EBOOK

Facial Biometrics Buyer’s Guide: Evaluating Modern Access While Preserving Privacy

alcatraz ai

Table of Contents

How to Select the Best Facial Authentication System for Physical Access Control in Your Organization

Did you know that enterprises experienced an average of 130 security breaches per year, per organization, with a growing number caused by a physical security breach?

While many businesses focus on digital access control, this alarming statistic highlights the urgent need for enhanced physical security measures in the digital age. Traditional physical access control systems are needed to ensure the safety of employees and assets.

Advancements in biometric technology can offer additional protection against unauthorized entry, providing companies with much needed peace of mind.

Facial biometrics technology is gaining popularity as it provides an accurate and reliable method of verifying an individual's identity by scanning and mapping their facial features. However, traditional facial recognition technology is plagued by inaccuracy and bias, given the legacy methods of collecting facial data are linked to privacy concerns and violations.

Facial authentication biometrics solve these problems with the privacy-first approach. It ensures high levels of security while preserving privacy by requiring the individual's consent (opt-in) before enrollment in the system. Facial authentication technology does not store Personally Identifiable Information (PII) that can be used or reconstituted to identify an individual.

Unlike facial recognition, facial authentication offers the benefits of biometric access control while addressing privacy concerns and offering fast and accurate authentication. The result is a modern facial biometric access control system that safeguards employees, visitors, and critical assets while streamlining operations and enhancing the end-user experience.

Our guide will help you evaluate facial authentication technology to select the appropriate physical access control system for your organization.

Why Organizations Choose Facial Authentication

Buyers can choose between access cards, keypad PIN codes, mobile credentials, and biometric credentials such as the person's iris or face. Most buyers and their users have familiarity with traditional access cards. However, the vast majority of card access control systems have vulnerabilities that are easy to exploit. Traditional access cards are easy to duplicate or clone, can be lost or stolen, and encourage tailgating behavior. Tailgating is where authorized cardholders enable unauthorized persons to gain entry into an area by holding the door open for another person or simply allowing them to follow.

Why are more and more organizations across various industries—from financial institutions and data centers to corporate and educational campuses—looking to facial biometrics for reliable access control?

According to the 2022 IBM Ponemon Report, approximately 9% of breaches come from unauthorized physical access, with tailgating as the primary way unauthorized people gain access.

Hackers and threat actors continue to prey on vulnerable systems.

As threats expand, facial authentication presents a solution with robust privacy and security that leads with the zero-trust model by identifying all users based on who they are.

In the introduction, we explained that some traditional facial recognition technologies can be rife with privacy concerns. Many facial recognition systems also require costly backend integration and setup, while others have performance issues based on changes in lighting.

In contrast, modern facial authentication enables the user's face as their access credential, creating a frictionless touch-free experience and strengthening security with tailgate detection, alerting, and data that can be used to inform improved behavior and compliance. It also addresses the issues that arise with traditional recognition by affirming privacy, reducing costs, and eliminating complex integrations.

Let's delve into compliance and data privacy for your facial authentication system.

Compliance and Data Privacy for Facial Biometrics

Companies seeking to purchase and deploy facial biometric access control systems must safeguard data and meet local, state, and global privacy regulations.

Individuals have a right to data privacy and security, and businesses must ensure compliance with regulations on every level. This includes U.S. laws such as the Illinois Biometric Information Privacy Act (BIPA), which states:

“Employees (like other classes of individuals) expect and demand that the companies they work for secure and safeguard their sensitive personal data while it is in the hands of their employer. These individuals have realized that data security is a right and expect that the companies they are employed by will protect that right and their data.”

Texas and Washington state have also passed biometrics laws, although BIPA is considered the most stringent. Compliance with the EU General Data Protection Regulation (GDPR) is also a requirement for most organizations utilizing biometric data.

Privacy data laws can vary, therefore staying informed of these location-based and broader mandates will provide a template for businesses to remain compliant. Creating safeguards for this data can be included in a company’s privacy policy or other contract.

Consider some compliance requirements, such as:

Privacy Policy

This should detail an employer's use of biometric data, retention schedule, and guidelines for permanently destroying biometric data.

Public Disclosure

Publicly disseminate the Privacy Policy and make it available in employee documents, handbooks, and post publicly where possible.

Data Retention

Biometric data must be permanently destroyed when no longer in use.

Data Security

Safeguarding biometric data from unauthorized access, disclosure, or acquisition.

