Accessia

SECURITY WHITEPAPER

Why more convenient also means more secure: key considerations for IT teams when choosing an access control platform

November 2024

CONTENTS

CLOUD VS ON-PREMISE

This whitepaper investigates the value of moving to a cloud-based access control platform, and explores the advantages of using a cloud-based system over an on-premise system, providing not only more convenience to IT teams, but also delivering an intrinsically more secure solution.

The whitepaper also looks at how to evaluate a cloud-based access control provider to ensure that they meet the expected standards for security and compliance in their processes, and that they provide the tools needed to allow the system to be deployed such that it gives administrators the required control and oversight of its operation.

On-premise solutions

A traditional on-premise access control solution is installed by an IT team standing up one or more servers on which the access control vendor's software will be run within the organization's data center, or all too commonly, underneath a reception desk. The door controllers connect to this server over the local area network.

The hardware required might be a bare metal server, or a virtual server, typically running a variant of Windows Server. To provide sufficient resilience to ensure that no events are lost, redundant disks or even machines might be required. On top of this hardware, the IT team will be required to license, install, and maintain an operating system. The access control solution may not be entirely self-contained and might need to be provided with other infrastructure, such as user directories or SQL servers, all of which must be paid for and installed by the IT team.

All this software must then be monitored, maintained, patched and updated by the IT team. Each of the independent components needs to be updated separately, and the IT team is responsible for dealing with any incompatibilities between different versions. Unless every component is kept up to date, the system will be running with known security vulnerabilities.

Depending on the vendor, access to the system to view event logs, or to make changes to the access control rules, could be provided in one of two ways. One option is for the server to provide a web interface, which can be accessed by users on the same network only if they know the correct address to browse to. The other option would be through a desktop application running on the server, which users must operate either on the server itself, or through a remote desktop connection. To minimize the security risks of this second approach, a complex system of user accounts with different permission levels must be set up on the server to ensure that users can only access the intended application and not be able to make changes to the underlying operation of the access control system.

If remote monitoring or configuration of the access control system by an off-site team is required, holes in the firewall need to be opened through from the internet. This exposes any unpatched vulnerability in the security system to malicious agents on the internet. Careful control and configuration of firewall access rules can mitigate this, at the expense of convenience and the IT team's time.

If the door controllers and the central server are on different networks, holes will need to be opened in the firewalls between these networks to allow traffic so that the controllers and server can talk to each other. The same applies for enabling administrative access for users. Sensible and secure network designs will often place end users' computers on a separate network to that of the building security system, needing to open holes between the networks undermines this effort.

On-premise access control systems are typically standalone because of the challenges of integrating them with third-party systems, regardless of whether those systems are on-premise or cloud-based. The detachment between, for example, a corporate directory and the access control system means that all changes made in the directory must also be manually applied to the access control system, taking time from the IT team, and leaving a margin for human error. In the worst case, even after an employee has left the organization, they may still have active credentials allowing them access to the building.

To scale an on-premise system across multiple buildings or multiple sites usually requires replication of the system onto each site, with the same costs in terms of time and money for each replica. Software updates for each are independent, as are changes to the configuration to add users. With every additional system, the amount of work for the IT team scales linearly, and so too does the chance of making a mistake.

Cloud solutions

To deploy a cloud access control system, the only requirement is for the on-premise devices to be connected to a network providing them with access to the cloud service. The Accessia AI Security Hub connects out to the cloud using only secure HTTPS connections and does not need to accept any incoming connections.

No part of an Accessia access control system needs to be provided, maintained, updated, or monitored by the customer. The cloud service is continually updated with security patches as soon as vulnerabilities are found and fixed, managed by both Accessia and Amazon Web Services (AWS). Even the AI Security Hub receives automatic updates, pushed down automatically from the cloud, and applied within seconds at a time convenient to the customer to ensure no impact on their building access.

