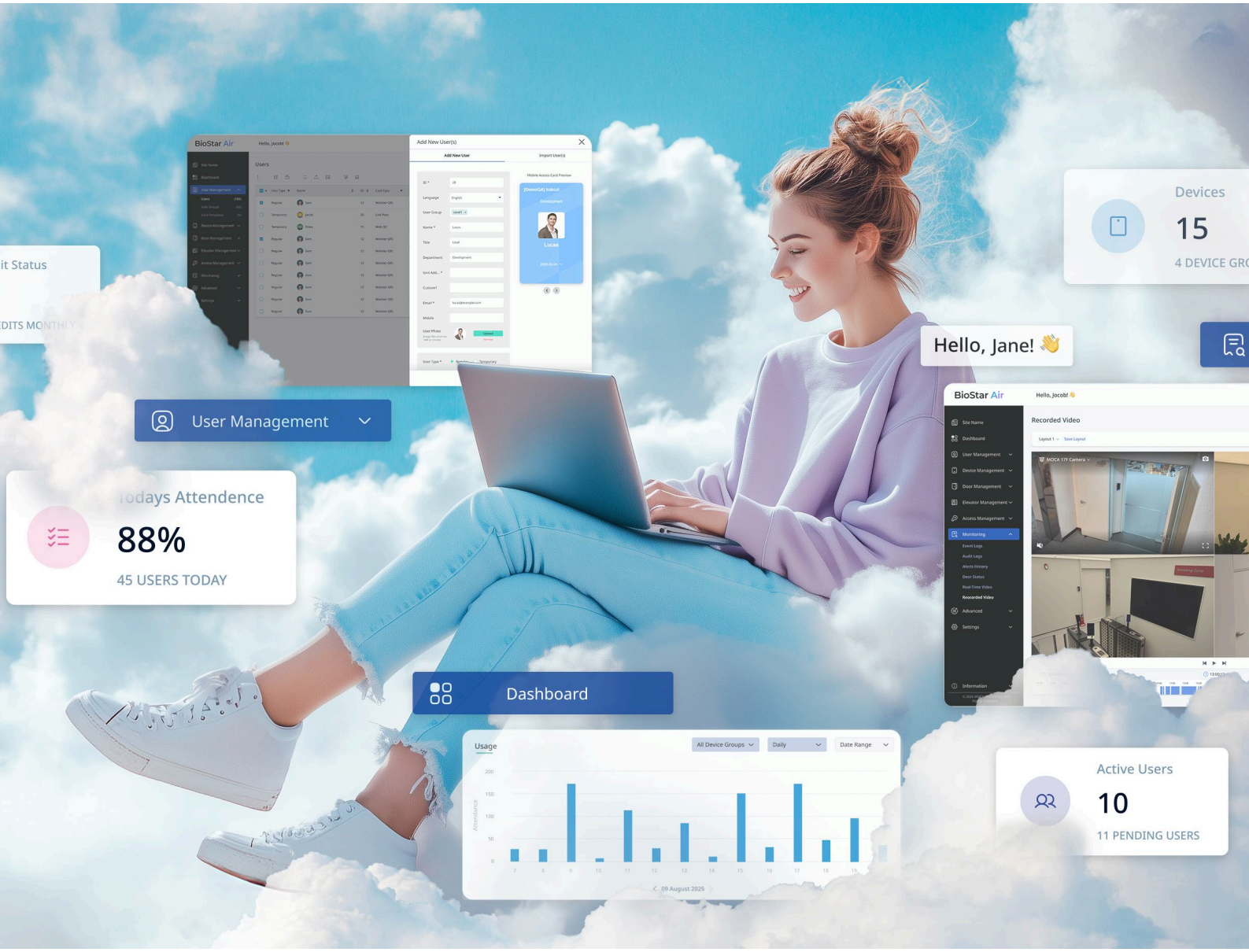
WHITEPAPER

Cloud access control:

And how to get it right.



suprema
SECURITY & BIOMETRICS

EDITORIAL

If you've ever built or scaled a business, you know that success comes down to a few fundamentals. You need to understand your customer better than anyone else. You need to solve real problems, not just ship features. And from focusing, ruthlessly, on what sets you apart.

