED turns green and automates entry if the person is over the set age threshold or verified with a database/ document, and red if predicted underage or no match is found. When linked to MyConnect customers can easily manage multiple devices from a single touchpoint. Notifications sent to an app of potential underage or unauthorised access attempts, remote approvals or denials, analytics and full management of employee and customer databases are all available via a customer friendly and intuitive platform. Its device-only pricing structure has no ongoing subscription fees. There is also an option to access an API for total software integration.

ITL builds, trains and tunes its own algorithms at their UK head office location to ensure high accuracy across all demographics and age ranges. Independent test results from Age Check Certification Scheme (ACCS) found that on average, ITL's technology overestimates 18-year-olds by 0.39 years and has an MAE (Mean Absolute Error) of 0.94 years. Facial analysis takes less than a second and does not require any cues or specific gestures from the customer, reducing friction and providing a seamless, non-intrusive customer journey. Passive liveness detection is designed to identify a valid face and reject any invalid or fraudulent faces such as a photo, video, 3D models, or any substitute for a live person's face. All processing takes place at the edge, enabling consistent and quick performance.

ITL's MyCheckr prevents underage access to Premier's Beer Cave



Background & Challenges

Premier is a large, fast growing group of independent retailers in the UK. Girish Jeeva owns a Premier located in Glasgow, Scotland. The store required a solution to help prevent underage customers accessing alcohol in a newly installed Beer Cave, to safeguard the business and reduce liability.

Project Plan

Following the success of ITL's age estimation technology at the till point, MyCheckr at the entrance to the beer cave was fitted.

Staff needed a mechanism to quickly react to underage customers trying to enter the beer cave without leaving the till point so MyCheckr linked with MyConnect was recommend.

How does it work?

The beer cave door is controlled by MyCheckr (set to 25 years). If a customer approaching the beer cave appears over 25, the door will automatically open with no interaction.

If a customer appears under 25 the door remains closed. MyCheckr is linked to MyConnect which sends notifications to the app on a tablet at the till point. The customer will need to show ID and once checked, staff can remotely open the door.

Results

- Frictionless, fast (< 1 second), non-intrusive age checks with automatic entry for those overage. Staff and regular customers can be added to the system for automated access
- Remote notifications allows efficient deployment of resources with more time to serve customers, audit logs and analytical data are also available
- Gives staff confidence to challenge underage customers, removing subjectivity, awkwardness and potential confrontation
- The appearance of MyCheckr acts as a theft deterrent, making potential shoplifters reconsider their intentions

Iris ID

irisid.com
sales@irisid.com
609-819-4747

With more than 25 years of national scale deployment expertise, New Jersey-based Iris ID delivers high assurance iris and face fusion multimodal biometric solutions, supporting large population identity systems worldwide. Its Iris ID solutions are deployed globally across North America, the Middle East, Europe, Africa, and Asia, and lays claim to being the world's leading deployed iris recognition platform.

Designed to meet strict government standards in multiple jurisdictions, Iris ID's technology is used by immigration and border control agencies, commercial entities, law enforcement, and national ID programs, as well as data centers, healthcare, research labs, energy utilities, and enterprise campuses. The confidential nature of its government and critical infrastructure deployments is a testament to a high level of trust from customers.

Iris ID's IrisAccess® iA1000 is a non-contact iris and face fusion authentication solution integrated with the IrisAccess Management System (iAMS), delivering true multimodal iris and face fusion at the algorithm level for superior accuracy and operational flexibility. Featuring iBeta Level 2 PAD compliant iA FacePAD v2.5.3 for advanced liveness detection, it delivers secure, privacy focused identity verification, augmenting PINs and cards with fast, accurate biometric authentication for access control environments. Its facial recognition algorithm recently made its debut on the National Institute of Standards and Technology (NIST)'s FRTE 1:1 Verification report.

For iris recognition, the iA1000 employs near infrared imaging combined with iris texture validation and natural ocular response analysis. The system analyzes authentic iris patterns, and image depth characteristics to differentiate between a live eye and artifacts such as printed eyes, cosmetic contact lenses or artificial representations.

Although Iris ID has been operating since 1997, the latest wave of AI technology is foundational to its current products, enhancing biometric accuracy, intelligent iris face fusion, and liveness detection while improving capture quality and overall system performance. Rather than replacing proven biometric science, AI augments it, strengthening security, defending against evolving spoofing threats, and enabling scalable, high confidence authentication in enterprise and national-scale deployments.

RealSense

realsenseid.com
sales@realsenseai.com
1+ 201.707.5518

RealSense delivers on-device Vision AI for biometric access control, combining advanced depth-sensing hardware with purpose-built edge AI software. Headquartered in Cupertino, California, RealSense builds high-performance vision systems that enable secure, touchless access and easy-to-deploy identity solutions for modern workplaces.

The company's solutions are designed for organizations that need strong security without added complexity or IT overhead.

RealSense ID Pro F500 is a compact, next-generation facial authentication solution designed for small and mid-sized businesses. It combines an active stereo depth sensor with a proprietary neural network to enable fast, reliable biometric authentication for doors, offices, and shared spaces. As an integrated platform, every component—from sensor to AI, is engineered to work together for security, privacy, and speed.

The system achieves 99.77% NIST-verified accuracy (1:1 verification) and is iBeta Level 2 & ISO 30107-3 PAD compliant, helping protect against spoofing while maintaining a seamless user experience. Authentication completes in ~300 milliseconds, enabling fast, touchless entry for employees and visitors.

Beyond facial authentication, ID Pro F500 includes advanced perception capabilities, such as person detection, body-part classification, and tracking, enabling smarter access control with features like presence awareness and improved entry-point security.