To monitor or configure the system, Accessia provides a web-based cloud portal, available from anywhere with internet access, as well as convenient mobile applications for iOS and Android. Because all communication to the access control system is via the cloud, there is no need for any network configuration to allow external access into the internal network. A remote team can monitor events within the system and make any needed configuration changes as though they were on the premise, with any modifications taking effect within seconds.

Accessia provides native integrations with cloud-based corporate directories, where every relevant change within the directory such as additions or deletions of users or groups is synchronized to Accessia in under a minute, with no manual input or duplication required. This reduces the amount of time spent administering users and groups and ensures that access permissions are always up to date, reducing the security risk of still-active leavers.

A cloud system grows naturally and effortlessly to handle multiple sites. Because each site receives configuration and reports back to a single cloud, all maintenance and monitoring can be performed in one place, with one set of users, and one single log. Accessia provides site-level filtering and controls so that the same user can have different permissions across different sites, and so that an observer can focus only on the relevant sites at any time.

Cloud access control can often provide the type of data and physical security that would otherwise be out of reach for some organizations. Many cloud vendors, such as Accessia, have their own internal security teams, tasked with monitoring for vulnerabilities, taking pre-emptive action against emerging threats, and maintaining best practice and compliance.

Summary

	On-premise	Cloud
Infrastructure requirements	Physical or virtual servers, operating system, databases, user directory, SQL server	Internet connection
Updates	Responsibility of the IT team to update every component individually in a timely fashion	Updates automatically
Access to the system	Internal web server or remote desktop connection to the access control server	Cloud web portal
Remote access	Requires firewall rules or VPN to allow external access into the network	Available from anywhere
Directory synchronization	Typically manual process	Native integration with cloud directories
Scalability	Grows in complexity and redundancy as number of sites increases	Equally simple for 10 users as for 10,000
Security practices	Best effort as time allows	Dedicated internal security teams

CHOOSING A RELIABLE ACCESS CONTROL PROVIDER

While cloud-based access control has been shown to be simpler and more secure, the security and reliability of the system is only as good as the provider of the service. How can an organization know that a particular access control vendor can be trusted?

The gold standard to show trustworthiness is external certification against recognized information security standards and regulations. These standards audit vendor processes of both software development and operations, and customer data handling, to ensure that the system has been developed and runs in such a way to keep customers and their data from attack.

Certifications & compliance

SOC 2

Accessia has been successfully audited for SOC 2 compliance, reinforcing a commitment to the secure handling of customer data. It is intended that Accessia will recertify annually.

ISO 27001

Accessia has achieved ISO 27001 certification, so customers can trust Accessia services, processes, and products to keep information protected.

NDAA

Accessia is compliant with The National Defense Authorization Act (NDAA) a US federal law that aims to protect cybersecurity and security.

Organizational processes

The certification shows that the access control provider has been verified by an external auditor to follow best practices. A trustworthy organization will be open about their internal processes to demonstrate their commitment to keeping their customers safe.

Accessia goes above and beyond to keep people and places safe and secure. From development processes to data protection, products to privacy policies, everything Accessia does has security, protection, and best practice built in.

Secure software development

The security of any access control system is only as good as its design and implementation.

Accessia prioritizes security throughout the development process. Every new feature is threat modelled as part of the development of the specification, to ensure that no new attack surfaces are exposed. All code changes are reviewed internally to minimize the chance of any accidental or malicious vulnerabilities entering the code. A thorough suite of automated testing is run on every change to ensure correct functionality, and further manual testing is performed before any code is released to customers. Any security issues found within this process are fixed before release.

External testing

While effective internal processes are necessary to build secure software, they should not be the only level of testing.

Accessia invests in thorough external testing and verification, including vulnerability tracking, and third-party penetration testing by an accredited company.

Software Bill of Materials

Modern software development relies on an enormous infrastructure of open source software from multiple sources, all of which have their own systems of vulnerability tracking and release. A security vulnerability in any of these software packages could compromise the security of the access control system.

