EBOOK

A New Path to Securing Access to Your Data Center

alcatraz ai

Table of Contents

Introduction

As the world sees an explosion in the number and size of data centers being deployed to support the growing demand for data and internet access, more bad actors are working to exploit vulnerabilities in the infrastructure for nefarious reasons. While more attention is given to cybersecurity, more than ever data centers must protect themselves from physical security breaches that can lead to theft of data and assets causing significant financial loss and loss of institutional trust and reputation.

The Access Control Landscape

While most of the media attention focuses on an organization's virtual perimeter and how hackers exploit software vulnerabilities, a growing number of attacks on data center infrastructure are being perpetrated through gaps in an organization's physical security posture. According to Statista, as of 2022, the average cost of a data breach in the United States amounted to 9.44 million U.S. dollars, up from 9.05 million U.S. dollars in the previous year. The global average cost per data breach was 4.35 million U.S. dollars in 2022*.

It is estimated that just
more than 10%
of malicious breaches were caused by a physical security issue.

As organizations invest in cybersecurity there has been growth in physical intrusions to access the data.

Security cameras, access control readers, and other devices that make up physical security systems are often overlooked as a source of vulnerability. For several decades physical security has often been "installed, and forgotten" as it does its job. This was partially true because traditional access control technologies have not changed significantly over the years and many of the biometric technologies failed to live up to their promise. As security technology advances with organizations implementing IP-based technology and the IoT devices, more thought has been put into how this might make their network more vulnerable, rather than closing gaps in their physical security posture.

Today's modern biometric security solutions not only work to protect the perimeter of the data center by strengthening access control, but are built on decades of experience in reducing network vulnerabilities and protecting individual privacy.

In this paper, we will share how AI-enable biometric access control using facial recognition built to protect individual privacy can improve the security posture of a data center, while increasing efficiency, and reducing costs.

The Challenges of Legacy Access Control Technologies

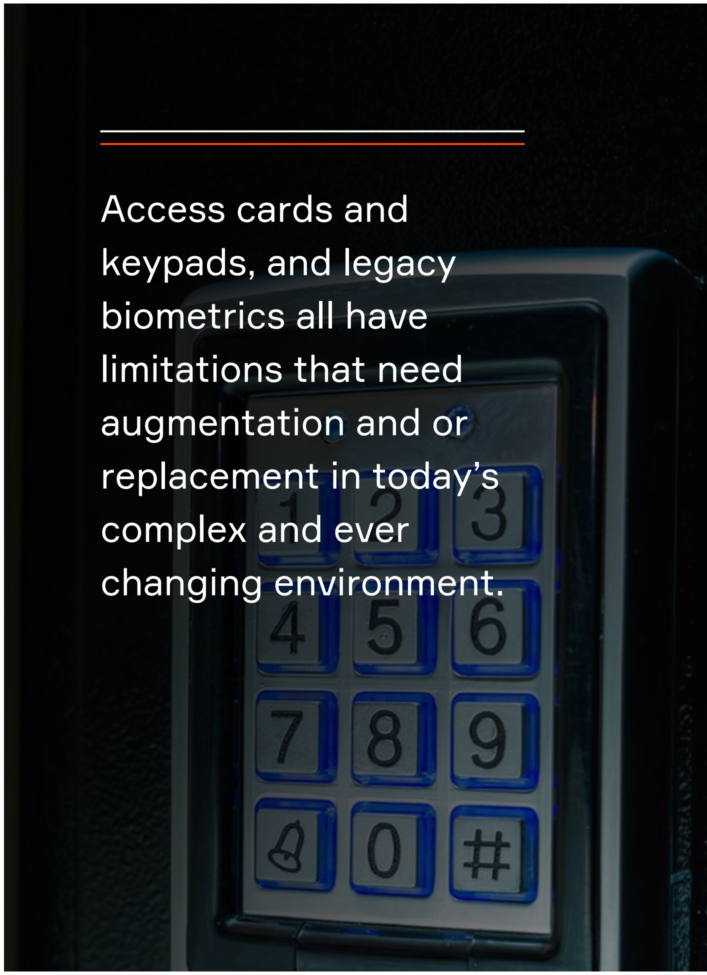
The traditional technologies used to secure and restrict physical access have not changed for many years.

Once authorized, users are provided credentials such as an access card and/or a PIN to authenticate the individual user at a keypad located near the point of access. The access control system replicates that process each time a person attempts to access the data center using credentials to verify the person is who he or she claims to be, then validate they are authorized to have access to the location or locations they are trying to access. For areas that need additional security, biometric access solutions such as finger-print readers, iris readers, or other biometric recognition are deployed. This process requires the system to authenticate a person by what they have, what they know, and with the biometric confirmation of who they are.