At Suprema, we follow the same principle. What sets us apart is clear: we understand credentials, and how people actually use them across roles, locations, and devices.

Today, access isn't about choosing one credential. It's about offering the right credential for the right person, in the right place. One user might unlock the front door with their phone, access the server room with their face, and use a PIN to get into a supply closet.

That kind of multi-credentials flexibility, especially when it includes fast, reliable biometrics, makes a real difference in everyday environments. Not just in government buildings or airports, but in places like coworking spaces, gyms, schools, and franchise locations. Places where people expect things to just work.

That's why we launched BioStar Air: the first truly cloud-native biometric access control platform, built for multi-branch management.

We didn't set out to build the most general cloud access platform. We built one with a purpose: to extend our industry-leading biometric technology to the cloud, without compromise. A platform that makes access control, without giving up what professionals need. One that addresses the real pain points our partners, clients, and installers face every day.

This eBook is about helping you see through the noise. It's a guide for what to look for when choosing a cloud access control platform: what matters, what doesn't, and what to expect if you want to grow with confidence.

Because in the end, this isn't about cloud vs. on-prem.

It's about building something that actually works, for the people who use it.

Thanks for reading. And thanks for building the future of access with us.

Hanchul KIM,
CEO of Suprema Inc.

Summary

Introduction

Why this eBook matters, now more than ever.

Access control has always been a cornerstone of physical security. But now, it’s also a lever for **business agility**, operational efficiency, and user experience. From multi-location franchises to coworking spaces, from growing startups to cloud-first organizations, the way we manage entry and identity is evolving fast.

And yet, confusion still dominates the market. Everyone claims to offer “cloud access control,” but the reality behind those claims varies wildly. Some platforms offer a veneer of cloud while hiding legacy infrastructure behind the scenes. Others lack the flexibility, scalability, or biometric capabilities needed to support modern business needs.

This eBook was written to help you cut through the noise. Whether you're upgrading a legacy system or launching a new site, you'll learn:

- What true cloud-native access control looks like
- Why biometrics are the ultimate test of architecture
- What features really matter for your business
- How to future-proof your access control investment

By the end, you won’t just know how to choose a cloud platform, you’ll know **how to choose the right one for you.**

1. Getting started: What is access control today?

Rethinking the door: From physical security to operational agility.

Access control has always been about determining who can go where, when, and how. But now, that definition is expanding. The systems that used to simply open doors now sit at the **intersection of physical security, digital infrastructure, and workplace operations.**

As organizations become more distributed, and user expectations shift toward seamless, app-like experiences, access control is no longer just about keeping doors locked, it's about enabling agility, efficiency, and scale.

From keys to credentials.

For decades, access control systems revolved around mechanical keys, then PIN codes, and eventually RFID cards and fobs. But today, we've moved far beyond that. Modern access systems now support a wide range of digital credentials, including:

- Biometric recognition (facial and fingerprint).
- Mobile credentials on smartphones.
- App-less options like QR codes and web links.
- Smartwatch access through Digital wallet (Apple, Android...).
- Traditional methods like PINs and RFID cards, for backward compatibility.

These options reflect a broader evolution: access control is no longer just hardware, it's a **digital identity** layer that spans locations, devices, and use cases.

From site-centric to user-centric.

Historically, access control was built around physical sites. Users had to be enrolled at a specific location, and credentials were often tied to a particular reader or controller. Any changes—adding a new user, updating credentials, revoking access—required manual, often on-site configuration. That model no longer works.

Today's organizations operate across multiple sites, time zones, and user types. The access control platform must be **as flexible and mobile as the people who use it**.

With modern cloud systems, the paradigm shifts from site-centric to user-centric. Now:

- One user can carry a single credential across many sites
- A single identity can include multiple credentials (face, mobile, PIN, card)
- Access rights can be assigned or revoked remotely, from anywhere
- Credentials sync across readers in real time, without manual setup

This shift reduces administrative overhead and provides a vastly better experience for both end users and system managers.

Access control is no longer just about security.

