GUIDE

Alcatraz Guide to Facial Authentication

Access Control Identity Authentication



alcatraz

Overview of Facial Authentication-Powered Access Control Systems

What is Access Control?

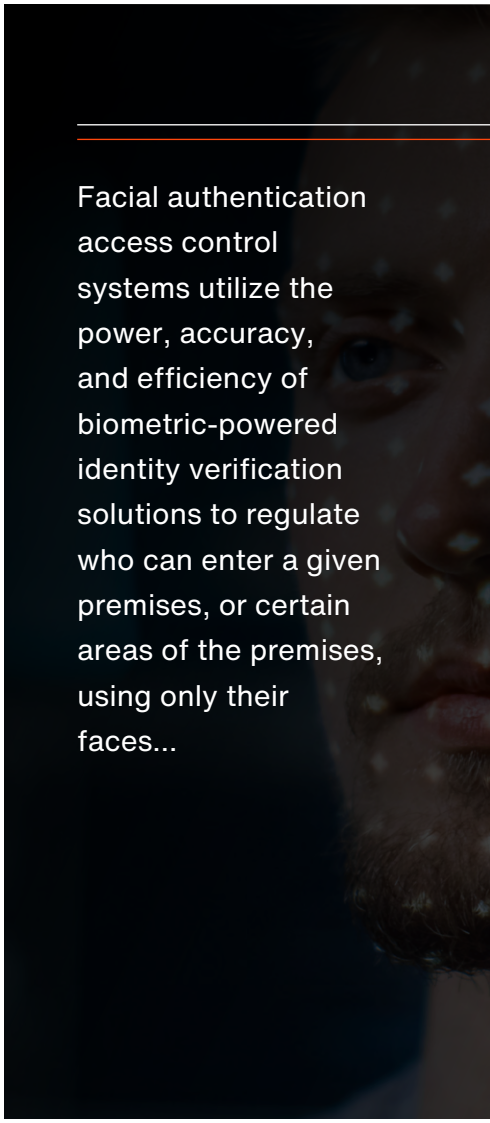
Access control systems are used to identify and authenticate the identities of individuals for purposes of granting access to specific physical spaces. Through automation of the authentication process, access control systems increase the level of security in operations and ensure the protection of people, property, and assets, while also streamlining key enterprise operational elements, such as compliance protocols and visitor management. In addition to dictating who is granted access to restricted spaces, access control systems can also regulate the times and conditions within which access is allowed.

What is Facial Authentication Access Control?

Access control systems today are now often powered by edge devices, making them extremely amenable for advanced facial authentication access control usage. Facial authentication access control systems utilize the power, accuracy, and efficiency of biometric-powered identity verification solutions to regulate who can enter a given premises, or certain areas of the premises, using only their faces and without the need to swipe a badge or enter a PIN number. Facial authentication access control technology relies on analyzing the characteristics of human facial geometry for identity authentication purposes. At the same time, these solutions also leverage artificial intelligence and machine learning to operate with increasing accuracy and speed.

How Does Facial Authentication Access Control Work?

Facial authentication technology involves the process of using biometrics to “scan” or digitally map an individual’s facial features or “geometry,” such as the distance between the eyes or the forehead and chin. These “scans of face geometry” are then used to create a mathematical algorithm or formula known as a “facial template” or “facial signature” of the extracted facial geometry data. An algorithm is then used to compare the extracted facial data with previously-generated, stored facial geometry data to verify/authentication, or identify, an individual associated with the extracted facial template.