The physical security posture also typically includes security personnel on-site.
However, each of these has impediments and challenges that have made data center security more penetrable than it should be.

Note: While there are other important technical and physical barriers used for access control, for this paper, we will focus on the authorization and authentication systems, not mantraps or other security devices/measures used to prevent or deter access and theft.

Imagine using a cell phone of the 1990's today. While you could still communicate via voice and text, virtually all the other benefits of technology are lost to you. Similarly, access cards and keypads, and legacy biometrics all have limitations that need augmentation and or replacement in today's complex and ever changing environment.
In this next section we'll highlight the challenges of each solution.



Access cards and keypads, and legacy biometrics all have limitations that need augmentation and or replacement in today's complex and ever changing environment.

The Monetary Cost of One Tailgating Breach

Tailgating Risks

Letting the wrong person into your building can have a devastating impact on your business in different ways. Here are five reasons why you need to stop tailgating.

- **A tailgater may be someone who desires to injure a family member, ex-spouse, or friend that works at your facility.**
- **If not data from hard drives or servers, the tailgater might be looking for supplies, raw materials, computers, or other valuable assets.**
- **Less common, but not unheard of in today's social world it might be an influencer or non-mainstream media person looking to sell a negative story or dig up negative information.**
- **Similarly competitors can find and leak information that could cause damage to your reputation, or,**
- **A person might infect your network with malware or ransomware, leaving your company disabled for days and even weeks.**

The Infrastructure Security and Resilience (ISR) Forum, reports that 41% of security executives estimate that one tailgating incident gone wrong will cost an organization between $500,000 to $2 million.

Even knowing the potential cost of a breach, 71% of respondents reported that their company is very likely or likely to experience a data breach due to tailgating.

A big concern is that employees don't see an issue with tailgating. In fact, 80% believe the actual cost of tailgating is insignificant. Where security personnel KNOW tailgating needs to stop ASAP. Sadly, traditional access control systems do not provide insights and actionable information to support the needed change in behavior with employees - until now.

41% of security executives estimate that one tailgating incident gone wrong will cost an organization between **$500,000 to $2 million**.

Access Cards

Access control cards are ubiquitous in the industry for their simplicity and ease-of-use.

In the data center environment it is rarely, if ever, used as a standalone control device, rather used in less secure areas or in a multifactor system. It is, however, that simplicity that makes them vulnerable in secure areas. Just because a card is used it does not guarantee that the person accessing the location is the person the card was registered to. Cards can and are shared, lost or stolen. Meaning you cannot accurately identify who specifically entered. Access cards are also ripe for tailgating or piggybacking as most systems cannot detect the number of people that enter once a card has been swiped. It is difficult for data center operators to pinpoint who is entering a restricted area at a given time.

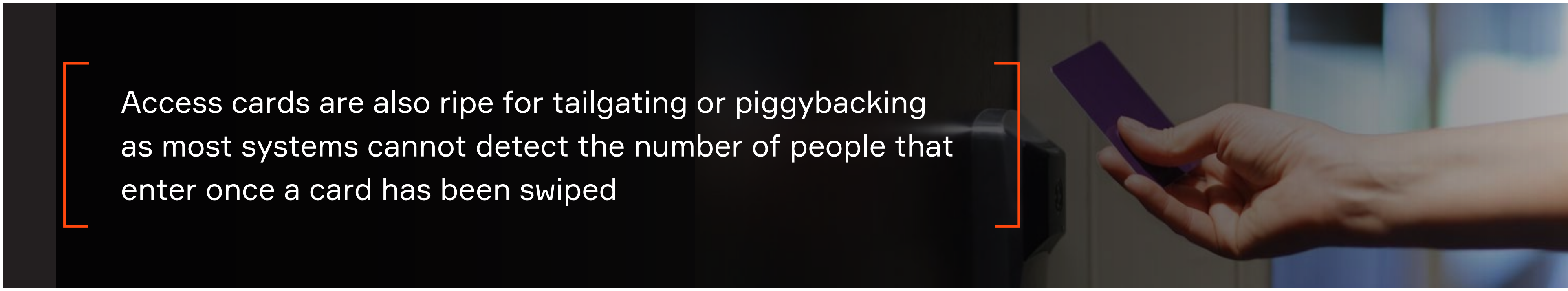
If a perpetrator were to use a stolen card or follow an authorized employee through an entryway, very little could be done to detect this wrongdoer before it was too late. The other downside to access cards is the burden of enrollment and card replacement. Data suggests that 10-to-15 percent of employees need to replace their access card each year, even more forget them meaning they have to wait to get new credentials and the security or human resource team loses productivity when they stop to enroll someone. This is in addition to the minimal cost of the badge, but together the process and assets can become costly.