Yes, access control still plays a critical role in physical security, but that's only part of its value.

Today, a modern access control system should also:

- Enable fast, automated onboarding and offboarding of users.
- Reduce reliance on on-site IT teams or front desk staff.
- Provide real-time visibility and control across distributed locations.
- Support privacy and compliance standards like ISO 27001 and GDPR.
- Deliver a smooth user experience: app-less mobile credential support, no complicated setup,...

But perhaps most importantly, access control has become a **core component of business operations**, especially in environments where space is rented, shared, or managed flexibly.

In coworking spaces, multi-tenant buildings, and franchise models, access control is now **baked into the business model** itself. It allows space managers to:

- Enroll new users remotely and automatically upon payment, before they even arrive.
- Grant access only for the duration of a membership or booking.
- Tie digital credentials to shared amenities like meeting rooms or printers.
- Troubleshoot access issues remotely, without stepping on site.
- Operate spaces around the world through a single cloud interface.

Access control is no longer just about unlocking doors, it's about **unlocking revenue**, efficiency, and experience.

It has evolved into a platform that supports automated service delivery, seamless customer journeys, and scalable operations, especially for space-centric businesses looking to do more with less.

But not every system has evolved.

Despite the clear shift in needs, many access control solutions on the market still follow outdated models. They may offer cloud dashboards but rely on local servers or door controllers behind the scenes. They may support mobile credentials or biometrics, but require clunky user experience and complex provisioning.

Some were built to manage buildings. Today's leaders need **systems that manage users**: securely, simply, and at scale.

This eBook was created to help you understand that shift and cut through the confusion. Yes, cloud access control is everywhere, but not all cloud systems are created equal. And before we dive into comparing modern cloud platforms, it's worth asking a more foundational question:

Why change anything at all? Why not just stick with what already works?

That's where we begin.

2. Why not just stick with on-prem access control?

It’s a fair question. On-premise access control has been the industry standard for decades. It offers total infrastructure control, offline reliability, and deep customization.

So why change? The truth is, on-prem systems still do some things very well. But as **organizations become more distributed** and user expectations shift, those same systems start to show their age. What used to be strengths, like full local control, can turn into operational roadblocks.

Two approaches. One future.

In access control, the conversation often turns into a binary: **cloud vs. on-premise**. But it’s not that simple. Both approaches offer clear advantages, and specific limitations. The key is knowing which model fits your needs today, and which will still serve you tomorrow.

Let’s break it down.

On-premise access control: Integrated security for complex environments.

For years, on-premise access control systems have been the standard, especially in enterprise, industrial, and high-security environments. Everything is hosted locally: the server, the database, the credentials, and the door controllers. That tight coupling enables a level of control and system depth that cloud platforms are still catching up to.

On-premise solutions often support a broader range of features, integrating access control, alarm management, video surveillance, time and attendance, and visitor tracking into a **single, unified system**. They also offer direct, hardware-level integrations with third-party systems like fire panels or building automation, making them highly adaptable to complex security ecosystems. That architecture offers some real strengths:

- **Total control** over data, network, and infrastructure.
- **No dependency** on internet connectivity or cloud uptime.
- **Low-latency** communication between components.
- Robust **local failover** and redundancy options.
- **High compatibility** with third-party hardware and building systems through direct wiring.

But it also comes with significant tradeoffs:

- Requires **dedicated IT** and physical infrastructure.
- Scaling across sites increases **complexity and cost**.
- **Difficult to manage remotely** or adapt quickly.
- **Manual software updates** and hardware maintenance add overhead.
- Less compatible with modern cloud tools or API-based workflows.

In an age of remote work, flexible access, and mobile-first management, on-prem systems, while still powerful, can become operational bottlenecks.

Cloud access control: Agility without the infrastructure.

Cloud-based access control takes a different approach. Instead of local servers, configurations, credentials, and data live in the cloud, accessible from anywhere, **managed centrally through a web interface or mobile app**.

