

EBOOK

Navigating the Future of Data Center Security

Genetec™

 alcatraz ai

Table of Contents

- 3 Introduction: Access Control Landscape
- 4 The Challenges of Legacy Access Control Technologies
- 5 The Monetary Cost of One Tailgating Breach
- 6 Future-Ready and Protect Your Data Center - What to Look for In A Complete Modern Access Control Solution
- 8 A New Path For Data Centers: Simplify Access and Increase Security with Genetec and Alcatraz AI
- 9 Primary Data Center Use Cases for the Alcatraz AI Rock and Genetec
- 10 Who Benefits from Alcatraz Facial Authentication and Genetec Security Center
- 11 Summary

Introduction

As the world sees an explosion in the number and size of data centers 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 much attention is given to cybersecurity, more than ever, data centers must protect themselves from physical security breaches that can lead to the theft of data and assets, causing significant financial loss and loss of institutional trust and reputation.

The Access Control Landscape

While most media attention focuses on an organization's virtual perimeter and how cybercriminals exploit software vulnerabilities, attackers increasingly exploit gaps in an organization's physical security posture to target data center infrastructure. The 2023 IBM Cost of a Data Breach Report calculated the average cost of a data breach from a physical security penetration at \$4.1 million. The same study reports that almost ten percent of all data breaches come from a physical breach, and it could take up to 198 days to trace the breach back to the physical security violation and 69 additional days to mitigate the damage.

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

Modern biometric and security solutions protect the data center's perimeter by strengthening access control and leveraging decades of experience in reducing network vulnerabilities and protecting individual privacy.

This eBook will share how advanced access control solutions built to protect individual privacy can improve a data center's security posture while increasing efficiency and reducing costs.

Nearly 10%*

of malicious breaches are estimated to be caused by a physical security issue.

*2023 IBM Cost of a Data Breach

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, systems provide users with credentials such as an access card and/or a PIN to authenticate the individual user at a keypad or reader near the access point. 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 they claim to be, then validate they are authorized to have access to the location(s) they are trying to access. For areas that need additional security, organizations deploy biometric access solutions such as fingerprint readers, iris readers, or other biometric recognition. This process requires the system to authenticate a person by what they have and know, along with the biometric confirmation of who they are.

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

Legacy access control technology, including traditional physical systems and proprietary integrations, poses significant challenges for organizations, leading to high maintenance costs and increased vulnerability to cyber threats. Many users struggle with legacy or end-of-life platforms, which demand frequent

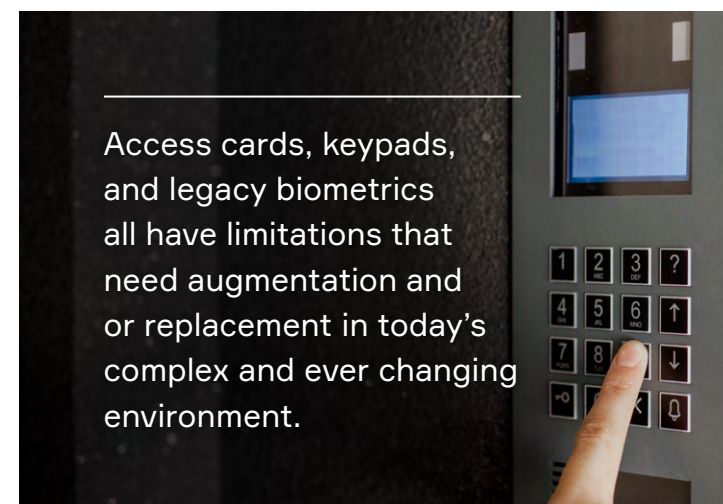
upgrades and ongoing support to mitigate risks. The expense and time required for maintaining these outdated systems are steadily rising, which makes a shift towards more modern and efficient access control solutions much more logical and valuable over time.

Outdated access control systems will also restrict organizations from leveraging new technologies, impeding their ability to adapt to an evolving physical security landscape. Integrating innovative solutions like wireless locks, among others, becomes challenging or even impossible with legacy systems. As more organizations transition to cloud technology, the limitations of legacy access control systems become increasingly apparent, hindering efforts to enhance security and streamline operations. Failure to update these systems will ultimately constrain the organization's ability to enforce security measures and optimize operational efficiency.

Finally, non-compliance with regulatory standards can pose a significant risk associated with outdated access control systems, originally designed to meet needs from over a decade ago. These systems are crucial in safeguarding sensitive information, such as employee data, from unauthorized

access. However, failing to adhere to regulations compromises the security of this confidential information, exposes employee and visitor data to potential breaches, and can result in significant fines.

Imagine using a cell phone of the 1990s today. While you can still communicate via voice and text, you lose virtually all the other benefits of technology. Similarly, access cards, keypads, and legacy biometrics and access control systems have limitations that need augmentation 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 devastating effects on your business.