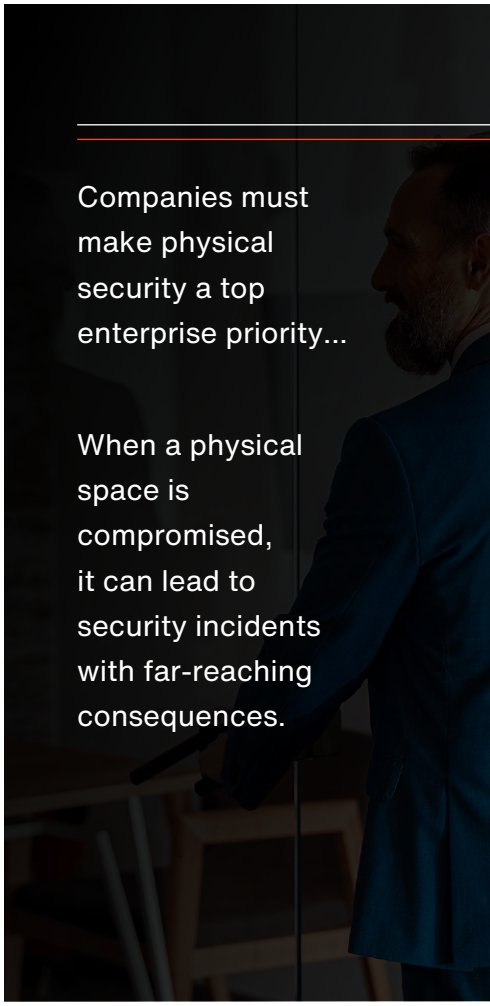
The Legal Landscape: Current Legal Risks and Liability Exposure

Physical Security

The nature of business risks and organizational liability exposure has expanded significantly in a relatively short period of time. Today, the list of potential risks and threats is seemingly endless. When a physical space is compromised, it can lead to security incidents with far-reaching consequences. Not only is short-term profitability almost always hampered, but these incidents also commonly involve long-term financial and reputational harms as well—some of which may take an organization years to recover from.

More than that, lax physical security measures can, in many instances, have negative legal implications as well. In this respect, federal laws and regulations—such as the Health Insurance Portability and Accountability Act ("HIPAA"), Gramm-Leach-Bliley Act ("GLBA"), and Payment Card Industry Data Security Standard ("PCI DSS"), among others—all contain requirements mandating physical security safeguards designed to ensure the protection of sensitive personal data. Moreover, state-level laws—such as the New York Stop Hacks and Improve Electronic Data Security Act ("SHIELD Act") and New York Department of Financial Services Cybersecurity Regulation—also contain physical security components as well.

Taken together, companies must make physical security a top enterprise priority. To address these risks, an increasing number of organizations are adopting a technology-driven approach to physical security, which affords organizations the ability to assess physical threats in real-time and, in turn, allows them to stay a step ahead of potential threats, while also mitigating the risk of legal non-compliance.



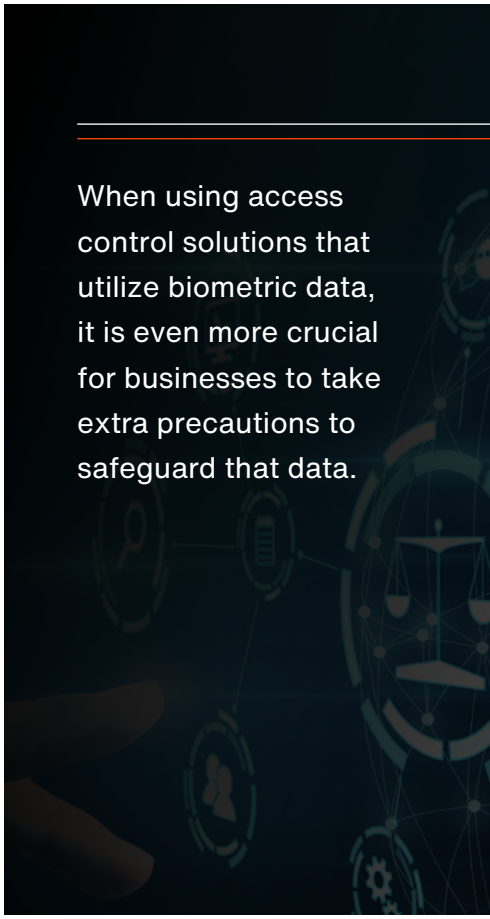
Data Security

Companies that utilize technologically-advanced access control systems must ensure that the data that is used to operate these tools is properly safeguarded as well. In particular, because credentials are the primary means by which bad actors hack into organizations and carry out cyber-attacks, access control assets are a particularly high-value target of malicious third parties and a critical point of vulnerability.

When using access control solutions that utilize biometric data, it is even more crucial for businesses to take extra precautions to safeguard that data. This is because—unlike usernames and passwords, which can easily be changed—an individual's biometric data has forever lost its ability to be used as a secure identifying mechanism after a security incident involving the compromise of such data. As noted in the text of the Illinois Biometric Information Privacy Act ("BIPA"):

> *Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, [and] is at heightened risk for identity theft[.]*

Furthermore, 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 come to realize that data security is a right and expect that the companies that they are employed by will protect that right, as well as their data.