Privacy is built in. All biometric processing occurs fully on-device, with no storage of images or personally identifiable information. The device stores up to 10,000 encrypted faceprint templates, which cannot be reconstructed into original images, supporting GDPR-aligned data protection practices. Enrollment supports both on-device and image-based workflows.

Purpose-built for access control, the solution features a wide vertical field of view and consistent performance across user heights. Its compact form factor, just one-quarter the size of a credit card, makes it easy to integrate into existing door systems, kiosks, and entry points.

Use cases include offices, coworking spaces, hospitality venues, time and attendance, kiosks, ATMs, light manufacturing, and robotics. Touchless biometric authentication enables faster, more convenient entry, improving both security and user experience.

RealSense ID Pro F500 supports deployment via REST APIs and SDKs for Windows, Linux, and Android, enabling straightforward integration with existing access control systems and the flexibility to scale over time.

Secure Mobile Facial Authentication for On-the-Go Identity Verification

Powered by RealSense™ ID BioAffix® Gate Vision Mobile by Ones Technology delivers fast, secure, and portable biometric authentication for field operations and high-security environments. Designed for use cases where fixed access points are impractical, the handheld device enables non-touch facial authentication in under one second while maintaining strict privacy, accuracy, and regulatory compliance. RealSense ID and BioAffix® Gate Vision Mobile earned the 2025 SIA New Products and Solutions Award (Mobile – Biometrics) and the 2026 Intersec Award for Best Homeland Security Solution, recognizing Ones Technology's innovation in mobile identity verification.

Traditional mobile verification systems often rely on centralized databases or constant network connectivity, increasing exposure to breaches and compliance risks. BioAffix Gate Vision Mobile addresses these challenges by performing all biometric processing locally on the device at the edge. RealSense ID combines an active stereo depth sensor with AI-driven liveness detection and anti-spoofing, ensuring that only real, live individuals can be authenticated—even in the presence of deepfake or presentation attacks.

Unlike cloud-dependent solutions, biometric templates can remain under user control on secure credentials such as ID cards or mobile wallets, minimizing centralized data storage. This architecture supports GDPR and sovereign identity requirements while reducing cybersecurity risk in sensitive environments.

Built for demanding conditions, BioAffix Gate Vision Mobile operates online or offline and integrates easily with existing access-control systems. By integrating the RealSense ID F450, BioAffix® delivers accurate facial authentication across lighting conditions and demographics, in a compact, ruggedized device designed for law enforcement, border control, first responders, event security, and remote infrastructure—bringing trusted biometric authentication wherever it's needed most.

ROC

www.roc.ai
sales@roc.ai
1290 Broadway, Suite 1200, Denver, CO 80203

ROC is a leading U.S. developer and manufacturer of Vision AI, delivering sovereign biometrics, video analytics, and mission intelligence through a unified platform. Trusted for high-stakes identity and security operations, ROC helps organizations improve access assurance, accelerate investigations, and strengthen situational awareness with real-time, actionable intelligence. All ROC technology is designed and developed in the United States, supporting a mix of domestic and international customers and channel partners across North America, Europe, the Middle East, and APAC.

ROC security products and solutions are deployed globally and are sold through an expanding network of certified partners. Its physical access control product, ROC Watch, is a multimodal Vision AI and video analytics platform built to interpret video in real time and post-event, used by security, law enforcement and public safety teams, and in the commercial market, deployed across school campuses, commercial properties, and corporate facilities that require real-time awareness and defensible identity decisions in physical environments.

Suited for deployments where existing PACS/VMS and camera ecosystems are already in place and must remain operational across mixed vendor environments, ROC Watch enables real-time, frictionless access control using Vision AI and biometric identification from existing cameras. It sends identity-aware alerts to connected access control systems to grant or deny access based on who is physically present – not just a credential, which can be used fraudulently.

The product offers configurable workflows per door/zone/site (intent-to-access, proximity, tailgating/2-man rules, parallel crowd processing, lockdown rules for watchlist or weapon detection) and complements existing PACS/VMS, protecting prior investments and accelerating time-to-value. It is designed for real-world deployments and can operate across challenging, uncontrolled, dense or high-throughput environments, across a wide range of lighting conditions, camera angles, and environmental complexities.

Powered by NIST-ranked face recognition algorithms, ROC Watch supports layered access control and broader security workflows including badgeless visitor management, perimeter protection, gun detection, watchlisting, incident management, video forensics, and automated license plate recognition (ALPR), delivered through one integrated platform.

Biometric Physical Access Control Buyer's Guide (Enterprise)

This section provides potential Enterprise buyers of biometric physical access control products and services with a guide to how to assess solutions. It also includes sections on deployment considerations.

Deployment Considerations for Enterprise Buyers

Enterprise buyers of biometric physical access control should be aware of the following deployment considerations.

1. Cost and Maintenance
3. Compliance
4. Security
5. User Experience
6. Performance
7. Integration

Cost and Maintenance

It is important that Enterprise buyers investigate the Total Cost of Ownership (TCO) considerations when deploying biometric physical access control systems. Enterprise buyers should look beyond the initial hardware costs and include software licenses, training, ongoing maintenance and replacement in their assessment.

Equally, it is important that buyers future-proof their investment by investing in scalable, modular systems that can grow with your organization and allow for easy component upgrades.

Compliance

It is important that buyers are compliant with state and federal data privacy. This is particularly important when collecting, using, and storing biometric data. Biometric data is classified as sensitive Personally Identifiable Information (PII). In the EU/UK, GDPR mandates strict consent, while in the US, BIPA (Illinois) and other laws require explicit written consent.