› Advantages of Access Cards:

- Inexpensive and widely accepted
- Status quo

› Disadvantages of Access Cards:

- Can be lost or stolen
- Easily replicated
- Heavy lift operationally
- Not a good user experience
- Has friction and not secure



Access cards are also ripe for tailgating or piggybacking as most systems cannot detect the number of people that enter once a card has been swiped

Keypads

Keypads remain one of the most common choices in access control, particularly when a multifactor authentication system is required.

The function of keypads in access control is simple. A door or gate remains locked until the user enters a valid combination string into a nearby number pad, usually a sequence of numbers. Most access control applications assign each user their own number, called Personal Identification Number (PIN). Unless the user enters a valid combination, the opening remains locked. Keypads are particularly attractive because of lower operating cost relative to credential-based options as there are no access cards or fobs to purchase or challenges of enrollment as with most biometric solutions.

However, keypads, like access cards are prone to weaknesses such a PIN being easily shared, worn or dirty buttons revealing codes, and people snooping to steal and memorize a person's PIN. More importantly, the use of keypads are vulnerable to tailgating and piggybacking as most systems cannot detect the number of people that enter once.

Advantages of PIN Readers:

- Typically lower cost of operations.
- Requires engagement of the person being authenticated.

Disadvantages of Readers:

- PINs can be shared or compromised.
- Users forget PIN require burdensome re-enrollment
- Cannot detect tailgating or piggybacking

Biometric Devices

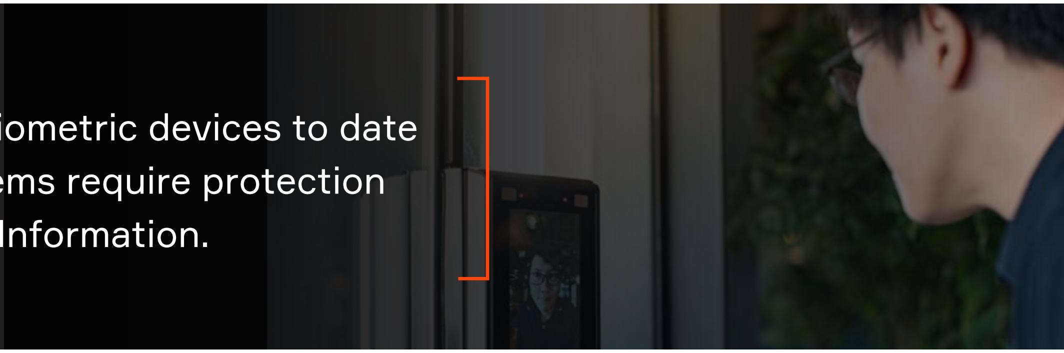
Biometric readers identify individuals through recognizable data or characteristics that are unique to them such as a person's iris, their fingerprint, hand or palm, or face.

Traditional biometric technologies–fingerprint readers, for example–have sought to fill the gap for an ultra-protective access control system but have weaknesses that have prevented them from living up to their promise and, while increasing security, made utilization more cumbersome for the end user, and management more difficult for the security administrators.

While the biometrics are unique individual identifiers, hackers have learned methods to get around the challenges by using masterprints for fingerprint or palm devices and spoofing facial recognition systems.

Iris readers are arguably the most secure, but tend to cause the biggest challenges for efficient movement and enrollment management. Finding the balance between easily and quickly enrolling people is typically a challenge and changes in individuals such as wearing glasses, going from beard to no beard, require time consuming re-enrollment. In addition, these biometrics often decrease the efficiency of movement between areas, incenting regular users to find ways around the system to improve their movement and use.

However, the biggest concern and challenge for biometric devices to date has been privacy of the user as the systems require protection of a person's PII or Personal Identifiable Information. This is valuable information that nefarious individuals would like to access and in some cases organizations or governments have abused it. The organization needs to treat sensitive biometric data with increased security, caution, and processes to protect against violations of regulation and compliance



The biggest concern and challenge for biometric devices to date has been privacy of the user as the systems require protection of a person's PII or Personal Identifiable Information.

Biometric technologies are more and more widely used, but there are still misconceptions on how the technology works as well as its advantages and disadvantages.