Here are five reasons to stop tailgating:

- Tailgating can lead to non-compliance with regulations, potentially resulting in hefty fines, legal penalties, and damage to your organization's reputation.
- A person might infect your network with malware or ransomware, leaving your company disabled for days and even weeks.
- The tailgater might be looking for supplies, raw materials, computers, or other valuable assets, such as data from hard drives or servers.
- A tailgater may want to injure a family member, ex-spouse, or friend who works at your facility.
- Similarly, competitors can find and leak information that could damage your standing or expose proprietary information.

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 and \$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. Security personnel know tailgating needs to stop ASAP. Sadly, traditional access control systems do not provide insights and actionable information to support the required change in behavior with employees—until now.



Future-Ready and Protect Your Data Center

What to Look for In a Complete Modern Access Control Solution

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

Here is what you should look for to help prevent security breaches, ensure regulatory compliance, maintain business continuity, and maximize uptime:

1. Built to protect privacy and support regulatory compliance

The solutions you select should prioritize the protection of data and individual privacy as a priority in their product development and deployment strategies. Physical access control devices should not expose personally identifiable information (PII). They should have features that automatically delete records and data based on parameters established in your company's privacy policy and remain compliant with current biometric privacy laws. Also, select partners that provide insight and best practices for deploying their devices and solutions to help you prevent future issues. The hardware solutions must also be NDAA-compliant and designed to support your other regulatory requirements. Regulatory compliance varies not only by industry but often by location, too. You must choose an access control system that fits your organization's regulatory landscape and adapts depending on location.

2. Designed to simplify enrollment and administration while increasing security

For most organizations, the process of enrollment and reissuing forgotten, lost, or stolen credentials is inefficient. It costs more than they think when considering lost productivity and the effect of interruptions on the workflow. While most companies plan to enroll new employees, contractors, and visitors, re-enrolling people requires security, 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 coined the term "facial authentication" in 2019

Facial authentication is transforming how we verify identities in security and access control. By harnessing the unique features of an individual's face, facial authentication transcends the limitations of traditional methods like cards and PINs, providing a sophisticated yet user-friendly approach to access control. Traditional facial recognition can collect biometric data without users' knowledge or consent and compare it to a large database. However, facial authentication from Alcatraz AI allows users to opt in or out of using the solution and does not expose any PII, ensuring user privacy.

3. Tailgate detection and alerting with ONVIF-compliant video and analytics

Open Network Video Interface Forum (ONVIF) is a recognized standard that allows video feeds to be connected to your Video Management Systems (VMS) with minimal programming time for Integrators. It provides interoperability between diverse IP video devices manufactured by different entities, streamlining integration processes for developers and ensuring proper system communication. ONVIF profiles S and T allow access events, such as tailgating, to be flagged in the VMS so that incidents can be seen in real-time or quickly reviewed forensically to see who the tailgater was and who allowed the tailgater to enter. This video evidence is invaluable in minimizing the risk posed by the tailgater and working to change the behavior of the person who allowed the tailgater to enter. A solution with ONVIF capabilities will greatly improve your response time and reduce your overall risk.

4. Offers flexibility and scales with your needs

Look for solutions that provide a cybersecure, continuous feature delivery offering. This allows you to continuously access new features, improve remote management, reduce IT and system maintenance costs, and scale your operations' needs. This combination of

hardware and software, protected by secure infrastructure, delivers the greatest amount of flexibility and options for the future.

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

Always look for a system that offers flexible hardware compatibility and a scalable open architecture that enables an organization to grow naturally and integrate its existing hardware into its new access control system. To go a step further, opting for a truly unified solution allows for a more streamlined installation process, a better monitoring experience, and seamless scaling in the future.

5. Built with trusted technology

Key areas to look for in a physical access control device are levels of encryption, the quality of cameras, and the quality of the facial recognition algorithm. Remember, only select a device that fully encrypts data at rest and in transit and uses the highest levels of encryption. Ensure they use 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

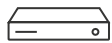
tablets. An access control solution offering OSDP (with secure channel) encryption protocols, widely recognized and accepted encryption standards, can be a sensible choice and result in security and flexibility enhancements. These bi-directional protocols ensure that sensitive information is never transmitted in plain text, further enhancing data privacy. A secure software solution built upon cybersecurity protocols is imperative when selecting a solution.

Did you know that with its truly open architecture, Synergis™ access control from Genetec allows your organization to efficiently scale in alignment with your business needs by reusing compatible third-party access control devices? This grants your organization the flexibility to choose whichever compatible hardware best fits your needs. Also, with direct-to-cloud hardware options available, Synergis is future-ready and will allow for a seamless shift to a hybrid or cloud deployment when needed.