The advantages are immediate:

- **No on-site servers** and limited infrastructure required.
- Manage all locations from a **single dashboard**.
- Remote enrollment, access changes, and real-time monitoring, **from anywhere**.
- **Fast deployment**: ideal for growing or distributed operations.
- **Continuous software updates** and built-in security patches.
- **Easier integration** with other cloud-based solutions.

These benefits make cloud access control especially appealing for organizations looking to reduce IT overhead, improve operational agility, and support flexible work models.

But cloud also comes with tradeoffs to consider:

- **Internet dependency**: Access control relies on a stable network connection. Local fallback, call it an offline mode, is essential in case of outages.
- **Less hardware customization**: Some cloud platforms standardize hardware interactions, limiting deep customization.
- **Recurring subscription costs**: OPEX-friendly , but long-term subscription models may exceed one-time CAPEX options.
- **Vendor lock-in**: With platform-centric ecosystems, switching providers can be complex once deployed at scale.
- **Data residency & compliance**: Depending on your region, storing access logs and biometric data in the cloud may require additional due diligence.

Cloud is not a silver bullet, but when built well, it can streamline operations, simplify deployments, and scale effortlessly across locations.

Quick comparison: Cloud vs. on-premise access control.

Key aspects	Cloud access control	On-prem access control
Deployment	No on-site servers. Quick setup.	Local servers. Full infrastructure control.
Reader connectivity	Cloud to device via internet.	Local controllers and LAN infrastructure.
Platform access	Manage from anywhere, desktop or mobile.	Requires local network or VPN.
Scalability	Multiple locations with minimal IT resources.	Large single-site, high-security environments.
Security	Built-in. Provider security dependent.	Full control. Internal maintenance reliant.
Customization	Standardized experience. Automatic updates.	Highly customizable. Manual updates.
Total cost of ownership	Ongoing subscription fees. Best for OPEX.	Higher upfront cost. Best for CAPEX.

3. Not all cloud access control is created equal.

Cloud access control can mean a lot of different things, and not all of them deliver the same convenience. Some platforms keep the old infrastructure and simply add a web dashboard. Others go further, hosting user data and access rules in the cloud but still relying on legacy hardware. And a select few are purpose-built for the cloud era, designed from the ground up for agility, scalability, and simplicity.

Understanding the types of cloud access control systems.

To help you make informed decisions, let’s break down the three primary types of cloud access control systems commonly found in today’s market.

Level 1: Cloud-managed access control (on-prem in disguise).

This approach is essentially traditional access control with a cloud gateway tacked on.

- The system runs on a dedicated server emulating traditional on-premise software, just hosted off-site.
- Each site requires manual setup and configuration.
- Core authentication logic and data remain isolated per customer, limiting real-time sync and cloud-native agility.

This setup adds complexity, installation cost, and limits scalability and you’re still managing infrastructure across locations.

Level 2: Cloud-hosted access control (traditional ACaaS).

This model is commonly marketed as “Access Control as a Service” (ACaaS). It introduces cloud-based credential management and user access configuration.

- Readers connect to a cloud-hosted platform to verify user identities.
- However, local door controllers (ACUs) are often still required, these devices relay commands from the cloud to the doors.
- Adding a new door usually means buying and configuring another controller, introducing cost and complexity.

While it supports centralized management, the system still relies on partial local infrastructure, limiting the benefits of true cloud agility.

Level 3: Cloud-native access control (e.g., BioStar Air).

