

Unleashing the Potential of Security: Embracing Cloud-Based Access Control Systems

Unleashing the Potential of Security: Embracing Cloud-Based Access Control Systems



Executive Summary

In today's rapidly evolving digital landscape, the imperative for robust security measures cannot be overstated. Cloud-based access control systems provide unparalleled advantages and the potential to revolutionize security protocols. By harnessing the scalability, flexibility, and real-time features of cloud technology, companies can boost their security measures and gain substantial operational efficiencies. Cloud-based systems offer significant advantages such as remote accessibility, integration with current systems, and predictive analytics for threat detection, marking a crucial advancement in safeguarding assets, data, and personnel. Acre Security is committed to advancing security solutions that meet the demands of contemporary business landscapes, ensuring that organizations are well-equipped to tackle emerging challenges with confidence and resilience.

Introduction

In the realm of physical security, cloud-based access control systems are no longer a futuristic concept but a tangible, rapidly advancing solution. At a time when contemporary IT professionals, security experts, and business owners are riddled with complexities of securing data and infrastructure, cloud-based access control systems are rising as a beacon of resilience and reliability.



Native Cloud vs. “Hybrid” Access Control Systems: An Examination of Cloud Configurations

Before delving into the intricacies of cloud-based access control systems, let's begin by clarifying the fundamental terminology crucial to our discourse.



Native Cloud-Based Access Control

Native or true cloud-based access control systems signify systems that are hosted on the service provider's infrastructure, providing the communication protocols needed to directly communicate with doors by leveraging the cloud. A truly native cloud access control system does not require an on-premises appliance, and instead communicates natively to the door or reader over IP. The increased availability of internet based services across different geographic regions makes it possible for this type of system to be accessed from anywhere with an internet connection.

A native cloud approach involves designing and building applications specifically for cloud environments. It embraces cloud-native technologies and leverages the full spectrum of cloud services to deliver scalable, resilient, and agile solutions. By harnessing cloud-native app technologies, businesses can achieve enhanced resilience and scalability, driving organizational success. Cloud-based access control systems facilitate seamless communication with card readers through innovative technological protocols, ensuring efficient and secure access management.

Throughout this white paper, the features and considerations that we are discussing refer to native or true cloud-based access control.



“Hybrid” Access Control

On the other hand, some manufacturers within the access control sector may use the term “hybrid” access control to describe systems that store access control data in the cloud while relying on a hardware appliance to connect to the doors. While these systems may fulfill a purpose, they do not deliver an authentic native cloud experience.

Moreover, requiring the use of a hardware appliance instead of a native cloud environment raises hardware expenses, introduces maintenance complexities, may restrict system scalability, ties the system to physical infrastructure, and limits flexibility and mobility.

When exploring cloud-based access control systems, be certain to ask if the system is inherently cloud-based or necessitates a hardware appliance for operation.

Top Priority: Safeguarding your Access Control System Data

In a time of advancing digital threats, it's crucial to protect sensitive personnel records, building security details, and other confidential information. A robust security plan for access control not only prevents unauthorized access but also guarantees data confidentiality.

A secure network must incorporate the following key features:



End-to-End Encryption:

All data transmitted between the access control devices and the cloud server, including sensitive information such as access codes and personal identification details, must be encrypted to prevent interception and unauthorized access.

Two-Factor Authentication (2FA):

To enhance security levels, two-factor authentication should be mandatory for system administrators and users accessing the control system remotely. This adds an extra layer of security beyond just a password, often combining something the user knows (a password) with something the user has (such as a mobile device).

Regular Software Updates and Patches:

The cloud-based system should automatically receive the latest software updates and security patches to protect against newly discovered vulnerabilities and security threats.

Advanced Threat Detection and Response:

The network should be equipped with tools that continuously monitor for suspicious activities or anomalies, with the capability to respond immediately to potential threats to minimize possible damage.

Redundant Data Backups:

Regular, redundant backups of all system data ensure that, in the event of a cyberattack or system failure, crucial information is not permanently lost and can be restored to maintain continuity of operations.