Biometric Privacy

Finally, companies that implement biometric-powered access control systems must also comply with the growing patchwork of biometric privacy laws and regulations that continues to expand at the state and municipal levels in the United States.

Currently, there are three states that have biometric privacy laws which require compliance when using any form of biometrics:

1. *Illinois's BIPA, 740 ILCS 14/1, et seq.;*
2. *Texas's Capture or Use of Biometric Identifier Act, Tex. Bus. & Com. Code § 503.001 ("CUBI"); and*
3. *Washington's RCW Chapter 19.375 biometric privacy statute, Wash. Rev. Code § 19.375.010, et seq. (more commonly known as "HB 1493").*

Of the three active, targeted biometric privacy laws on the books at this time, BIPA is considered the most stringent and has created the greatest amount of liability exposure for companies that use facial authentication or other forms of biometrics in their operations.

Generally speaking, these statutes impose a common set of core compliance requirements, which entail the following:

- ***Privacy Policy.*** *A publicly-available privacy policy must be established setting forth a employer's retention schedule and guidelines for permanently destroying biometric data.*
- ***Data Retention/Destruction.*** *Biometric data must be permanently destroyed when the first of the following takes place: (1) the initial purpose for collecting the biometric data is satisfied; or (2) within a year of the last interaction between an individual and the employer.*
- ***Notice.*** *Written notice must be supplied to all data subjects prior to the time any biometric data is collected.*
- ***Consent.*** *Written consent (sometimes referred to as a "release") must be obtained from all data subjects prior to the time any biometric data is collected (or disclosed).*
- ***Disclosures.*** *If consent is not obtained for the disclosure of biometric data, such data may not be disclosed to a third party unless the disclosure completes a financial transaction requested by a data subject, is required by law, or is required in connection with a valid warrant or subpoena.*
- ***Selling or Profiting From Biometric Data.*** *Biometric data may not be sold or otherwise used in for-profit transactions.*
- ***Data Security.*** *Biometric data must be safeguarded from unauthorized access, disclosure, or acquisition: (1) using the reasonable standard of care applicable to an employer's given industry; and (2) in a manner that is the same as, or more protective than, the manner in which other types of sensitive data is safeguarded.*



In addition, the Federal Trade Commission ("FTC") has made policing improper facial recognition practices a core focus for the country's de facto federal privacy and security regulator, which the agency accomplishes by pursuing enforcement actions for "unfair or deceptive acts or practices" involving the use of facial recognition under Section 5 of the Federal Trade Commission Act ("FTC Act").

At the municipal level, Portland, Oregon, has adopted an across-the-board ban on the use of facial recognition by private entities, Portland, Or., City Code ch. 34.10 ("Portland Facial Recognition Ordinance").

New York City ("NYC") has also enacted two ordinances governing the use of facial recognition and other forms biometrics by specific industries:

1. *the NYC "Commercial Establishments" Biometric Identifier Information Ordinance, N.Y.C. Admin. Code § 22-1201, et seq. ("NYC Commercial Establishments Biometrics Ordinance"); and*
2. *the NYC Tenant Data Privacy Act, N.Y.C. Admin. Code § 26-3001, et seq. ("TDPA").*

Broader, more comprehensive state consumer privacy laws—specifically, the California Privacy Rights Act of 2020 ("CCPA"), Colorado Privacy Act ("CPA"), the Connecticut Data Privacy Act ("CTDPA"), Utah Consumer Privacy Act ("UCPA"), and Virginia Consumer Data Protection Act ("VCDPA")—also contain provisions that directly implicate the collection and use of biometric data. In addition to including biometric data within their scope of covered personal information, these laws also categorize certain uses of biometric data as a form of "sensitive" data which triggers heightened compliance obligations beyond those applicable to more general types of personal information, such as names and addresses.

In particular, these consumer privacy statutes generally impose the following compliance obligations:

- CCPA: Disclosures contained in notices at collection pertaining specifically to biometric data processing activities and adherence to the CCPA's "Right to Limit," which is akin to an opt-out right.
- CPA, CTDPA & VCDPA: Affirmative opt-in consent and the completion and documentation of a data protection assessment ("DPA").
- UCPA: "Clear notice" prior to processing biometric data and opportunity for consumers to opt-out of such processing.