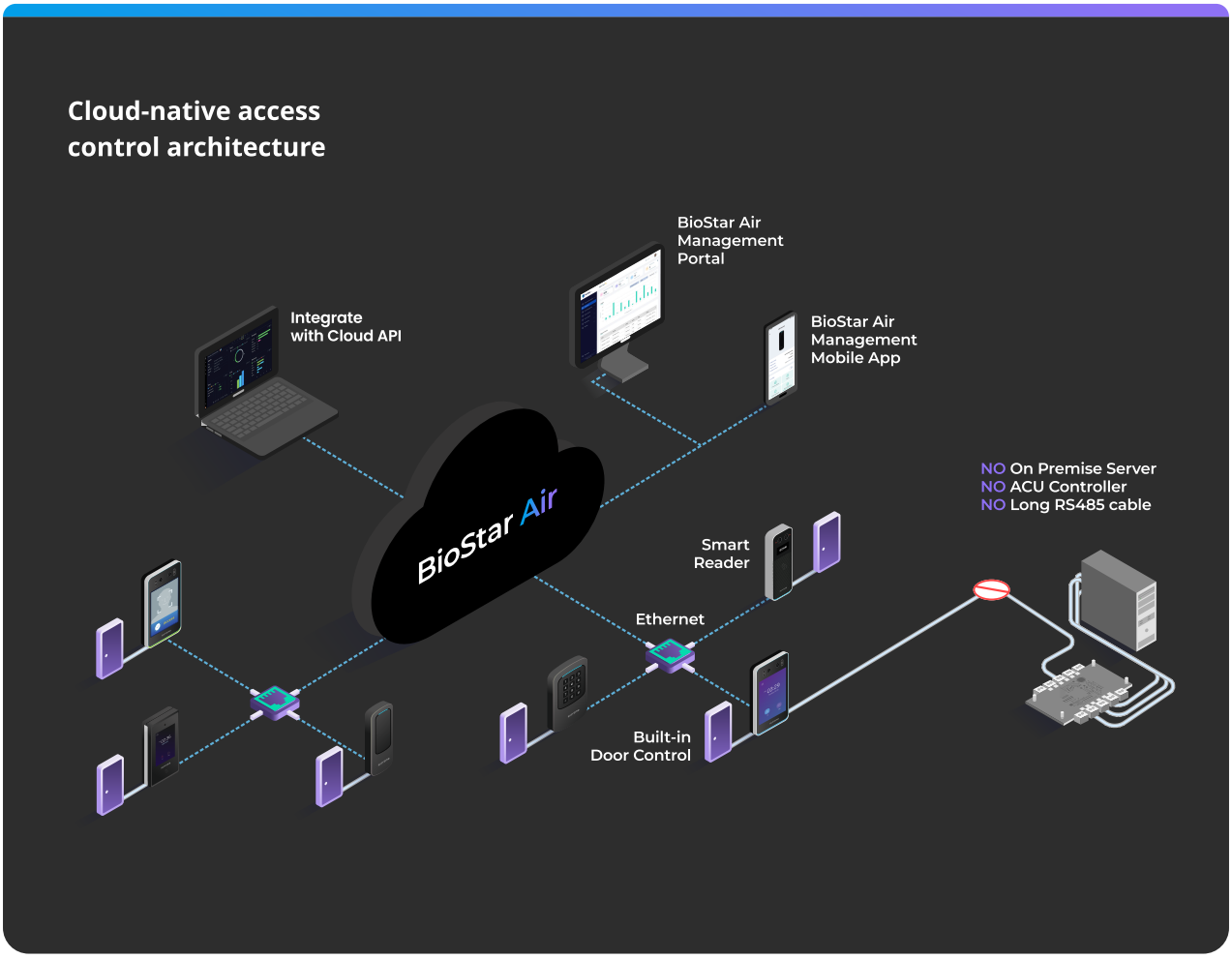
Cloud-native platforms aren’t retrofitted versions of old systems, they’re purpose-built for modern connectivity, multi-site scalability, and mobile-first operations. Instead of relying on local servers or intermediate controllers, these solutions leverage edge architecture and smart devices that operate independently, sync instantly, and scale effortlessly.

BioStar Air is a leading example of this new generation.

Unlike most cloud systems that require door controllers or third-party biometric workarounds, BioStar Air connects Suprema's smart readers directly to the cloud, via standard IP, without any local server or sync tool. Readers handle access logic independently and communicate with the cloud for real-time updates across all sites, regardless of network boundaries.

Here's how it works in practice:

- **No controllers**. No server closets. Just install a Suprema reader, connect it to the network, and you're online.
- **Smart edge readers** process access decisions locally, with built-in relays and processors.
- **Multi-site management** is seamless. One system governs access across offices, warehouses, retail locations, and remote facilities.
- Credential updates and logs sync instantly across locations, with no duplicated data or manual push/pull.