Accessia maintains an SBOM, a dynamic inventory that specifies all the dependencies upon which Accessia software is built. This means that in the event of a vulnerability being disclosed in any part of that software supply chain, it can be quickly identified and steps taken to mitigate risk.

Training and development

Hackers and other malicious actors are continually evolving their techniques, whether technical or social attacks.

All Accessia employees undergo compulsory security training monthly and Accessia conducts regular phishing simulations to educate employees and increase security awareness.

Data privacy

Threats to customer security and privacy can come from not just within the company or external attackers but have also been seen from employees of other access control vendors.

Accessia only ever accesses an organization's data with the customer's consent for troubleshooting or support purposes and access rules for Accessia employees are tightly controlled. Any access to the cloud services, whether an attempt to view data or to make a modification to the functioning of the service, by any member of the Accessia team, is automatically logged and shared with the rest of the team. This ensures that there is effective protection against internal actors, where no one can access customer data or make a change which could compromise customer security without this action being both visible and able to be countered quickly.

Accessia does not collect any customer data other than that strictly necessary for the correct operation of Accessia products and services. Additionally, Accessia does not share data with third parties unless correct operation requires it.

Architecture & infrastructure

A cloud-based access control system takes the burden for providing infrastructure away from the IT team and takes the responsibility for creating and managing this infrastructure into the provider. It is therefore essential that this infrastructure is designed to be resilient, scalable, and secure to prevent any loss of access to the customer.

Choice of platform

Accessia is built on AWS. AWS architecture is not only infinitely scalable to be able to cope with ever-increasing demand, but also fully redundant, even at a single region level with production data stored across three physically separate and independent Availability Zones. Most of the world's largest organizations use this model to deliver their services and, with so much being reliant on this architecture, it is constantly monitored and tested to ensure availability and reliability, making it reassuringly robust and resilient with an excellent uptime record. Further, AWS has outstanding security practices and an exceptional information security reputation with SOC 2 Type 2 and ISO 27001 certification and compliance, among others.

Accessia uses AWS' purpose-built tools to ensure that no AWS components can access each other unless they need to. This keeps network traffic segmented and reduces the risk of unauthorized access by only allowing specific components or users to access certain resources.

The data centers from which Accessia cloud services are hosted feature sophisticated security measures such as their own biometric access controls and advanced video surveillance, as well as security patrols and limited human access. Security at this scale is not financially viable for many organizations to implement themselves, so choosing a cloud access control provider allows an organization to benefit from additional layers of security without the associated outlay.

Data protection

Keeping the system secure relies on keeping out bad actors, who might try to impersonate a cloud service or an on-premise device to send dangerous configuration or inject misleading events. Additionally, access control event data itself can be considered a security and privacy concern, as it reveals sensitive information about the operation of an organization.

There are two sides to effective data protection: encrypting the data, to prevent it being read by anyone other than the intended audience; and authentication of both ends of any connection to ensure that only real users or genuine components of the access control system are given the keys required to decrypt the data.

Encryption

All data in the Accessia cloud is stored encrypted at rest, using AWS' standard methods of data protection so that even if the data is stored within a data center shared with other AWS customers, the data is available only to the Accessia service. Furthermore, each customer's sensitive data is then further encrypted with a key specific to that customer.

When sent outside the data center, all data is protected using industry standard TLS encryption, with the latest ciphers and signing algorithms used to ensure maximum security.

Authentication

To ensure that an Accessia AI Security Hub connects to the Accessia cloud, and that the cloud accepts connections from only genuine Accessia AI Security Hubs, the two ends authenticate each other using mutual TLS authentication. The certificate on the AI Security Hub is issued with the serial number of that Hub, and signed by the Accessia root certificate, and this is the only means by which the identity of the Hub is ascertained. A mapping from serial numbers to customer organizations is kept within the cloud, to ensure that only the organization which owns that controller is able to push configuration or receive events.