Finally—similar to the new U.S. consumer privacy statutes—the European Union's General Data Protection Regulation ("GDPR") classifies biometric data—when used for identification purposes—as a subset of sensitive personal data known as "special category personal data." The GDPR generally prohibits the processing of "special category" biometric data for the purpose of uniquely identifying an individual unless one of nine exemptions applies to permit such processing. Those exemptions include, among others, explicit consent; employment, social security, and social protection (if authorized by law); and vital interests. In addition to requiring a legal basis for processing biometric data, the GDPR also requires the completion of a data protection impact assessments ("DPIA") prior to any processing of biometric data for identification purposes.

Note, however, that biometric data is not classified as "sensitive category personal data" subject to the above requirements and limitations when such data is used for purposes of authentication.

How Alcatraz AI Helps

Physical Security

Alcatraz AI's advanced facial authentication access control solution, the Rock, provides enterprise users with a myriad of significant enhancements to physical security, including the following:

Biometrics—The Superior Access Control Technology

Biometrics represents the only way of providing certainty that unauthorized individuals are not able to access restricted physical spaces. Unlike traditional access control mechanisms, such as badge cards, biometric data—by providing a method of identity authentication based on physical attributes—cannot be inadvertently lost, shared, or copied, resulting in a superior level of physical security.

More Secure Authentication Method

Traditional access control mechanisms leave companies vulnerable to malicious security incidents through a range of vulnerabilities, such as stolen credentials and social engineering. The Rock allows employees and others to automatically and seamlessly prove who they say they are using just their face, eliminating the need for unwieldy passwords and easily lost badge cards.





Top Performance in Accuracy

The Rock's use of advanced facial authentication—with 2D and 3D sensors onboard capturing data—provides a higher level of accuracy during the authentication process, further contributing to the delivery of a superior level of physical security as compared to other forms of access control. In addition, the facial authentication algorithm used by the Rock has undergone extensive testing by the National Institute of Standards and Technology ("NIST"), a non-regulatory federal agency of the U.S. Department of Commerce responsible for utilizing its expertise to assist both the private sector and the federal government in the development and promulgation of voluntary consensus standards ("VCS") relating to a range of critical information security and privacy matters. Of note, NIST testing has verified the accuracy of the Rock's facial authentication technologies and the extremely low likelihood of mistaken identities among all demographics.



Tailgating Detection

A long scanning range and field of view allows the Rock to detect and prevent tailgating. Auto-tagging and alerts allow administrators to address concerns without the need for specialized guards or other hardware.



Video Monitoring

The Rock functions as an Open Network Video Interface Forum ("ONVIF") camera, offering an even higher level of security and providing a unique perspective of personnel accessing secure areas by allowing security teams the ability to monitor developments at access control points, and assess potential threats, in real-time.

> We knew that tailgating was happening, but until we implemented the Alcatraz AI Rock, we had no idea to what extent - we were playing with fire"

Multi-Factor Authentication (MFA)

The Rock's access control system can be paired with any third-party badge reader for a two-factor or three-factor security solution and enhanced security in more restricted areas.

Protect Against Sophisticated, Evolving Threats

The Rock's advanced face biometric capabilities provide a superior level of security and protection against even the most sophisticated forms of identity theft and other fraudulent techniques, such as deepfakes and synthetic identities—ensuring the highest level of security against evolving threats, while delivering a paramount user experience.