This architecture doesn't just simplify setup, it changes how you think about scale. Organizations can start small, deploy quickly, and expand later without rewiring systems or re-enrolling users.

Biometrics: The ultimate Litmus test.

Want to know if a cloud platform is truly ready for modern access control? Look at how it handles biometrics.

Most cloud platforms:

- Integrate third-party readers via APIs or middleware.
- Maintain separate databases for biometric data.
- Require multiple photos or long scans for face enrollment.
- Deliver inconsistent results with outdated matching algorithms.

BioStar Air:

- Native biometric support (face & fingerprint).
- Single-look facial enrollment.
- Remote enrollment with just one selfie from your phone.
- Real-time cloud propagation to all readers.
- AI-driven matching accuracy and anti-spoofing at the edge.

For **Erik Cornelius**, Head of Product for BioStar Air at Suprema, this is where most cloud platforms fail, not because they don't try, but because their foundations were never built for biometrics:

> *"Biometric enrollment speed is the ultimate litmus test. It's where architecture and user experience collide. If enrollment takes 30 seconds, requires multiple photos, or doesn't sync instantly across devices, you're not looking at a real cloud-native platform. With BioStar Air, enrollment and propagation across reader takes less than five seconds. This means the biometric profile is instantly available on every connected reader in the world the moment you step away. No extra software. No secondary enrollment. That's what we call a true "one-shot enrollment", and it's a night-and-day difference from what most vendors offer."*

The importance of a unified experience.

Access control should be simple, for both admins and users. But many "cloud" systems still rely on:

- Clunky desktop software or VPNs.
- Manual syncing of credentials.
- Separate portals for enrollment or reporting.

BioStar Air centralizes everything into one intuitive platform:

- Manage access, credentials, devices, and users from one web portal.
- Enroll and revoke users from a mobile app.
- Get real-time door status, video footage, and alerts anywhere.

Not all cloud platforms are created equal. True cloud-native access control delivers more than just remote access, it redefines how organizations secure, scale, and support their spaces.

4. Real use cases where cloud-native just wins.

A feature list can tell you what a platform does. A use case shows you what it changes.
For many businesses, access control isn't just about security, it's about operational efficiency, user experience, and scaling without complexity. BioStar Air's cloud-native architecture, controllerless setup, and remote-first approach unlock clear advantages in the real world.

Multi-site coworking & flexible offices.

Coworking spaces are dynamic by nature: users come and go, schedules change daily, and administrators need to control access **across multiple locations, often with lean teams.**

With BioStar Air, coworking operators can:

- Enroll members remotely before their first visit.
- Offer mobile credentials or app-less Link Passes.
- Remotely unlock doors to host office tours over FaceTime or video calls.
- Grant access to shared and private areas with flexible rules.
- Centrally manage multiple branches under a single interface.

> *"We live in Sydney, two hours away from the space, and we travel a lot. We needed an access control system that allowed us the luxury of not being on site and managing the space from anywhere in the world."*
> **Sergio DE CAIRES**, Owner, iCo Creative Maitland.

Residential buildings with shared amenities.

Managing access to residential units is straightforward. Managing access to gyms, pools, rooftops, clubhouses, and delivery rooms? Not so much, **especially when buildings are part of a larger property network.**

BioStar Air enables:

- Granular control over shared and private spaces.
- QR credentials for visitors without app installs.
- Auto-expiring credentials for service providers and delivery access.
- Partitioned tenant control in multi-dwelling units.

> *"It's not just about integrating keys with doors; it extends to ancillary services like laundry, cleaning, and more, simplifying the lives of both tenants and property owners."*
> **Anggit TUT PINILIH**, CEO, Mamikos.

Franchises with no on-site IT staff.

Franchise operators need consistency **across locations and minimal overhead**. Most don’t have IT personnel at each site, and traditional systems make it hard to scale without significant investment.

BioStar Air delivers:

- Pre-configured reader kits that plug directly into the cloud.
- Easy credential provisioning from HQ or mobile app.
- Remote monitoring of all branches in one view.
- Access control that doubles as an operational tool (e.g., T&A and shift schedules).