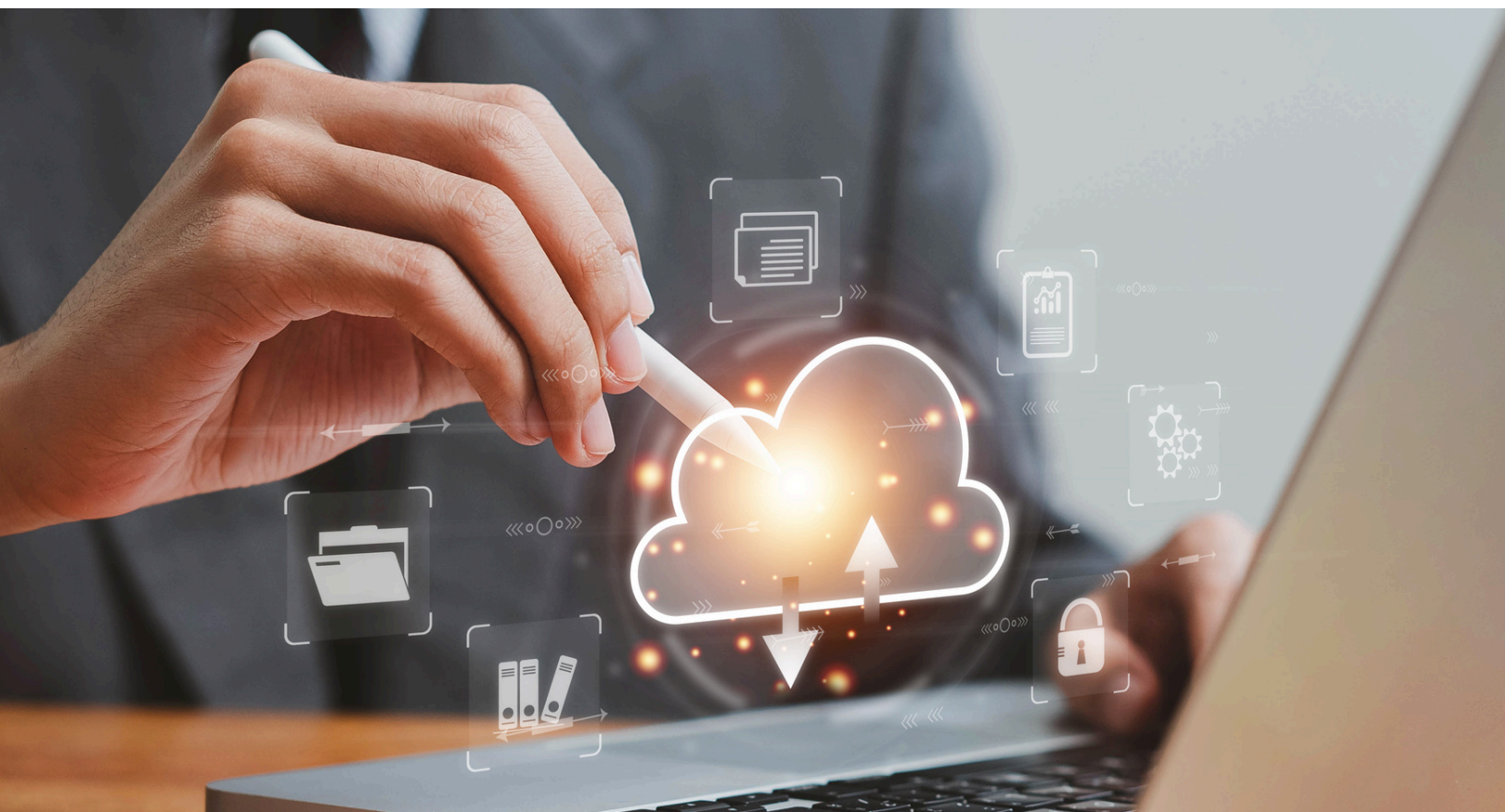
Compliance and Regulatory Requirements

Aligning with compliance and regulatory requirements is more than just a checklist; it's a necessary shield to safeguard reputation and avoid hefty fines. Cloud-based systems often come with compliance controls built-in, mitigating the brunt of manual oversights and human errors.



ISO 27001 certification holds paramount importance for cloud-based access control systems, serving as a testament to a system's reliability and the provider's commitment to data security. This rigorous international standard delineates the requirements for establishing, implementing, maintaining, and continuously improving an Information Security Management System (ISMS).

By adhering to ISO 27001, providers of cloud-based access control systems unequivocally demonstrate their dedication to safeguarding sensitive information against security threats. It reassures clients that the highest standards of data protection are not just promised but ingrained in the provider's operational ethos. Compliance with ISO 27001 is a distinguishing factor that sets apart companies committed to excellence in security, ensuring they are well-equipped to protect their clients' most valuable assets in an increasingly digital world.