It is recommended that a Data Protection Impact Assessment (DPIA) is conducted at the beginning of the deployment project to justify the use of biometrics and ensure the collection is fair and proportionate. This includes establishing clear policies for deleting data once an employee leaves or consent is withdrawn.

Security

Security is at the core of biometric physical access control systems so it is imperative that buyers ensure that their solutions are secure. A vitally important consideration with biometric systems is to ensure the system does not store actual images of fingerprints or faces, but rather encrypted mathematical templates that cannot be reverse-engineered.

Additionally, does the supplier have physical security and cybersecurity certifications and adhere to guidance / best practice?

User Experience

Creating the right user experience for people accessing buildings and rooms is an essential consideration when designing a modern access control solution. With biometric solutions, buyers must consider how the enrollment process is implemented, ensuring that staff are adequately trained and how to support large decentralized workforces.

Performance

Does the system meet, and exceed performance requirements, especially at peak times.

In high-traffic areas, select systems with fast recognition speeds to prevent bottlenecks and research environment factors including an evaluation of the installation location. Fingerprint systems may struggle in high humidity or very dry conditions, while facial recognition may struggle with extreme lighting or, for some, face masks.

Integration

Especially important when adding biometrics to existing PACS, ensure that new biometric technologies integrate with existing systems. Ensure the new biometric system integrates with current HR, IT, and security software (e.g., VMS, alarm systems).

If you need support for integration, then choose an integrator that has proven experience of integrating biometric technology to physical access control systems.

Choosing an Enterprise Biometric Physical Access Control Supplier

This section provides potential Enterprise buyers of biometric physical access control products and services with a guide to how to assess solutions.

It is important to note that this guide should not be used as the sole method for assessing biometric physical access control solutions as that is based on an organization's individual and specific requirements that should be included in a comprehensive assessment.

The buyers guide also includes a list of biometric physical access control vendors (suppliers) that are active in the market. For a select number of vendors, there is a profile of the company and their products.

Biometric Update and Goode Intelligence strive to provide accurate information, but we must point out that our list of vendors is not comprehensive. We have selected a representative group of vendors, but we do not guarantee that our list is exhaustive. The analysis is presented on a "best efforts" basis, and we cannot accept any liability for any errors or omissions.

If a vendor considers that we have unreasonably omitted them then there is an opportunity for them to engage with Biometric Update and Goode Intelligence for inclusion in subsequent editions of this report.

This report identifies the following baseline criteria for measuring whether a biometric physical access control solution or product is suitable for an enterprise user.

1 **Cost:** Does it meet your budget expectations: This is especially important with hardware based deals that include installation, maintenance and replacement fees. If the deal is linked to an identity and access management solution, then does the fee involve a per-user fee.

2 **Technology Type**: Choose the technology and biometric modality based on security needs (e.g., iris for high security, facial for speed/hygiene, fingerprint for cost-effectiveness).

3 **Accuracy and Speed:** The solution should have high accuracy (low false positives and false negatives) and be able to process access requests in all physical conditions including low-light and wet weather. Can the solution deal with peak times, e.g. the start and end of a business day for office use.

4 **Liveness Detection:** Accuracy and Reliability - is it a certified / tested product? The main standard for testing liveness detection are the ISO/IEC 30107-3:2023 standard. This is considered to "table stakes" when assessing whether a liveness detection solution is effective.

5 **Environmental Factors:** Consider if readers work in direct sunlight, high humidity, or extreme temperatures.

6 **Bias:** Ensure the solution has been tested for bias and is fair in its analysis of different types of presented biometric data.

7 **Security:** Does the supplier have physical security and cybersecurity certifications and adhere to guidance / best practice?

8 **Privacy and data protection compliance:** Does it meet EU GDPR and other state legislation related to the collection, storage and use of biometric data?

9 **System Integration:** Ensure compatibility with existing Video Management Systems (VMS), alarms, and HR software.

10 **Scalability:** The system should grow with your business, supporting additional doors or users without complete overhaul.

11 **Backup Solutions:** Ensure the system has fail-safe options like PIN codes or RFID cards if the biometric scanner fails.

12 **Contactless vs. Contact:** Consider contactless options (e.g., facial recognition) for hygiene-conscious environments.

Enterprise Vendor Featured Profiles

Biometric Update and Goode Intelligence have identified a diverse group of vendors delivering physical biometric access control technologies for enterprise and high-security environments. These solutions combine advanced modalities such as face, fingerprint, iris, vein, and multimodal authentication with centralized management platforms, anti-spoofing capabilities, and integration into broader physical access control and identity systems.

The enterprise segment includes both biometric component suppliers and full platform providers serving corporate campuses, critical infrastructure, government facilities, healthcare systems, and data centers. As organizations move toward unified identity strategies that converge physical and logical access, it is important that enterprise biometric access vendors support scalable orchestration, compliance, auditability, and interoperability across complex environments.

Alcatraz

alcatraz.ai
10061 Bubb Rd, Cupertino, CA 95014, USA
408-513-4727

Alcatraz provides facial biometric authentication for access control in physical security, combining advanced AI at the edge and privacy-by-design to deliver frictionless, secure, seamlessly integrated access for global enterprises. The Cupertino, California-based firm is a pioneer of Facial Authentication-as-a-Service (FAaaS), and helps protect over four million employees (and counting) worldwide with a 95% customer satisfaction rating.