A New Path For Data Centers: Simplify Access and Increase Security with Genetec and Alcatraz AI

Alcatraz AI and Genetec have looked at delivering secure access control from a different angle.

With its patented technology, Alcatraz AI's facial authentication solution, intelligent tailgating detection, and simplified enrollment process integrate with Genetec to transform physical security and protect individual privacy.



Seamless integration to reduce touchpoints, providing video at the door via an ONVIF camera, and incorporating the stream into the Genetec video management system.



Live tailgating detection alerts, coupled with door-level video, help to prevent the industry's most challenging breach to detect.



Automated enrollment for all authorized users without exposing any personally identifiable information (PII).



Enterprise-grade networking and security, with end-to-end encryption and customizable hosting options.

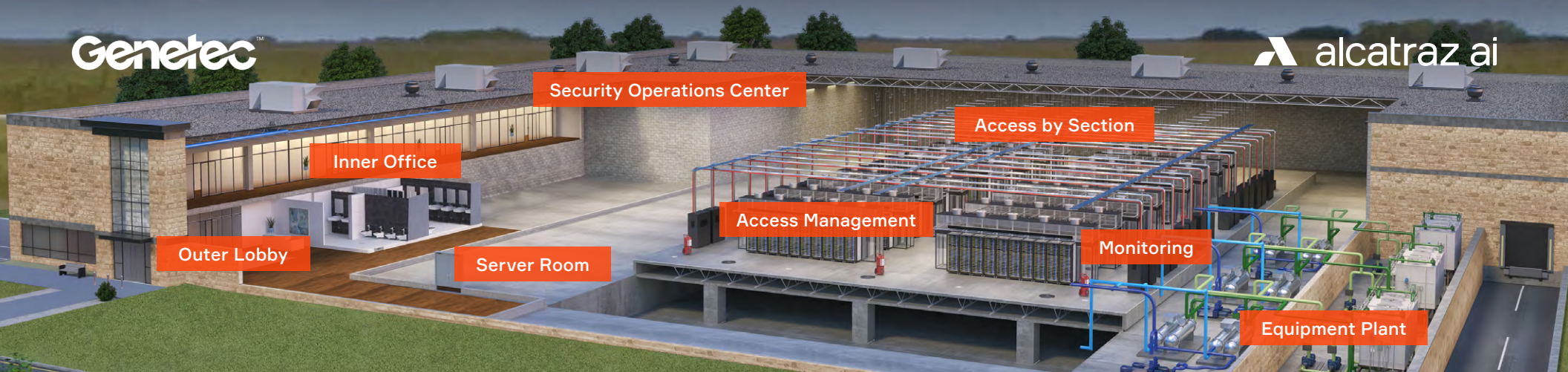


Easy-to-deploy enclosure management solutions with Synergis, which allow for a unified experience and a reduction in alert noise.



“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 of Sales,
Alcatraz AI



Data Center Use Cases

Outer Lobby

The heightened security around data centers means that even the lobby is more secure than lobbies in other facilities. Facial authentication can add a layer of protection for returning contractors or frequent vendors.

Inner Office

The office spaces in a data center require an elevated level of access control. Adding facial authentication from Alcatraz AI reduces the risk of copied or stolen card credentials.

Server Room

Alcatraz AI serves as vital biometric access validation for a two—or three-factor authentication system, securing the modern vaults known as server rooms, which store valuable information.

Security Operations Center

Overseeing the data center is a full-time job. Alcatraz AI can immediately detect tailgating incidents and provide door-level video of each event to Synergis™ to eliminate unauthorized access.

Access Management

As part of Genetec's unified approach, Synergis, and ClearID enable data centers to customize access management by granting or revoking access based on time slots, user profiles, roles, or specific area requests.

Access by Section

Data centers may structure employee access by section, representing different tier levels of service or unique customers. Alcatraz AI can ensure that only the proper staff enters the appropriate section.

Monitoring

Data centers often require constant monitoring to safeguard hardware that contains sensitive data. Using a unified solution will cause less alarm fatigue and better customization. Genetec enables companies to easily monitor alarms and intrusions through a single system and efficiently report them when needed.

Equipment Plant

A building's equipment is always essential, but cooling systems and UPS equipment are the difference between success and being out of business for data centers. Protect these vital assets by elevating the access protection by adding the Alcatraz solution.

Who Benefits from Alcatraz Facial Authentication and Genetec Security Center



Compliance Manager

Ensures that work plans meet operational standards

- Ensures that work plans meet operational standards through a unified security platform and saves time by easily retrieving information and reports for audits.
- Utilizes NDAA-compliant hardware to support compliance with BIPA, CCPA, GDPR, and other privacy standards and regulations.