Cost Reductions

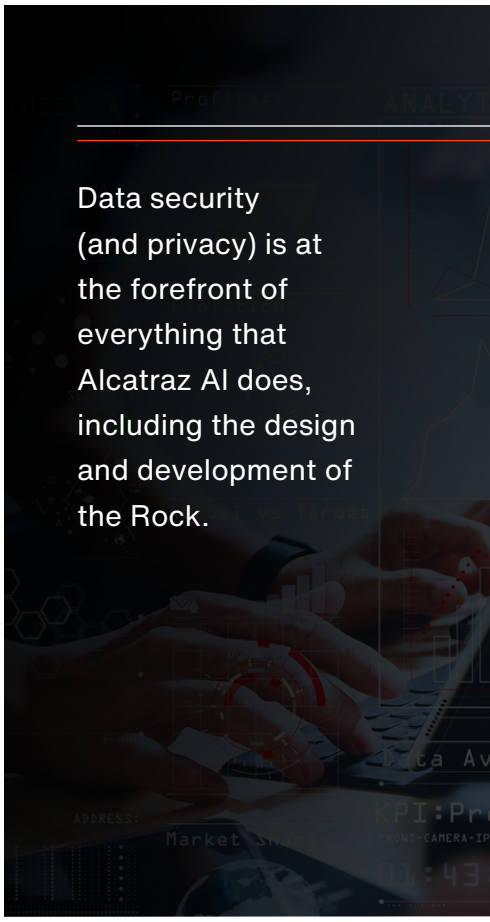
The Rock's utilization of advanced AI and machine learning capabilities provides users with an access control mechanism that not only provides an increased level of security, but also significantly reduces the cost associated with using an automated access control mechanism.

Leveraging the world's number rated facial recognition algorithm, the Alcatraz Rock is the leader in next-level access control technology.



Data Security

Data security (and privacy) is at the forefront of everything that Alcatraz AI does, including the design and development of the Rock. For this reason, the Rock has number of features built into its hardware that provide for a high level of security over the data that is processed and stored through Alcatraz AI's advanced access control solution, including the following:



Data Security Certifications

Alcatraz AI has proven its commitment to delivering enterprise-grade, biometrics-specific security and privacy safeguards through its acquisition of several universally-recognized certifications offered by the International Organization for Standardization ("ISO"), the world's largest developer and publisher of international enterprise and industrial security and privacy standards. Alcatraz AI is certified in ISO 27001, ISO 27017, and ISO 27018, and continues to not only meet—but exceed—industry standards for security and privacy.

Tamper Detection

The Rock's advanced technology allows real-time alerts if anything happens to the device. Even when removed, the system is secure.

Encryption

The Rock processes, transmits, and stores all facial biometric data in an encrypted format—both while in transit and at rest—to significantly mitigate the risk of data compromise when employees use Alcatraz AI's access control system for identity authentication purposes.

Profile Expiration

To better ensure that only authorized individuals have access to secure areas, the Rock offers an "auto delete" option that removes users who have not accessed the system during a timeframe as defined by the user's security team.

Admin Portal SSO Configuration

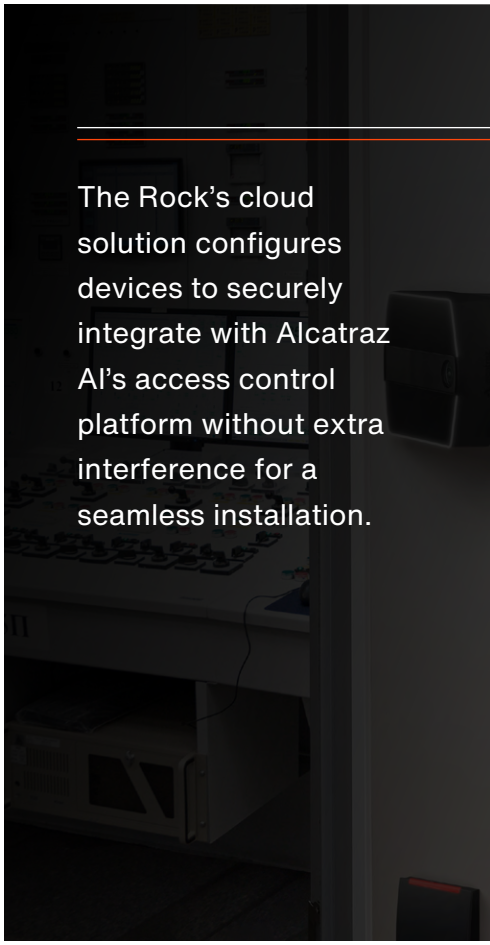
The Alcatraz AI admin platform is designed to seamlessly integrate with leading single sign-on (“SSO”) companies, including Microsoft Azure Active Directory, Okta, and Ping Identity, to increase the level of security and compliance at points of potential cyber-attacks.