No Profiting From Biometrics

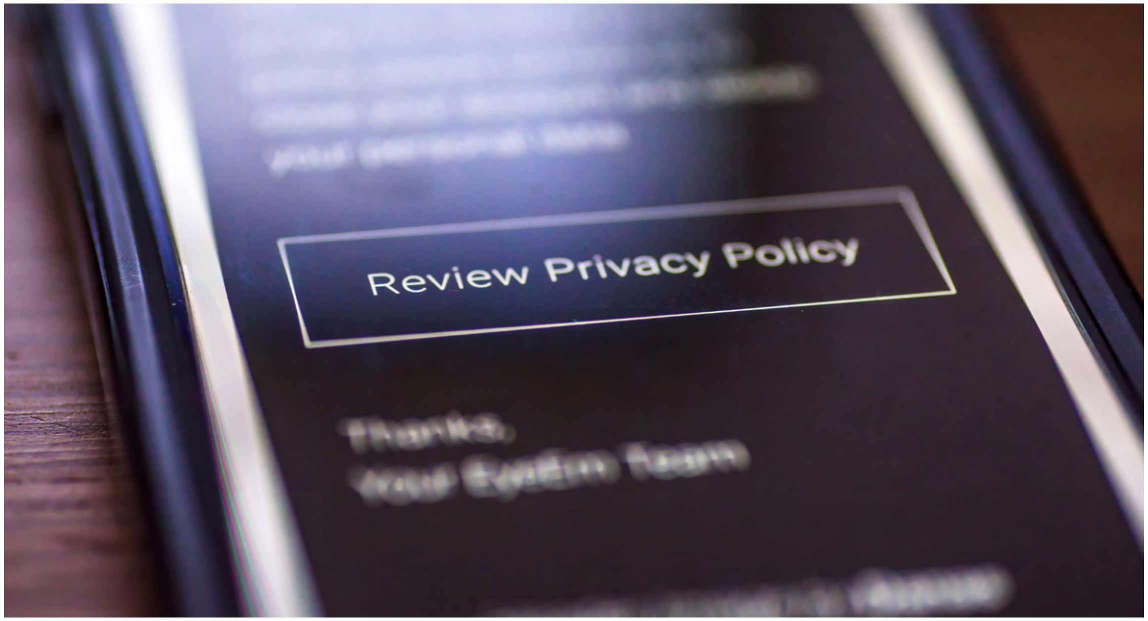
Organizations must not sell or profit in any way from the biometrics data they collect.

Organizations should obtain written consent from data subjects before collecting their biometric data. Consent must be obtained before any biometric data is collected, and the notice of collection should be clear and understandable to all participants.

Privacy policies must be publicly available and articulate core compliance requirements for all parties involved to avoid disputes. Businesses should also ensure that their employees are trained in handling biometric data and understand the importance of data privacy and security. Consistent adherence to and regular review of these policies is essential to ensure compliance with any biometric privacy laws and regulation updates.

As many institutions continue to upgrade and strengthen their security infrastructure, they must consider compliance with GDPR and new or evolving state laws and regulations. Modern facial authentication offers the highest level of security and the most frictionless experience possible, meeting regulatory compliance standards and creating a seamless access control experience.

By implementing these measures and staying up to date with biometric privacy laws and regulations, businesses can simplify compliance and ensure that they are using facial biometrics in a way that adheres to data privacy regulations.



Biometrics With Simple Integration and Scalability

When evaluating your modern facial authentication system, ensure it eliminates complications with your previous infrastructure, such as ripping and replacing it.

Select a biometric authentication solution that runs natively on your existing access control system without integration, as this delivers a simpler connection for enhanced security and ease of use. By eliminating integration, your organization can upgrade to facial biometrics painlessly. We'll discuss more criteria to evaluate biometric vendors in the next section.

Cloud-based systems are effective for large enterprises, as they can scale up or down depending on the number of users and facilities. Additionally, they provide continuous delivery of improved services and features and reduce the total cost of ownership.

We've found modern facial authentication to offer a robust solution for enterprises that merge with other institutions. Instead of ripping and replacing another system following a merger, companies can create a zero-trust environment by adding a facial biometric solution to their existing system at key access points. Using the cloud, users gain simplified enrollment of hundreds and thousands of end users.

Modern facial biometrics enable this to work natively with current access control systems to share activity data within the primary system. All of this is achieved without the need for any integration, including your Video Management System. This saves organizations time, money, and administrative burden.

The shift towards cloud-based security systems provides increased accessibility, flexibility, scalability, and cost savings for institutions. Cloud security offers quick scalability for ever-changing security needs without any physical changes to infrastructure. They also work natively with existing access control and Video Management Systems, reducing integration challenges and complications.

Facial biometric systems offer a powerful solution for enhancing security in the financial sector, data centers, healthcare, and other industries. Advancements in technology and cloud-based systems allow for easier adoption of this innovative technology into existing security infrastructures.