The company's flagship product is Rock X, a facial authentication device for physical access control, which uses 3D face scanning with liveness detection to verify identity with high accuracy and minimal friction. It includes AI tailgating / piggybacking detection, provides video and SIP intercom, and deploys seamlessly with existing access control systems as a standalone or multi-factor solution.

Alcatraz's plug-and-play biometric solution protects Fortune 500 companies and critical facilities worldwide, with deployments across North America, Europe, the Middle East and Asia-Pacific. Adoption is strongest in sectors with high security and compliance needs: data centers, technology companies, financial services, healthcare and life sciences and critical infrastructure (e.g., airports and utilities), universities and stadiums are all counted among Alcatraz's customers.

AI is central to Rock X's capabilities. The device's on-board machine learning AI drives real-time facial authentication, liveness detection, tailgating analytics and adaptive learning, powering the product's high security and efficiency. Privacy and compliance are built in on the design level, adhering to strict regulatory alignment with major data protection laws like GDPR and CCPA.

Rock X is fully agnostic and designed to plug into existing access control systems via open standards (Wiegand, OSDP) and native integrations with leading platforms. Most deployments require minimal configuration: just mount the device and connect it, to enable full functionality within hours. Alcatraz basically provides Facial Authentication as a service like nobody else.

Alcatraz believes there is a growing demand to unify physical and digital access, and to accommodate this, its open platform and APIs enable integration with logical access systems, allowing facial authentication to serve as a secure credential for both doors and digital systems.

HID

hidglobal.com
611 Center Ridge Drive, Austin, TX 78753,
United States
(800) 237-7769

HID is a recognized leader in physical access control and trusted identity solutions, delivering secure, highly scalable systems that protect people, places, and assets. Its comprehensive portfolio spans credentials, readers, controllers, cloud-enabled platforms, and identity services that seamlessly unify physical and digital security across buildings, campuses, and industries – improving security, compliance, and operational efficiency.

Part of the ASSA ABLOY Group, HID is headquartered in Austin, Texas, with over 4,500 employees and international offices that support more than 100 countries. It boasts one of the access control industry's broadest ecosystems, with a wide network of software partners, system integrators and OEMs developing on top of HID readers, credentials, controllers and cloud platforms.

HID secures every layer of the access control stack, designing its products to offer maximum flexibility and choice for end users. Seos credentials deploy AES-128 with mutual authentication for anti-cloning protection; mobile credentials introduce the ability to revoke credentials remotely; Signo readers use certified secure element hardware to secure cryptographic keys and encrypt communication upstream via OSDP; and further upstream Mercury MP Controllers are subject to rigorous third-party penetration testing to proactively identify and address vulnerabilities before they can be exploited.

HID believes the next generation of physical security is defined less by hardware and more by how identity is managed and delivered. The siloed badge-for-buildings model is fading, and as the industry shifts from static cards to mobile-first credentials, integration must be seamless and flexible. Organizations are accelerating toward converged physical and logical credentials, driven by the need for a single identity that works consistently across doors, networks, and cloud applications. Coexistence by design ensures mobile credentials are deployed alongside physical cards, allowing users to adopt mobile access without disrupting existing workflows or infrastructure

HID mobile access integrates with existing access control systems through secure APIs, minimizing system changes and avoiding rip-and-replace upgrades. For deployment, credentials can be provisioned through the HID mobile app, added to Apple Wallet or Google Wallet, or embedded via SDK into a HID technology partner's application.

IDEMIA Public Security

idemia.com
smart-biometrics@idemia.com

IDEMIA Public Security (IPS) is a trusted provider of secure, government-grade biometrics-based solutions to 600 government, state, and federal agencies. With decades of experience in biometric technologies, IPS enables safer, frictionless, and fairer ways to secure travel, access, and citizen protection.

Adoption of biometric access control is accelerating across financial services and critical infrastructure, as tightening regulations and rising fraud drive organizations to strengthen identity-based security. For IPS, data centers represent a particularly fast-growing segment, given their stringent protection requirements. At the same time, stadiums and arenas are adopting biometrics to pair enhanced security with faster entry and better fan experience, while enterprises continue to scale deployments of highly secure workplace access solutions.

IPS delivers frictionless biometric access control solutions that prevent credential-sharing and secure high-traffic facilities without slowing people down. Using industry-leading contactless fingerprint and facial recognition technologies, these solutions authenticate users almost instantly and integrate seamlessly with existing systems – helping organizations strengthen security, improve throughput, and simplify identity management.

AI is at the core of IDEMIA Public Security's biometric innovation, driving industry-leading accuracy, quasi-instant authentication, and consistent performance across diverse environments and populations. Beyond speed and precision, AI plays a critical role in security, detecting sophisticated presentation attacks, including emerging threats such as AI-generated deepfakes.

IPS integrates advanced liveness detection and presentation attack detection (PAD) to protect both physical access points and digital identity verification. These technologies detect sophisticated spoofing attempts including masks, replicas, and AI-generated deepfakes, ensuring the biometric data comes from a real, live person, whether authenticating at a secure facility or during remote identity proofing. The company's solutions are certified against ISO/IEC 30107-3, the international standard for presentation attack detection.

Organizations are increasingly seeking a single, trusted identity solution to secure both physical environments and digital systems. IDEMIA Public Security enables this convergence by delivering biometric authentication that integrates seamlessly with physical access control platforms and enterprise identity management systems.

Innovatrics

innovatrics.com
sales@innovatrics.com
Tomášikova 64, 831 04 Bratislava, Slovakia
+421 2 2071 4056

Since 2004, Innovatrics has been providing biometric solutions to public and private sector organizations for a range of use cases. The company is based in the EU and develops proprietary software for fingerprint, facial, iris, and palmprint biometrics, along with liveness detection and related technologies. Innovatrics' algorithms are built with advanced, AI-powered machine learning models, and have consistently ranked among the fastest and most accurate in the world in independent evaluations.