Advantages of Fingerprint Scanning:

- Fingerprints are unique identifiers to the individual.
- Most people are familiar with using the method.
- No need to remember complex passwords.

Disadvantages of Fingerprint Scanning:

- Temporary or permanent injuries and scars can interfere with scans.
- It can be bypassed with methods that copy and replicate fingerprints.
- In rare cases, it can be bypassed by using someone's finger while they are unconscious or incapacitated.

Advantages of Iris Recognition:

- The Iris is well protected against damage from minor injuries or changes that affect scanning devices.
- The iris is an invariant organ with a high level of randomness between individuals.
- No need to memorize complicated passwords.

Disadvantages of Iris Recognition:

- This technology requires friction at the point of access.
- Requires varying distances between the device and the user's eye causing challenging user experience
- In certain light conditions, the chances of iris recognition can be poor.
- Does not detect or inhibit tailgating or piggybacking

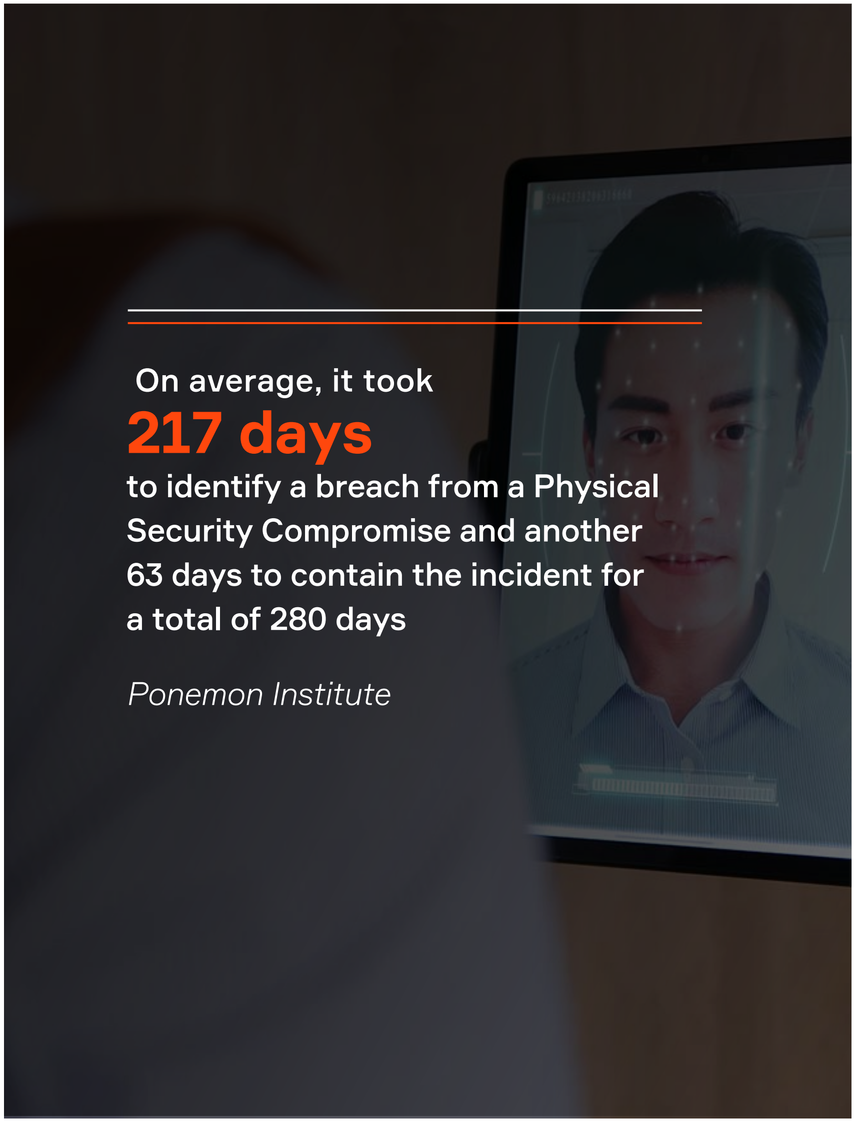
Legacy facial recognition technology has become increasingly popular in recent years, but similar to other biometric technologies there are misconceptions as well as advantages and disadvantages.

Advantages of Legacy Facial Recognition:

- Requires limited interaction with the device compared to cards or codes.
- Effective when combined with other biometric and traditional methods.