To further prevent an attacker extracting the private key from the AI Security Hub, the key is stored within a secure element on the Hub, and so cannot be taken and used on an alternative device. Secure Boot is implemented on the AI Security Hub to prevent an attacker loading unauthorized software onto the Hub.

Resilience

In the case of a physical security breach, having reliable logging of access events leading up to that breach is essential to trace and understand what happened. A lost event can mean the difference between catching the perpetrator and allowing them to go undetected.

Accessia takes the reliability of logging very seriously. Any event from the AI Security Hub is cached on the Hub until it has been confirmed to have been ingested and stored by the cloud, so that even in the case of full or partial cloud outages, nothing will be lost. Queues with retry mechanisms are used before event processing so that even under high load with large numbers of events arriving, nothing will be lost.

All event data is stored in a data store which is replicated across multiple shards, ensuring that even if one shard is lost, the data can be recovered from the remaining shards. Additionally, regular backups are taken so that in the unlikely event of complete database loss, customer data can be recovered from the backup.

Data jurisdiction

It is usually desirable to keep customer data local to where it was generated. This is both for regulatory purposes, where data is legally required to be stored in the same jurisdiction, and for performance reasons, so that time critical data is not routed halfway across a continent.

By taking advantage of different AWS data centers across the world, Accessia can offer organizations the ability to store their data in a data center geographically close, satisfying all legal requirements, and providing the best possible performance.

Availability

A concern with cloud services is that correct function is dependent on the cloud being available and that there is a risk of being locked out, or of doors being unlocked, if connectivity is lost.

If an organization suffers a network outage, the AI Security Hub will continue operating as usual and all door settings and user permissions will remain as per their schedule. To enable this, the Hub stores its settings and schedule for at least the next year. During the outage, event logs are stored locally until the network is restored and are then sent to the cloud as normal.

HELPING ORGANIZATIONS KEEP THEMSELVES SECURE

To keep an organization's people and property safe and secure, the access control system needs to not only be built in a secure and reliable way, but must also provide the administrative tools needed to manage access controls for users and to give insight into any changes made by those users. The system should have been designed from the ground up with these controls built in.

Multi-level admins

Accessia offers six levels of user accounts with varying permissions from Primary admin across all sites to Default user with limited permissions. Each new user added to Accessia has the lowest level of permissions by default.

Multi-site / Multi-geography

Accessia allows for users to be granted different levels of permissions on different sites within the same organization. For example, a receptionist in one office can administer their own workplace but not another. Further, each site created in Accessia is entirely independent from other sites, so changing access schedules or permissions for one site will not affect another site. Primary admins can retain control over all sites within an Accessia deployment.

Secure by default

Accessia uses the highest security settings as default at setup, ensuring security from day one and saving time. This includes new users having the lowest level of access permissions by default and new doors being automatically set to locked for all users until an access schedule is added.

Single sign-on (SSO)

Accessia supports integration with identity providers such as Entra ID SAML SSO for simpler sign-on and fewer credentials to manage. This also ensures that employees with Accessia admin permissions cannot access the management portal if they are removed from an organization's corporate directory, removing the likelihood of incorrect permissions or still-active leavers.

Audit logs

Each administrator action including changes, additions, and deletions is logged and visible in Accessia audit logs. These logs are immutable. Organization administrators can receive notifications for any changes made to Accessia systems and set-up, including user permissions and access schedules.

Direct support

Accessia offers 24/7 direct support to customers with expert help only a phone call away and no third-party triage.

About Accessia

Ultra secure, next generation access, experience, and analytics technology that's simple to use, easy to manage, and delivers unparalleled intelligence into how workplaces are used

Find out more at **accessia.com**

For further information about security at Accessia, visit our **security center** or email our security team: security@accessia.com

www.accessia.com

hello@accessia.com

company/accessiatech