Innovatrics has offices in Slovakia, Brazil and Singapore and additional sales representation in India, the Middle East and Africa. The company also operates an R&D center in Czechia, and its headquarters in Bratislava is located in "Biometrics House," which demonstrates its biometric technologies for converged physical and logical access control in an operational setting as "the Most Biometric Building in the World."

The flagship PBAC system offered by Innovatrics is its Seamless Access Control, which provides secure, touchless building entry through facial or palm recognition. The solution can perform biometric matching on edge devices for fast and privacy-preserving user authentication, or on a server for enhanced management control, and includes QR codes as a fallback access control credential.

Advanced features like liveness detection, debounce (to avoid unintended triggers) and anti-hammering (to prevent brute-force attacks) secure the system against common attacks.

Adoption of Innovatrics' biometrics for PBACs is growing across several sectors to deliver stronger security and a smoother user experience. Notable among those are office buildings, where Innovatrics' technology is frequently deployed to replace physical access cards with touchless biometric entry. Facilities with higher security requirements such as critical infrastructure sites are also implementing biometrics from Innovatrics to improve identity assurance and auditability.

Innovatrics' access control software integrates with existing systems, with native support for widely used systems like Integriti and Nedap AEOS. Innovatrics provides ready-to-use integration samples and clear documentation for system integrators through a public GitHub repository to enable fast installation with third-party access control platforms. The software is offered in a modular architecture that eases extensions and further integrations as needed.

Iris ID

irisid.com
sales@irisid.com
609-819-4747

With more than 25 years of national scale deployment expertise, New Jersey-based Iris ID delivers high assurance iris and face fusion multimodal biometric solutions, supporting large population identity systems worldwide. Its Iris ID solutions are deployed globally across six continents, and lays claim to being the world's leading deployed iris recognition platform.

Designed to meet strict government standards in multiple jurisdictions, Iris ID's technology is used by immigration and border control agencies, commercial entities, law enforcement, and national ID programs, as well as data centers, healthcare, research labs, energy utilities and enterprise campuses. Iris ID sees strong adoption of its solutions in government and critical infrastructure sectors, where high assurance identity verification is mandatory. Additionally, enterprise workforce management and time & attendance adoption is growing, particularly in regions where hygiene, fraud prevention, and compliance are key operational priorities.

Iris ID's IrisAccess® iA1000 is a non-contact iris and face fusion authentication solution integrated with the IrisAccess Management System (iAMS). Featuring iBeta Level 2 PAD compliant iA FacePAD v2.5.3 for advanced liveness detection, it delivers secure, privacy focused identity verification and accurate biometric authentication. Its facial recognition algorithm recently made its debut on the NIST FRTE 1:1 Verification report.

For iris recognition, the iA1000 employs near infrared imaging combined with iris texture validation and natural ocular response analysis. The system analyzes authentic iris patterns and image depth characteristics to differentiate between a live eye and artifacts such as printed eyes, cosmetic contact lenses or artificial representations. It integrates through REST APIs, while supporting industry-standard protocols such as OSDP and Wiegand, allowing IT administrators to manage devices, users, and authentication policies across multiple sites with connectivity to existing access control panels.

Because the iA1000 can operate as a credential reader, similar to a traditional card reader, and communicate via OSDP or Wiegand, deployment typically does not require changes to existing door controllers or infrastructure. It offers enterprise ready integration via iAMS with centralized management, REST APIs, OSDP support, fast contactless throughput, and seamless deployment.

Organizations increasingly want a single, high assurance identity that governs building access, workstation login, VPN access, and privileged system authentication, eliminating gaps between physical and cybersecurity domains. Iris ID's biometric platform supports this convergence strategy, securing physical access points through standard access control integration (OSDP/Wiegand) while also enabling logical authentication through SDKs and API-based integrations for workstation and application. By using iris and face biometrics as the credential, organizations can establish a strong identity foundation that spans doors and digital systems.

RealSense

realsenseid.com
sales@realsenseai.com
1+ 201.707.5518

RealSense delivers on-device Vision AI for robotics and biometric access control, combining advanced depth-sensing hardware with purpose-built edge AI software. Headquartered in Cupertino, California, RealSense builds vision systems that enable machines to securely understand and interact with the physical world—powering safer automation, frictionless entry, and trusted identity verification.

The company's solutions are designed for high-security environments where performance, accuracy, and privacy are critical.

RealSense ID Pro F500 is a next-generation facial authentication solution for enterprise access control, combining industry-certified accuracy, advanced anti-spoofing, and integrated perception capabilities in a compact, on-device platform. It uses an active stereo depth sensor and proprietary neural network to enable fast, highly accurate biometric verification for physical security and identity workflows.

The system achieves 99.77% NIST-verified accuracy (1:1 verification) and is iBeta Level 2 & ISO 30107-3 PAD compliant, providing strong protection against presentation attacks. Built for demanding environments, it authenticates in ~300 milliseconds, enabling secure, high-volume operation across diverse users and lighting conditions.

Beyond facial authentication, RealSense ID Pro F500 introduces advanced perception capabilities, including person detection, body-part classification, and tracking. Purpose-built for biometrics, the platform extends beyond identity verification to support contextual awareness, including presence detection, adaptive access policies, and enhanced security monitoring.