Disadvantages of Legacy Facial Recognition:

- Lighting changes can affect system performance and accuracy.
- Facial expressions, loss of weight, shaving or having facial hair may change the system's performance and accuracy.
- Facial accessories such as glasses can make it difficult to recognize the user.
- Burdensome enrollment process.
- Protection of PII



On average, it took

217 days

to identify a breach from a Physical Security Compromise and another 63 days to contain the incident for a total of 280 days

Ponemon Institute

Future Proof and Protect Your Data Center

Next we'll look in-depth at the six key elements of a modern facial biometric offering that can help prevent security breaches, ensure regulatory compliance, and maintain business continuity.

1. Built to protect privacy and support regulatory compliance

2. Designed to simplify enrollment and administration while increasing security

3. Works natively with existing systems - no "rip and replace"

4. Offers needed flexibility and scales with your needs

5. Tailgate detection and alerting with ONVIF compliant video and analytics

6. Built with trusted technology

What to Look for In A Modern Biometric Access Control Device

When looking for technology to strengthen your security posture, improve the efficiency of your operations, reduce costs, and support other business initiatives, improvements in biometric technology, particularly facial authentication, are making it more simple and secure.

Here is what you should look for:

1. Built to protect privacy and support regulatory compliance

The vendor you select should prioritize protection of data and individual privacy as a priority in their product development and their deployment strategies. The device should not store PII and have features that automatically delete records and data based on parameters established in your company's GDPR, BIPA, and or CCPA processes and requirements. Also, select a partner that provides insight and best practices for deployment of their devices to help you prevent future issues.

2. Designed to simplify enrollment and administration while increasing security

For most organizations the process of enrollment and reissuing credentials that are forgotten, lost, stolen is inefficient and costs more than they think when one considers lost productivity and the effect of interruptions on the workflow. While most companies plan for enrolling new employees, contractors, and visitors, re-enrolling people requires security or HR or someone to stop their important work to engage with the person in what is often a time consuming process. Select a solution that simplifies the enrollment process by making it more autonomous and provides the flexibility you need depending on your security posture. For instance, can people who only access less secure areas quickly self-enroll or for more secure areas are they able to do it quickly in the presence of security personnel, but with no physical involvement from the team.

Alcatraz AI has coined the phrase "Autonomous access control experience".

This applies to the experience end users see by not having to do anything besides walk up to the door to enter, but it also applies to the enrollment process. For people that have an iPhone, and of course there are millions of them, they enrolled in Face ID without the help of an administrator. We set out to make the access control enrollment just as simple. Employees, contractors, or visitors, simply walk up to a dedicated self enrollment station on a stand - with or without security present. They present their access card and follow the visual cues on the LED screen to move their head up, down, left and right and in a few seconds they will get the green check that enrollment is complete.

3. Works natively with existing systems - no “rip and replace.”

The ideal solution should work with your existing access system - both hardware and software, to avoid costly equipment replacement, labor and programming of a new system. It is also ideal to purchase a solution that does not require software integrations to work with your existing systems. These integrations take time to develop, are costly and can often be “broken” when new versions of the native system are released, necessitating patches to be written to repair the integrations.

4. Offers needed flexibility and scales with your needs

Look for a vendor that provides a cybersecure, hardware-as-a-service offering. This provides you with the ability to continuously access new features, improve remote management, reduce IT and system maintenance costs, and scale with the needs of your operations. This combination of hardware and software, protected by secure infrastructure delivers the greatest amount of flexibility and options for the future.

5. Tailgate detection and alerting with ONVIF compliant video and analytics

ONVIF is a recognized standard that allows video feeds to be connected to your Video Management Systems (VMS) with minimal programming time for Integrators. An ONVIF video feed allows access events, such as tailgating, to be flagged in the VMS so that incidents can be seen in real-time if a guard is in place, or easily reviewed forensically to see who the tailgater was and who allowed the tailgater to enter. This video evidence is invaluable to both minimize the risk posed by the tailgater and to work to change the behavior of the person who allowed the tailgater to enter.

Having a door level view of the event is another plus to look for when selecting a solution. Existing cameras can also capture tailgating events, but are often mounted too high up to properly see the face of the tailgater, especially if that person prevents detection by using a cap, hood or a facial covering.

6. Built with trusted technology

Three key areas are their level of encryption, quality of cameras, and quality of facial recognition algorithm. Only select a device that fully encrypts data both at rest and in transit and uses the highest levels of encryption. Ensure that they use both 2D and 3D cameras to validate liveness and prevent spoofing. This is critical as it ensures the user is present, preventing authentication using a printed picture or pictures on phones or tablets.

Finally, ensure they have a top rating for their recognition/ authentication algorithm as tested by the National Institute of Standards and Technology.

It is particularly important to have a top rating for 1:N identification. The devices must also be NDAA compliant and designed to support your other regulatory requirements.