Exploring the Advantages of RESTful APIs for Cloud-Based Access Control Integration

APIs (Application Programming Interfaces) serve as the conduits through which different software applications communicate with one another. They enable a set of rules and protocols that allow one application to access the functions or data of another, promoting interoperability and efficiency. In the landscape of cloud-based access control, APIs are pivotal for integrating various security and administrative systems, ensuring seamless operation and management.

RESTful APIs, a specific type of API, employ the Representational State Transfer (REST) architectural style, leveraging standard HTTP methods to facilitate communication between systems. This approach makes RESTful APIs remarkably efficient and flexible, enabling them to support a wide range of applications and services. They are designed to be stateless, meaning each request from a client to a server must contain all the information needed to understand and complete the request, which inherently enhances security and performance. The use of standard HTTP ensures RESTful APIs are universally understood, further promoting ease of integration and scalability in cloud-based access control systems.

RESTful APIs offer these key benefits:

1. Flexibility and Interoperability

Being rooted in web standards, RESTful APIs offer unparalleled flexibility and interoperability, enabling users to interact with access control resources effortlessly. This flexibility fosters a harmonious integration with diverse systems and applications, amplifying the adaptability and extensibility of cloud-based access control solutions.

2. Simplified Integration

The adoption of RESTful APIs streamlines the integration of cloud-based access control systems with other technological infrastructures, simplifying the process of connecting and managing access resources across different platforms. This simplified integration enhances operational efficiency and promotes a cohesive access management ecosystem.

3. Enhanced Scalability

RESTful APIs facilitate enhanced scalability within cloud-based access control, empowering users to adapt their access management infrastructure in response to evolving demands. This agility ensures that access control systems can effectively accommodate varying user requirements and operational scenarios.

4. Improved User Experience

By leveraging RESTful APIs, users benefit from an improved experience characterized by streamlined interactions with access control resources. The user-centric design and functionality of RESTful APIs contribute to a more intuitive and responsive access management framework, enhancing user satisfaction and operational fluidity.

5. Rigorous Security Measures

RESTful APIs reinforce the security posture of cloud-based access control systems, facilitating the implementation of robust authentication and authorization protocols. By integrating stringent security measures, such as API key usage, RESTful APIs contribute to fortifying the protective layers safeguarding access control resources.

Improving Scalability and Boosting Performance

For access control systems in the cloud, scalability is a significant advantage. Scaling enables manual adjustments to system resources like bandwidth and storage to meet varying load requirements without sacrificing speed or availability, providing the flexibility to expand or shrink resources as per demand. Performance optimization is equally paramount, ensuring access control systems run smoothly under varied load conditions, always maintaining high reliability and minimal latency.

By utilizing the cloud, businesses can easily scale their access control systems up or down to meet changing needs. This eliminates the need for costly hardware investments and minimizes downtime during system upgrades or expansions. Additionally, cloud based access control systems can leverage advanced data processing technologies, such as machine learning and artificial intelligence, to improve performance and enhance security measures.

Enhancing Cloud-Based Access Control Systems with Auto Scaling

Auto scaling goes beyond traditional scaling, using algorithms to analyze demand and adjust resources in real-time. Whereas scaling requires manual adjustments, auto scaling increases efficiency by reducing human involvement. It ensures the system remains responsive and cost-effective by dynamically allocating resources based on usage patterns. By implementing auto scaling, businesses can rest assured that their access control systems are not only equipped to handle unpredictable loads but are also optimized for cost, avoiding unnecessary expenditure on unused resources.

In cloud-based access control systems, auto scaling plays a pivotal role in ensuring seamless and efficient operations.

Here's why it's a fundamental component:

Performance Optimization

Auto scaling enables access control systems to dynamically adjust their capacity based on real-time demand. This means that as the number of users accessing the system fluctuates, the resources allocated to handle the load can automatically scale up or down. As a result, the system can maintain optimal performance levels during peak usage periods without incurring unnecessary expenses during off-peak times.

Enhanced Load Balancing

Auto scaling facilitates effective load balancing by distributing incoming access requests across multiple instances. This not only prevents any single component from becoming overwhelmed but also ensures that each request is efficiently handled, thereby optimizing the overall user experience. By dynamically adjusting resource allocation, the system can effectively manage varying traffic patterns and maintain a consistent level of responsiveness.