IT Director

Leads all aspects of IT services to support the goals of the data center

- Enjoys working with a flexible platform built with privacy and cybersecurity in mind and feels confident having more control over access to restricted areas.
- Feels the added confidence of increased security with facial authentication to access server rooms and critical equipment.



Physical Security Manager

Assesses threat levels and mitigates security incidents

- Assesses threat levels and implements a unified security plan to mitigate security incidents, all by working from a single intuitive platform.
- Receives tailgate alerts in real time to take immediate action.



Operations Manager

Maintains smooth operations by mitigating disruptions

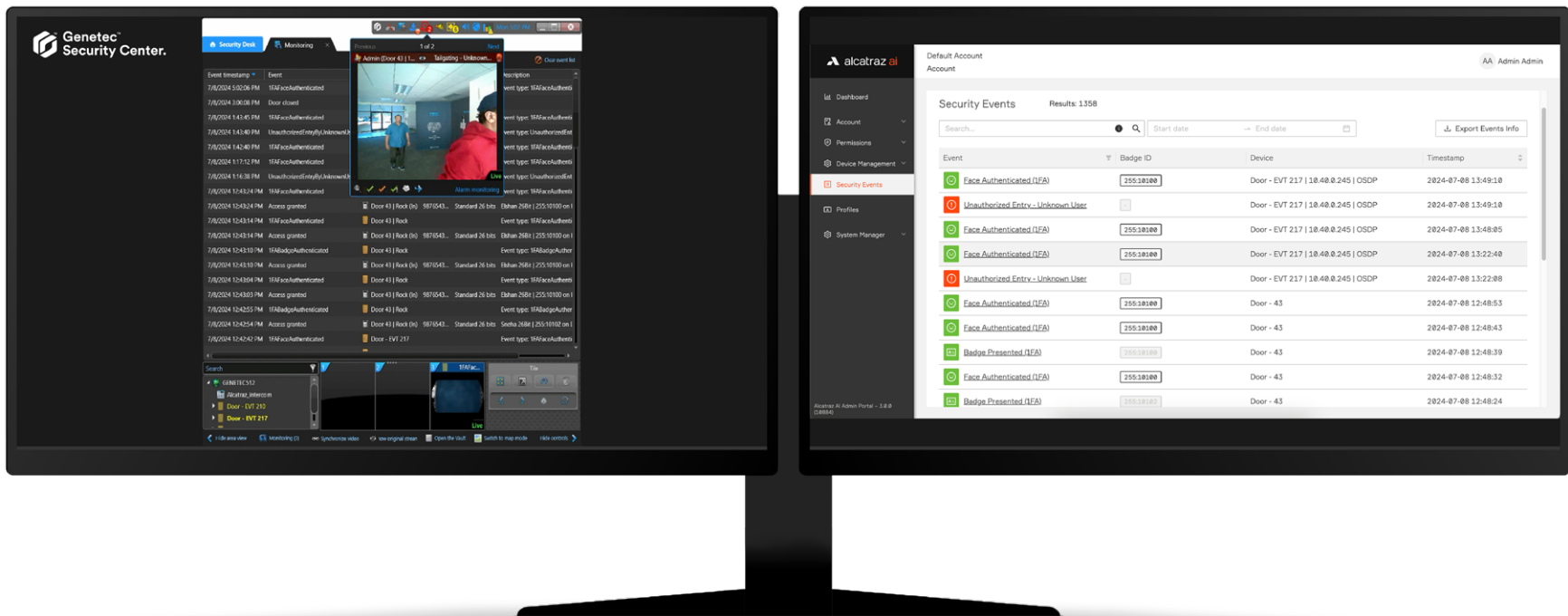
- Maintains smooth operations and secure movement of people through the facility with a cloud-based, multi-site security system that enables centralized monitoring and compliance.
- Reduces traffic during shift changes by enabling frictionless access via facial authentication while identifying anyone trying to enter the protected space who may not belong.

Summary

The complexities of data center environments, changes in employee, contractor, and customer behavior, staffing challenges with security personnel, and the increased sophistication of “bad actors” make protecting a data center more challenging than ever.

The legacy technologies of the past have and continue to play a role in the physical security of facilities. Still, modern access control technology is 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.

Facial authentication from Alcatraz AI and Genetec Security Center can make your data center more secure, help you operate more efficiently, and create a better user experience for everyone who is authorized to be there and the team that has to manage and administer the system. With Alcatraz AI and Genetec, you can navigate the future with ease and better protect your data center.



To learn more about how Alcatraz and Genetec can strengthen your access control, schedule a [free demo](#) to witness the power they harness together.

[Schedule a demo](#)

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


Contact Alcatraz AI

alcatraz.ai

sales@alcatraz.ai

(650) 600-0197

Connect with Alcatraz AI

 [linkedin.com/company/alcatraz](https://www.linkedin.com/company/alcatraz)

 twitter.com/alcatrazai