A New Path For Data Center Biometric Access Control

Alcatraz AI has looked at delivering secure access control from a completely different angle.

Our Founder Vince Gaydarzhiev was part of the team that developed Apple FaceID and he asked how I can take this tech that millions of people use every day to unlock their phones to open a door in the physical world in a more secure and simple way. Alcatraz AI delivers on a vision of secure, simple and frictionless access control at every step with our ground-breaking product - the Rock. Alcatraz is a simple, yet powerful physical access control solution that uses AI and machine learning to adapt to the changes in people and the environment and evolving business needs.

Using a person's face as their credential, the Alcatraz Rock is a frictionless, AI-enabled access control solution that works natively with virtually all access control solutions as a standalone reader or part of a complex, enterprise, multi factor authentication system. Built from the ground up with a focus on privacy, this facial recognition device enables touchless entry into physical locations.

Its multi-sensor technology allows it to accurately authenticate individuals from a distance and determine if they have clearance to enter a secure area or not functioning similarly to a badge, but with less friction, improved accuracy and with the features and data insights needed to detect and alert on tailgating and piggybacking incidents and deliver the information needed to address the behavioral causes of tailgating. It is PoE+ powered and uses Wiegand/OSDP outputs and inputs.

The Rock detects and alerts to tailgating incidents and provides actionable information to modify employee behavior. The Alcatraz solution only grants access to those who are registered in the access control system and denies authentication to those who are not. If an unauthorized individual tries to follow an authorized individual through the door, the Rock will detect and alert the security center through the access control system.

Alcatraz AI is a simple, yet powerful physical access control solution that uses AI and machine learning to adapt to the changes in people and the environment and evolving business needs.

The alert will be logged in the system along with a still picture of the unauthenticated person from the ONVIF camera positioned at eye level so that security can act quickly and with certainty to identify who the tailgater is and identify the person who allowed the behavior. Reports can be run that identify tailgating incidents, the number of tailgaters, and provide insight into the employee(s) who allow tailgaters so that corrective action can be taken to change their behavior.

Leveraging the world's number rated facial recognition algorithm, the Alcatraz Rock is the leader in next- level access control technology and offers a suite of features to strengthen your security posture, while reducing the administrative burden and improving the user experience.

It can be used as a primary authentication or multi-factor authentication device that can supplement an existing access control infrastructure without the need to “rip and replace” the current infrastructure.

Features of Alcatraz AI The Rock

- **Multi-Sensor Technology**
- **PoE Powered**
- **Wiegand/OSDP Outputs & Inputs**
- **Tamper Detection**
- **Thoughtful User Interface**
- **Enrollment Intelligence**
- **Tailgating Intelligence**
- **Mask Enforcement**

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

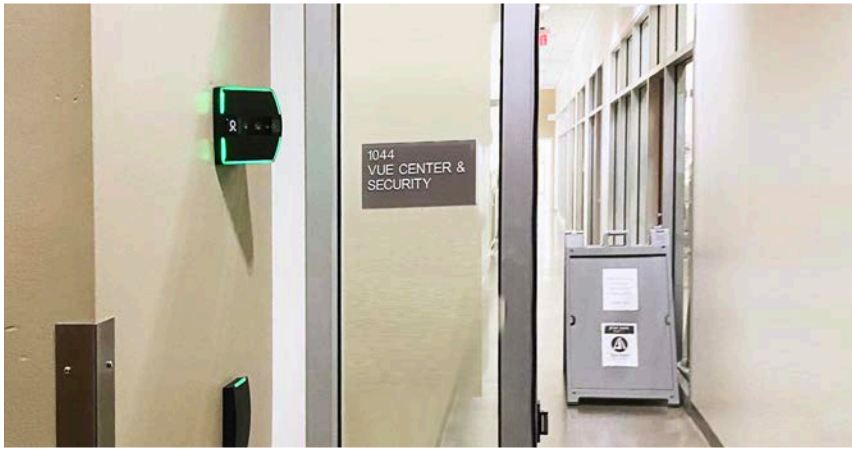
Primary Data Center Use Cases for Alcatraz AI

Building entry screening

The Rock can be used as the primary access control device to enter the building, or added to augment and strengthen the current system. As all entrances and locations require the use of individual authentication to gain access to relevant areas of the data center, strengthening security at the first step and ensuring it is “the authenticated” person versus an authenticated card or PIN, provides an added layer of protection. The Rock’s simple enrollment process helps ensure the right person is granted access, and that visitors who are properly screened can be more efficiently and effectively enrolled in the system.