Privacy and security are foundational, with all biometric processing performed fully on-device and no storage of images or personally identifiable information. The device stores up to 10,000 encrypted faceprint templates, which cannot be reconstructed into original images, supporting enterprise, government, and GDPR-aligned privacy requirements. Enrollment supports on-device and image-based workflows.

Purpose-built for access control, the solution features a wide vertical field of view and consistent performance across user heights. Its compact form factor—just one-quarter the size of a credit card—enables seamless integration into readers, turnstiles, and speed gates.

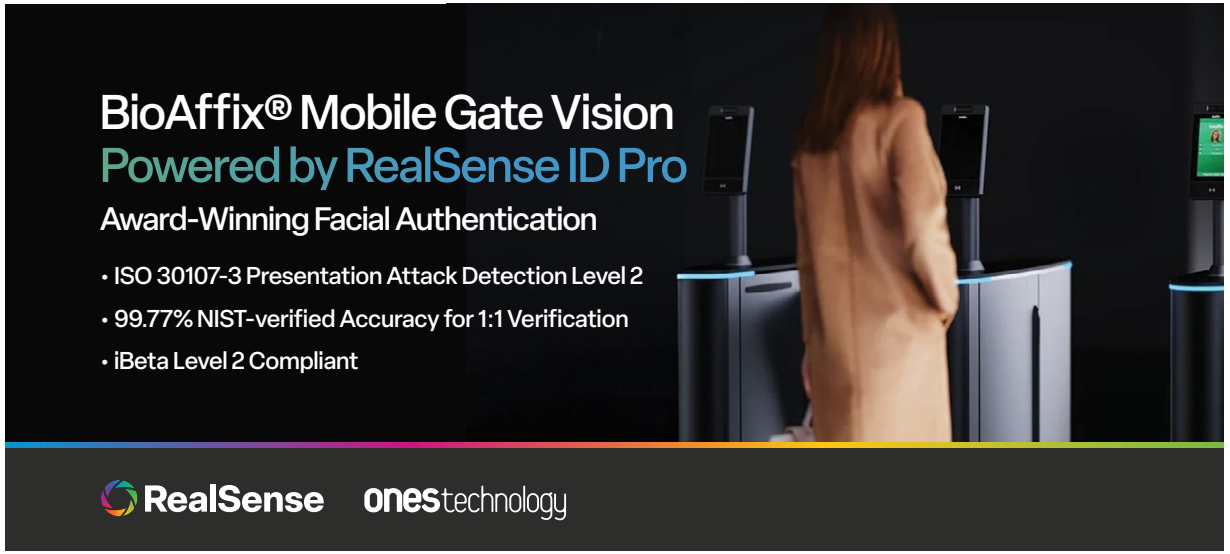
Use cases span transportation, enterprise access control, time and attendance, manufacturing authorization, and robotics. In transportation, touchless biometric authentication enables faster movement through secure areas, supporting high-volume, walk-through experiences that improve efficiency and user experience.

RealSense ID Pro F500 supports deployment via REST APIs and SDKs for Windows, Linux, and Android, enabling integration with identity and access systems and scalable rollouts.

Fast, Secure Facial Authentication for High-Traffic Access Control

Powered by NIST-verified RealSense™ ID, BioAffix® Gate Vision by Ones Technology delivers rapid, reliable biometric access control for high-security environments including airports, data centers, metro stations, and government facilities. With RealSense ID integrated, Gate Vision enables non-touch facial authentication in under one second while maintaining high standards of privacy, accuracy, and regulatory compliance—earning the 2025 SIA NPS Award in Biometrics and the 2026 Intersec Award for Best Homeland Security Solution.

Traditional access control using badges, QR codes, or fingerprints can be increasingly vulnerable to fraud and security breaches. Many also struggle to comply with evolving regulations governing how biometric data is stored, shared, and protected. RealSense ID addresses these challenges by combining an active stereo depth sensor with AI algorithms for reliable liveness detection, preventing spoofing attempts; BioAffix® Gate Vision integrates this capability with identity badging.



RealSense ID also performs all processing locally on secure hardware. Biometric templates can remain under user control on tamper-proof ID cards or mobile devices rather than centralized servers, enabling a simple one-to-one match between the live facial scan and the stored credential. This architecture supports GDPR compliance and sovereign identity requirements while minimizing security risk.

BioAffix® Gate Vision supports multiple authentication methods, including biometric templates on smart cards, mobile apps, QR codes, and Bluetooth Low Energy (BLE) tags. BLE walk-through functionality allows users to authenticate without stopping, enabling high throughput in busy environments.

By integrating the RealSense ID, BioAffix® delivers accurate facial authentication across lighting conditions and demographics—redefining secure access control with speed, privacy, and confidence.

ROC

www.roc.ai
sales@roc.ai
1290 Broadway, Suite 1200, Denver, CO 80203

ROC is a leading U.S. developer and manufacturer of Vision AI, delivering sovereign biometrics, video analytics, and mission intelligence through a unified platform. Trusted for high-stakes identity and security operations, ROC helps organizations improve access assurance, accelerate investigations, and strengthen situational awareness with real-time, actionable intelligence. All ROC technology is designed and developed in the United States, supporting a mix of domestic and international customers and channel partners across North America, Europe, the Middle East, and APAC.

ROC security products and solutions are deployed globally and are sold through an expanding network of certified partners. Its physical access control product, ROC Watch, is a multimodal Vision AI and video analytics platform built to interpret video in real time and post-event, used by security, law enforcement and public safety teams, including RTCC and smart city operations, that require real-time awareness and defensible identity decisions in physical environments.