Cloud Data Storage Solution

The Rock’s cloud solution configures devices to securely integrate with Alcatraz AI’s access control platform without extra interference for a seamless installation. The system logs profiles on the edge (in the device) and then stores them in the Alcatraz AI cloud, for easy profile management and storage. More than that, the storage of data in Alcatraz AI’s cloud—separate and apart from physical Rock devices—provides a much more robust level of security, all without introducing any added friction.

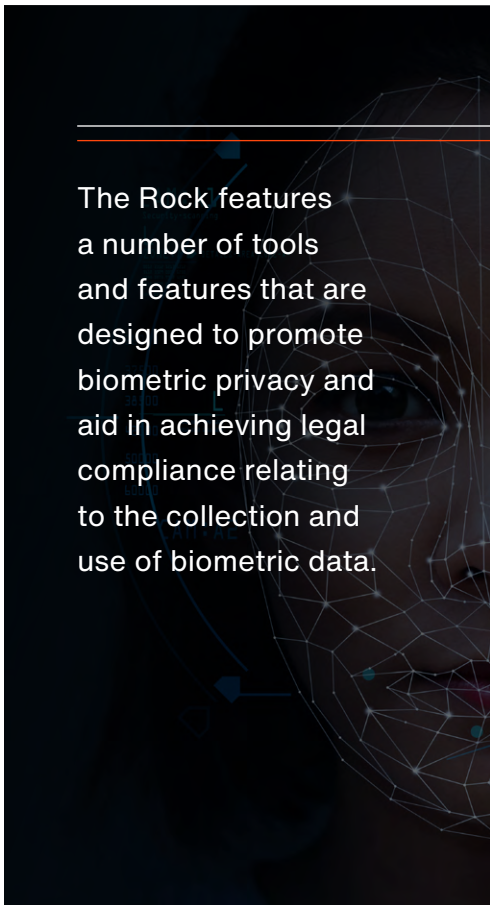
Data Security Legal Compliance

For companies operating in regulated sectors, the high level of data security built in to the Rock allows clients to ensure they satisfy applicable data security requirements relating to the collection and use of personal data through the operation of their face biometric-powered access control solution. With the Rock, companies are better positioned to satisfy even the most rigorous data security standards through use of a more secure authentication mechanism (what you are) that is superior to both passwords (what you know) and device-based methods (what you have).



Biometric Privacy

As indicated above, today employees, contractors, vendors, and visitors not only expect, but demand, transparency regarding the purposes for which their biometric data is collected and how that data is safeguarded, as well as control over how their biometric data is used. With its suite of biometric privacy-focused features, The Rock provides Alcatraz AI customers with a visible demonstration that they take the privacy and security of biometric data seriously. In particular, the Rock features a number of tools and features that are designed to promote biometric privacy and aid in achieving legal compliance relating to the collection and use of biometric data, including the following:



Advanced Biometric Privacy Controls

The Rock provides a range of tools that can be configured to aid in achieving compliance with any combination of the growing patchwork of laws and regulations that govern the collection and use of biometric data, including non-access user management, real-time event log monitoring, customizable data retention schedules, and hard data deletes.

Data Deletion

The Rock can be configured to automatically delete employees' profile data from the system at any given time or interval. Employee profile data can also be manually deleted at any time (but only by authorized personnel) from all Rock devices that are a part of the system, as well as from Alcatraz AI's platform.

Audit Trail

The Rock records the time and date of each employee's use of the Alcatraz AI access control solution and provides access to such data in its platform, along with the ability to obtain copies of this information for record-keeping and compliance purposes.

THIS DOES NOT CONSTITUTE LEGAL ADVICE. This publication may not be reproduced or distributed in any form without Alcatraz AI's prior written permission. It consists of the opinions of Alcatraz AI, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Alcatraz AI disclaims all warranties as to the accuracy, completeness, or adequacy of such information. Although Alcatraz AI materials may address legal issues, Alcatraz AI does not provide legal advice and its informational materials should not be construed or used as such.

Now is the time to modernize and upgrade your access control security

Contact Us

Alcatraz.ai

sales@alcatraz.ai

Connect with Us on Social Media

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/contact/demo

Schedule a demo

Intertek · FC · CE · ISO 27001 · ISO 27017 · ISO 27018 · BIS · NDAA COMPLIANT · BIPA · CCPA · CUBI · HB 1493 · CPA · GDPR · Designed & Manufactured IN THE USA

alcatraz

© 2025 Alcatraz | All rights reserved.