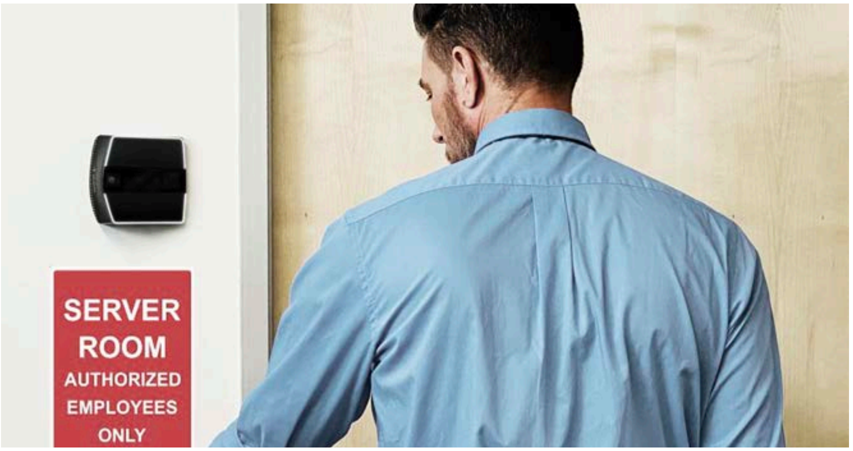
Secure corridors

The Rock already works with many of the leading mantraps and turnstile providers. Adding the facial authentication at this layer can help you better maintain the flow of people at the front entrance, help prevent tailgating of unauthorized individuals into secure areas, and increase the effectiveness of security personnel by alerting them to unauthorized individuals and tailgaters in real-time. It helps remove the element of human error in recognizing a person, or catching a person who might have had access privileges revoked or otherwise changed, but security personnel are unaware.



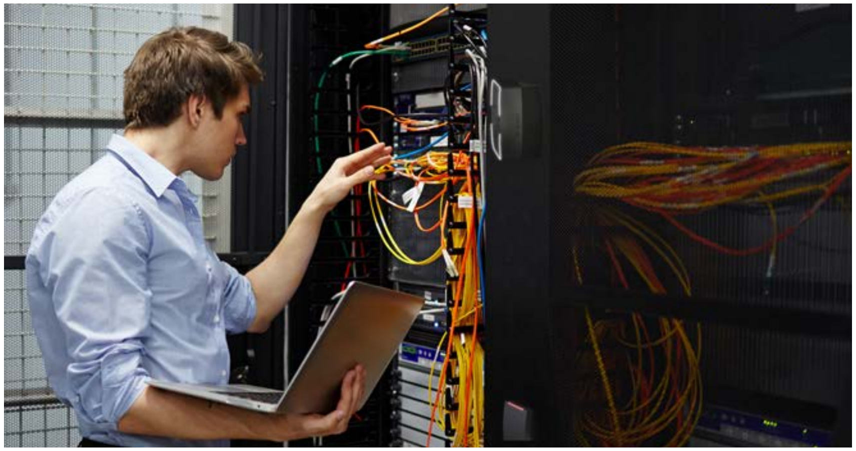
Computer room access

The next layer of authentication is at the computer room (server room or suite) where entry is only granted upon dual authentication via badge and biometric facial authentication system. The use of facial biometrics from Alcatraz AI, increases the security and allows two-factor authentication at the speed of one factor authentication, and again alerts and information to prevent tailgating and ensure compliance by individuals.



Cage or rack level access

In virtually every instance, the final layer of authentication at the cage or server rack level is accessed by key lock or card reader and biometric scanner. A Rock on each cage or rack can help ensure only authorized and authenticated individuals access the area. The addition of the ONVIF compliant camera at “eye level” provides additional validation and improved forensic data should there be a concern or incident. Because the Rock works natively with your current systems, individual tenants could choose to add Rocks to their racks/cages to increase their posture and the data center manager without disruption to the current infrastructure. The view from the Rock is much better than the traditional video wall or ceiling mounted cameras that also monitor sites.



Cover remote access points and augment

Human intervention in the form of security guards is a key element of the physical security environment in most data centers. However, guards cannot be at all access points at all times, and human relationships and behavior create identification and accountability errors that can compromise the security posture. The Rock can be used at remote locations to augment your human resources covering remote corridors, emergency exits, and in other unique locations. The Rock is like a security guard at every door that never goes on rounds, takes breaks, or gets distracted by outside stimuli. Unlike humans the Rock manages access authorization based on the access control system criteria and makes only data-driven decisions without regard for relationships or rare potential for manipulation by third parties, and unlike humans it is always vigilant. The Rock's detection and alerting capabilities, along with high-quality video gives security guards better data and information to do their job.