Suited for enterprise and government deployments where existing PACS/VMS and camera ecosystems are already in place and must remain operational across mixed vendor environments, ROC Watch enables real-time, frictionless access control using Vision AI and biometric identification from existing cameras. It sends identity-aware alerts to connected access control systems to grant or deny access based on who is physically present – not just a credential, which can be used fraudulently.

The product offers configurable workflows per door/zone/site (intent-to-access, proximity, tailgating/2-man rules, parallel crowd processing, lockdown rules for watchlist or weapon detection) and complements existing PACS/VMS, protecting prior investments and accelerating time-to-value.

Powered by NIST-ranked face recognition algorithms proven in real-world, high-throughput environments, ROC Watch supports layered access control and broader security workflows including badgeless visitor management, perimeter protection, gun detection, watchlisting, incident management, video forensics, and automated license plate recognition (ALPR), delivered through one integrated platform.

A hardware-agnostic platform designed for integration-first deployments, ROC Watch also supports a flexible alerting service for third-party workflows via REST API and other notification methods (e.g., MQTT), depending on operational needs.

Vendor Directory

A

Aratek

aratek.co

Aratek is a global biometric technology provider specializing in fingerprint, facial recognition, and multimodal authentication devices. Founded in 2004, the company develops hardware and software solutions for identity verification, enrollment, and secure access across government and commercial sectors.

Aratek's portfolio includes FBI-certified fingerprint scanners, mobile biometric terminals, and integrated access control devices designed for high-accuracy performance. Its solutions support applications such as border control, national ID programs, financial services onboarding, and enterprise physical access management worldwide.

Arana Security

aranasecurity.com

Arana Security is a UK-based manufacturer and provider of biometric and RFID-enabled access control solutions. The company designs and develops secure entry systems tailored for enterprise, data center, critical infrastructure and high-security environments.

Its portfolio includes biometric readers, multi-factor authentication devices, and integrated access control platforms that support scalable, high-assurance identity verification. Arana Security works with integrators and end users to deliver compliant, future-ready security systems across the UK and international markets.

C

CyberLink

cyberlink.com

CyberLink is a Taiwan-based technology company founded in 1996, known for multimedia software and AI-powered facial recognition technologies. Through its FaceMe® platform, CyberLink provides facial recognition solutions for identity verification, access control, and smart security applications.

FaceMe delivers high-accuracy facial recognition with liveness detection, edge deployment capabilities, and integration with access control and video management systems. The platform is used across enterprise offices, manufacturing facilities, retail environments, and smart cities to enable secure, contactless authentication and real-time identity management.

H

HID Global

hidglobal.com

HID Global, headquartered in Austin, Texas, provides secure identity and access control technologies for organizations worldwide. A subsidiary of ASSA ABLOY, HID is known for its smart cards, mobile credentials, biometric readers, and identity management solutions.

HID Global delivers interoperable access control systems supporting physical and logical security. Its

portfolio includes RFID credentials, multi-factor authentication devices, and biometric solutions tailored for enterprise, government, healthcare, and financial services environments.

I

IDEMIA

idemia.com

IDEMIA is a global provider of biometric identity and secure credential solutions serving governments, enterprises, and financial institutions worldwide. Headquartered in France, the company delivers technologies spanning civil identity, border control, payments, and enterprise access management.

IDEMIA's portfolio includes facial, fingerprint, and iris recognition, digital identity platforms, secure document issuance, and biometric access control systems. Its solutions support high-assurance identity verification, large-scale enrollment and matching, and secure authentication across physical and digital environments.

Innovative Technology

innovative-technology.com

Innovative Technology is a UK-based technology manufacturer specializing in secure payment validation and biometric authentication solutions. Founded in 1992 and headquartered in Oldham, England, the company develops hardware for cash handling, age verification, and identity-based access control.

Its biometric portfolio includes facial recognition terminals designed for age estimation, access control, and secure vending applications. Innovative Technology's solutions are deployed across retail, gaming, transportation, and commercial environments, combining embedded AI with edge-based processing to deliver fast, privacy-conscious identity verification.

Innovatrics

innovatrics.com

Innovatrics is a Slovakia-based biometric technology company specializing in large-scale identity management and authentication solutions. Founded in 2004 and headquartered in Bratislava, the company develops fingerprint, facial, iris, and palm recognition software used in government and enterprise deployments worldwide.

Innovatrics provides Automated Biometric Identification Systems (ABIS), border control solutions, and digital identity platforms designed for high accuracy and scalability. Its technology supports national ID programs, law enforcement, voter registration, and secure access control environments requiring fast matching performance and robust biometric accuracy.

iProov

iproov.com

iProov is a UK-based biometric authentication provider specializing in facial verification with advanced liveness detection. Headquartered in London, the company delivers cloud-based identity assurance technology designed to protect against presentation attacks, injection attacks, and deepfakes.

In physical access control environments, iProov enables high-assurance, contactless facial authentication for secure facility entry and restricted areas. Its technology can be integrated with access control systems and kiosks to verify individuals

against enrolled identities, supporting government, critical infrastructure, and enterprise deployments requiring strong anti-spoofing protection.

Iris ID

irisid.com

Iris ID is a global provider of iris recognition technology for secure access control and identity authentication. Headquartered in Cranbury, New Jersey, the company designs and manufactures contactless biometric readers used in government, healthcare, corrections, and critical infrastructure environments.

Iris ID's platforms deliver high-accuracy, fast throughput authentication and integrate with leading physical access control systems. Its iris-based solutions are well suited for high-security facilities requiring strong identity assurance, auditability, and reliable performance across large user populations.