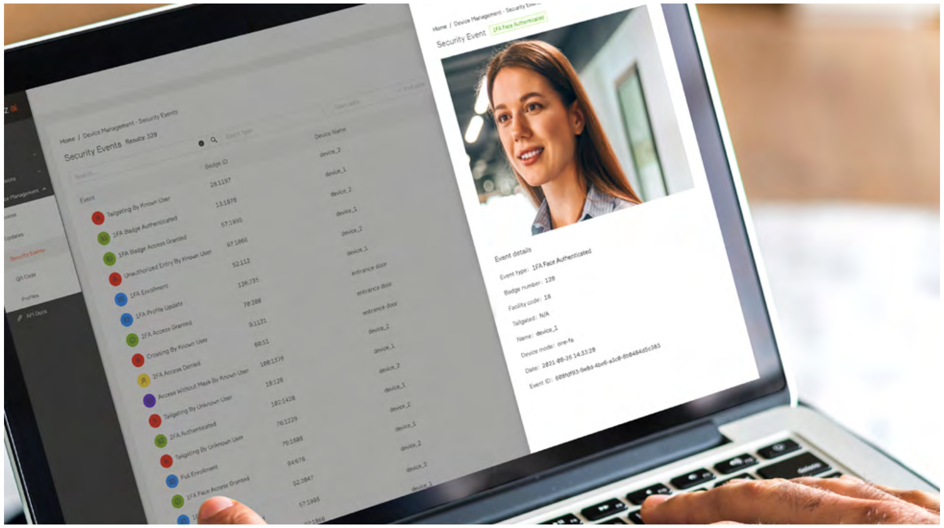
How to Select a Facial Biometrics Vendor

When evaluating a facial biometrics vendor, focus on security, privacy, and the end-user and administrative experience. Below we detail the top things to consider when selecting a facial biometrics vendor and how to assess their dedication to protecting data privacy and security.

Transparency and Control

It's crucial to prioritize transparency and control when it comes to facial biometrics technology. The issue of data storage and usage is of utmost concern. Therefore, selecting a vendor with an open and transparent policy on this matter is vital. The vendor should be transparent about using and retaining the captured facial data.

Identify a facial biometric vendor that offers features like privacy consent management, including opt-ins, opt-outs, mobile enrollment, and data retention and deletion features that simplify the administrative burden and compliance with data retention regulations and policies.



Privacy and Security

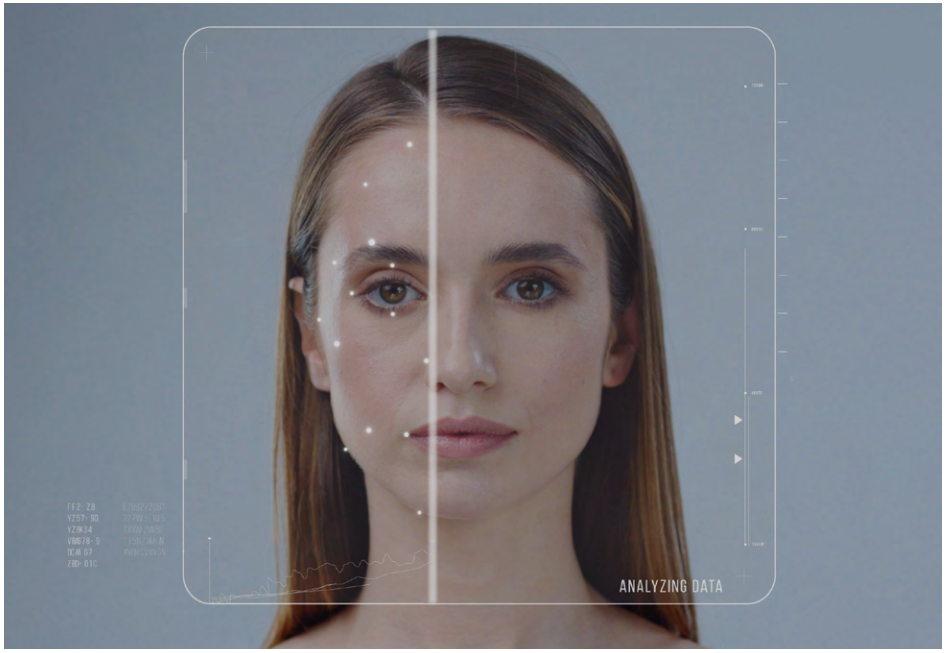
To safeguard privacy while ensuring secure authentication, vendors must offer a facial authentication solution that effectively delivers on privacy and security.

Vendors must provide access control solutions that do not require storing visual data but instead rely on algorithms that compare facial features. Solutions that show the user’s image could be an exposure of Personally Identifiable Information (PII), which can violate certain privacy laws. To ensure compliance, consider solutions that anonymize user data. Companies can enhance their security measures by working with a vendor that adopts these privacy-centric practices.