Redundancy: Building Resilience and Ensuring Reliability

The cloud, with its advantageous features, brings a vital element – redundancy. By distributing resources across multiple data centers, cloud-based access control systems promote a resilient environment that resists data loss or interruptions due to site-specific adversities. In the event of a disaster, recovery can occur swiftly and seamlessly from another data center. This ensures that your access control system remains available to protect your people and property, regardless of any unforeseen circumstances.

Implications for IT and Physical Security

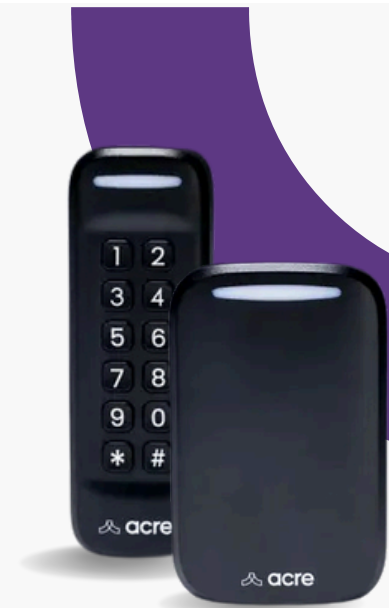
For IT professionals and physical security experts, the implications of cloud-based access control run deep. Not only do these systems promise a reduction in low-value IT tasks, but the forward-leaning security measures anticipate potential breaches, ensuring proactive prevention rather than reactive measurements. As organizations continue to rely on cloud-based technology for their access control needs, it is essential for IT and physical security teams to be well-versed in the latest advancements and best practices of this rapidly evolving field. Through continued education and training, these professionals can stay ahead of potential threats and protect their organizations' assets effectively.

The Acre Commitment: Delivering a Secure and User-Friendly Access Control Experience

Acre is reshaping security with the convenience of one innovative, flexible, and secure solution. **Widgets and custom dashboards** make your Access Control user experience simple, easy, and customizable to the way you want it. Deployed in the **cloud, on-prem,** or a **combination**, you can engage your best software experience from anywhere with your choice of Windows, macOS, iOS, Android, or any modern browser.

Our **RESTful API** enables users to deploy an extensive range of technologies through a straightforward process for easy integrations between Acre Access Control and a multitude of systems:

- Single card solutions for photo ID badge, access control, time and attendance, payment, and other systems
- Blue light emergency phones to enhance safety
- Wireless locks to secure common spaces
- Mobile credentials for a convenient and modern access control experience
- Biometric readers for high-security areas
- Video cameras throughout the facility
- Visitor management systems
- Intrusion and fire systems
- Active directory connection to streamline HR operations



In conjunction with our open API, users gain unrealized operational efficiency with the unique Acre **FITS** (Functional Integration Toolkit Scripts) **process automation** capabilities. FIT Scripts combine programming, integrations, and workflows to deliver maximum efficiency daily, and reporting for event, system, and process analysis.

Acre Access Control leverages **redundancy and auto scaling** to further enhance the resilience and reliability of our cloud-based Access Control solution. This strategy ensures that the access control system remains operational and available, even in the face of unforeseen failures or spikes in demand.

Our company is proud to be **ISO 27001** certified for our cloud-based access control and visitor management solutions, demonstrating our dedication to implementing robust Information Security Management Systems (ISMS) that meet the highest standards set by the International Organization for Standardization. This certification underscores our commitment to safeguarding data with utmost security and reliability.

Backed by 45 years as a physical security industry leader, Acre Security is a trusted name in safeguarding assets worldwide, known for our proficiency and our unwavering pledge to security excellence. Our state-of-the-art technology is scalable to worldwide enterprise levels and strikes the perfect balance between advanced security features and user-centric operability.



At Acre Security, our commitment to you is simple: We want to eliminate your risk.

We don't want you guessing if you're secure. We want you to know. And, we have the experience, expertise, and execution to do it, with 21% of our company resources focused on R&D. The technology we choose, driven by the end user experience we desire, impacts the software we develop, and adheres to our go-to-market strategy of being a disruptor. Reshape your security perspective, explore new possibilities for productivity, and find innovative ways to meet your strategic business goals by simply choosing Acre.





acresecurity.com