IriTech

iritech.com

IriTech is a biometric technology provider specializing in iris recognition hardware and software for identity authentication and access control. Headquartered in Fairfax, Virginia, the company develops compact, high-performance iris cameras and SDKs used in government, enterprise, and healthcare environments.

IriTech's solutions enable fast, contactless authentication for secure physical access to facilities, including data centers, laboratories, and restricted corporate sites. Its iris recognition technology is designed for high accuracy, scalability, and integration with existing access control systems, supporting deployments that require strong identity assurance and resistance to spoofing.

M

Miaxis

miaxis.net

Miaxis is a biometric technology provider focused on fingerprint-based access control and workforce management solutions. The company develops hardware terminals and software platforms used to secure physical facilities and manage employee attendance across commercial and industrial environments.

Miaxis' portfolio includes fingerprint readers, standalone access control devices, and integrated time and attendance systems designed for reliability and ease of deployment. Its solutions are commonly used in offices, factories, schools, and public institutions seeking cost-effective biometric authentication for secure entry and workforce tracking.

N

Nymi

nymi.com

Nymi is a Canada-based technology company specializing in wearable biometric authentication for secure access control. Headquartered in Toronto, Nymi developed the Nymi Band, a wrist-worn device that uses heart rhythm (electrocardiogram) biometrics to continuously authenticate the wearer.

In physical access control environments, the Nymi Band enables hands-free, contactless entry to secure

facilities, workstations, and industrial equipment. Designed for regulated and high-compliance sectors such as pharmaceuticals, manufacturing, and critical infrastructure, Nymi supports strong identity assurance while improving workflow efficiency and auditability.

P

Paravision

paravision.ai

Paravision is a U.S.-based provider of advanced facial recognition and biometric identity technologies. The company develops high-accuracy computer vision software designed for identity verification, authentication, and watchlist screening across security-sensitive environments.

In physical access control applications, Paravision's facial recognition technology enables secure, contactless entry to facilities and restricted areas. Its software can be integrated with access control systems, cameras, and kiosks to support real-time identity matching, high-throughput environments, and strong anti-spoofing protections for enterprise, government, and critical infrastructure deployments.

Princeton Identity

princetonidentity.com

Princeton Identity is a U.S.-based biometric technology company specializing in iris recognition for secure physical access control. Headquartered in New Jersey, the company develops contactless iris authentication solutions designed for high-security environments requiring strong identity assurance.

Princeton Identity's platforms integrate iris recognition into access control readers and turnstile systems, enabling fast, touchless entry to facilities such as data centers, corporate campuses, healthcare sites, and critical infrastructure locations. Its technology emphasizes accuracy, anti-spoofing protection, and seamless integration with existing physical access control systems.

R

RecFaces

recfaces.com

RecFaces is a biometric software provider specializing in facial recognition solutions for physical access control and workforce management. The company develops facial authentication platforms designed to integrate with enterprise access control systems and video surveillance infrastructure.

RecFaces' technology enables contactless identification for secure facility entry, time and attendance tracking, and visitor management. Its solutions support real-time facial matching, watchlist alerts, and centralized management, serving corporate offices, industrial sites, healthcare facilities, and other security-sensitive environments requiring scalable biometric access control.

ROC

roc.ai

ROC is a U.S.-based computer vision company specializing in multimodal biometric recognition, including facial, tattoo, and object recognition

technologies. Headquartered in Denver, Colorado, ROC develops AI-driven identity solutions for government and security-focused applications.

In physical access control environments, ROC's facial recognition technology enables contactless identity verification and watchlist screening at secure facilities. Its platform supports high-accuracy matching, forensic-grade analysis, and integration with existing security and surveillance systems, serving law enforcement, corrections, and critical infrastructure deployments requiring advanced biometric intelligence.

S

SALTO Systems

saltosystems.com

SALTO Systems is a global manufacturer of electronic access control and smart locking solutions, headquartered in Spain. Founded in 2001, the company provides wireless, cloud-based, and mobile-enabled access systems for commercial, institutional, and residential environments.

SALTO's portfolio includes smart locks, access control software, mobile credentials, and cloud-based management platforms. Its solutions are widely deployed across corporate offices, healthcare facilities, education campuses, hospitality properties, and multi-family housing, enabling flexible, scalable physical access control with centralized management and real-time monitoring.

Suprema

supremainc.com

Suprema is a South Korea-based provider of biometric access control and time attendance solutions, serving enterprise and commercial markets worldwide. Founded in 2000, the company offers fingerprint, facial recognition, and mobile credential technologies through a global partner network.

Suprema's access control platforms combine biometric readers, controllers, and management software designed for scalability and integration. Its solutions are deployed across corporate campuses, data centers, healthcare facilities, and critical infrastructure sites requiring secure and flexible entry management.

X

Xperix

xperix.com

Xperix is a South Korea-based manufacturer of biometric identification devices and security solutions. The company develops fingerprint scanners, live scanners, and multimodal biometric terminals used in government, law enforcement, and enterprise security environments worldwide.

In physical access control applications, Xperix provides high-performance fingerprint and multimodal authentication devices designed for secure facility entry and identity verification. Its solutions support integration with access control systems and are deployed in environments requiring reliable biometric performance, including public sector facilities, critical infrastructure, and commercial sites.

Resources

Find more information and resources about biometric physical access control here:
https://www.biometricupdate.com/service-directory/physical-biometric-access-control

Find information and resources about biometric liveness detection here:
https://www.biometricupdate.com/2025-face-liveness-market-report-and-buyers-guide

BIOMETRIC UPDATE.COM

GOODE INTELLIGENCE
YOUR PARTNER FOR BUSINESS RESEARCH & ANALYSIS