Strong Encryption and Compliance

It is imperative to demand the highest level of biometric data encryption at rest and in transit to ensure protection against unauthorized access. Look for solutions that have policies where profiles expire and biometric data is automatically deleted after a certain period based on the last time the user interacted with the system. These types of policies will minimize the possibility of data being compromised. Solutions that do not tie biometric data to individuals or PII add an extra layer of protection for the individual.

When selecting a vendor, always look for one who prioritizes product development in compliance with industry standards such as GDPR, CCPA, or BIPA. Protecting your user data is vital, so don't settle for anything less than the best security, encryption, and privacy measures available.



Independent Testing and Certification

Another way to confirm that your facial biometrics solution provider is dedicated to data privacy and security is their commitment to independent validation and garnering the appropriate certifications. Verify if the solution has undergone independent auditing, testing, and certification such as ISO 27001.

Industry-recognized certifications offer third-party assurance that vendors meet the highest security and data privacy standards. Independent testing is equally important to ensure the technology operates accurately and meets these standards. Opting for certified vendors and tested technologies is a clear way to demonstrate a strong commitment to cybersecurity.

Experience Advanced Security with Alcatraz AI's Facial Authentication

With a higher level of accuracy and the elimination of PIN codes and easily misplaced or stolen cards, facial authentication technology is the key to protecting security with simple and reliable access. Facial authentication makes entering secure areas as easy and protected as opening a smartphone.

Strengthen your physical security by upgrading to advanced facial biometrics with ease using the Alcatraz AI solution. Our advanced enterprise-grade solution, the Rock, offers superior physical access control, thanks to its use of 2D and 3D sensors that capture accurate data while ensuring data privacy.

Here are six compelling reasons to deploy the Rock:

No Exposure of Personally Identifiable Information (PII)

Alcatraz AI doesn't expose PII, not even to system administrators. By prioritizing privacy and data security, Alcatraz AI sets a new standard in safeguarding sensitive information.

Seamless Authentication

The Rock ties directly into your existing access control system and simply matches the "data blob" to the corresponding unique ID code already assigned to authenticate the user.

No Integration Required

Alcatraz AI works natively with your existing access control system and with your current Wiegand or OSDP connections, eliminating the need to rip and replace or pay for costly system integration.

AI-Algorithms Enhance Accuracy

Machine Learning enables the Rock to intelligently adjust capabilities in lighting changes and to adapt to changing user characteristics, such as glasses, weight loss, or facial hair.

Tailgating Detection and Alerts

Using advanced computer vision and AI technology, the Rock verifies authorized individuals in real-time and determines whether a single person or multiple people entered a secure area at the time of authentication. The Alcatraz solution provides an alert to the access control system and actionable data to enforce compliance and change behaviors.

Zero Trust Environment

Alcatraz AI makes implementing a zero-trust environment easier by identifying users based on who they are, not what they have, like a card that can be lost or stolen. This reduces the risk of a breach and supports the zero-trust model across the organization.

Alcatraz AI highly prioritizes ensuring data security and privacy in every stage of development and design for the Rock. We have obtained certification in various security and privacy industry standards, including ISO 27001, ISO 27017, and ISO 27018, and we exceed the industry’s standards.

The Rock's facial authentication algorithm has been tested extensively by the National Institute of Standards and Technology (NIST) and is highly accurate with a very low risk of mistaken identities across all demographics. Its long scanning range and field of view allow it to detect and prevent tailgating, while its video monitoring functions as an Open Network Video Interface Forum (ONVIF) camera, providing a unique perspective of personnel accessing secure areas with simplified integration into existing Video Management Systems (VMS).

→ Protect your business from unauthorized physical access with the Alcatraz AI Rock — facilitating the future-proofing of biometric access control.

→ With facial authentication technology, you will experience the ultimate level of protection for restricted spaces.

→ Stay ahead of physical security challenges and improve your employee and administrative experience by adding this critical solution to your access control system today.

Discover Alcatraz AI Today

Get the ultimate level of protection to make spaces safer and more secure with advanced facial authentication technology. Contact us for a demo and to learn more about how Alcatraz AI can help you secure your business.

Experience secure, integration-free facial biometric access with Alcatraz AI.

Contact Alcatraz AI

alcatraz.ai

sales@alcatraz.ai

Connect with Alcatraz AI

www.facebook.com/alcatrazai

linkedin.com/company/alcatraz

twitter.com/alcatrazai

To learn how the Alcatraz Rock can provide a secure environment for your organization, please sign up for a demo: alcatraz.ai/demo

Schedule a demo

Intertek ISO 27001 CCPA NDAA COMPLIANT GDPR Designed & Manufactured IN THE USA

alcatraz ai