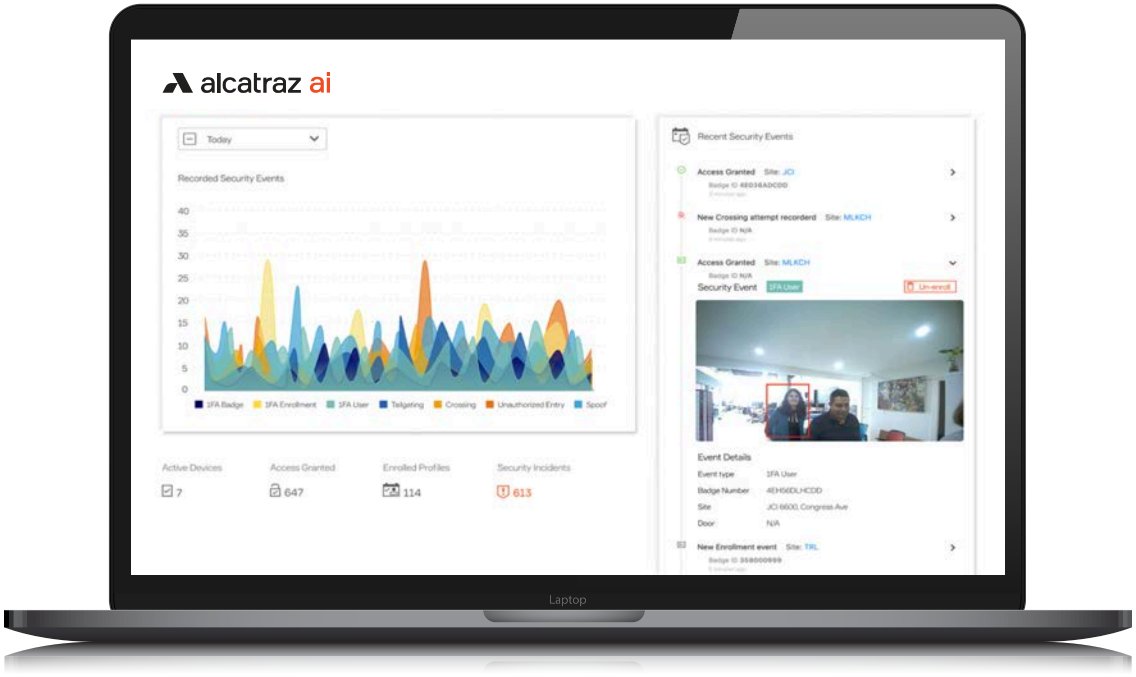
> One data center customer told us they "had zero tolerance for tailgating" but admitted no one had ever been terminated as they lacked the data and video to change people's behavior and positively identify employee offenders, until now."
>
> – Greg Sarrail, Vice President, Alcatraz AI

Summary

The complexities of data center environments, changes in employee, contractor and customer behavior in the post-COVID environment, staffing challenges with security personnel, combined with the increased sophistication of "bad actors" makes protecting a data center more difficult than ever.

The legacy technologies of the past have and continue to play a role in the physical security of facilities, but modern biometric technology, artificial intelligence, and machine learning are quickly replacing those legacy devices or being added to the current access control systems to increase security, improve efficient movement of people, and support regulatory and legal compliance, all while protecting the privacy of individuals.

The Rock from Alcatraz AI can not only make your data center more secure, it can help you operate more efficiently and create a better user experience for everyone who is authorized to be there and your team that has to manage and administer the system. It's time to take a new path to protecting your data center with biometric access control.



Active Devices 7

Access Granted 647

Enrolled Profiles 114

Security Incidents 613

Access Granted Site: JCI
Badge ID 4E036ADCDD

New Crossing attempt recorderd Site: MLKCH
Badge ID N/A

Access Granted Site: MLKCH
Badge ID N/A

Security Event 1FA User

Event Details

Event type 1FA User
Badge Number 4EH56DLHCDD
Site JCI 6600, Congress Ave
Door N/A

New Enrollment event Site: TRL
Badge ID 358000999

To learn more about how Alcatraz can strengthen your access control schedule a free demo to witness firsthand how simple and effective the Rock is to use.

Contact Us

Alcatraz.ai

sales@alcatraz.ai

Connect with Us on Social Media

f www.facebook.com/alcatrazai

in 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

UL FC CE ISO 27001 GDPR CCPA

alcatraz ai