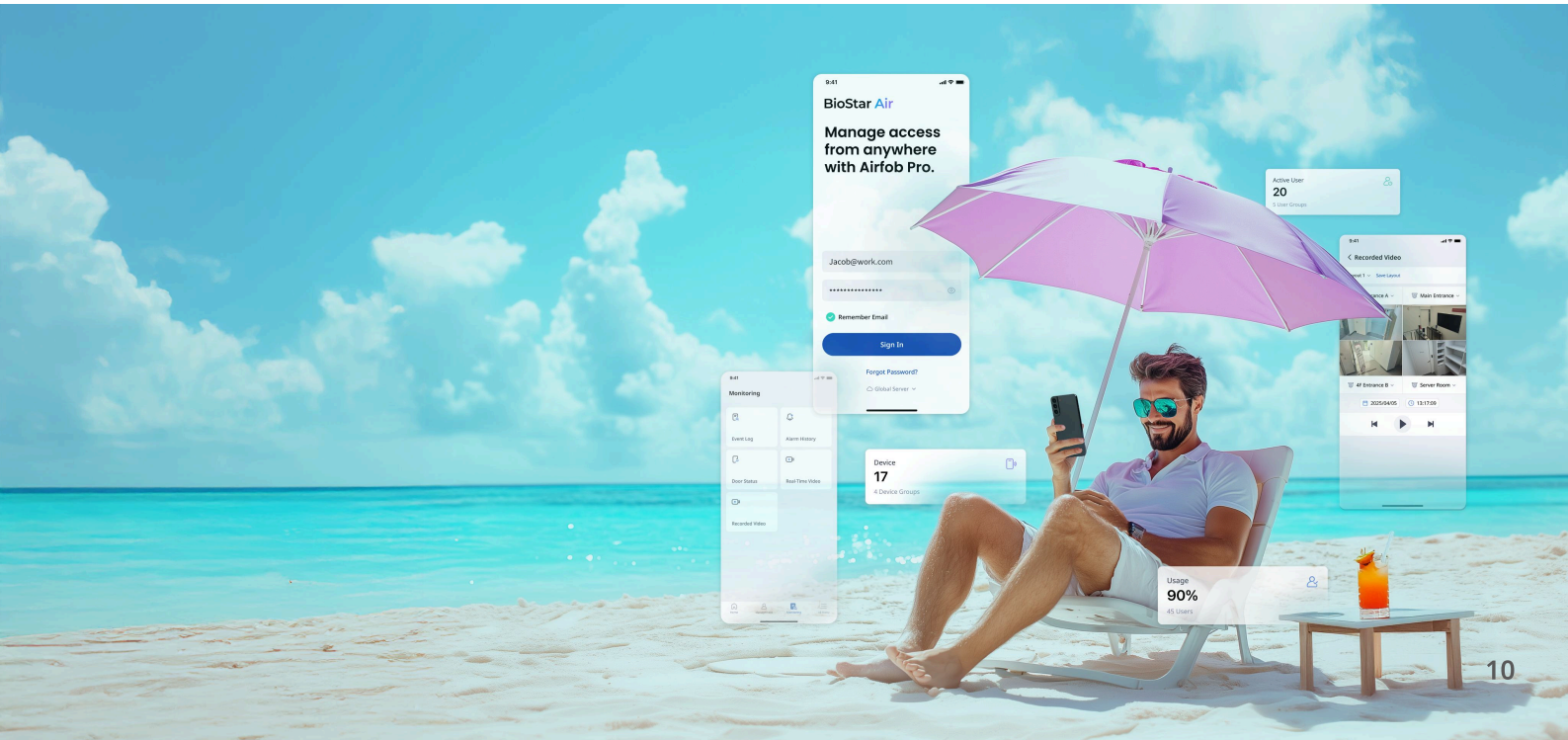
> *“BioStar Air has simplified member management and access control, reducing time and costs associated with physical access cards, improving the user experience and also enabling the launch of FIVESPOT, a members-only lounge for individuals. You can now use all FIVESPOT locations with a single membership.”*
> **Seunghyo KANG**, IT/INFRA Team, FASTFIVE

Retail chains needing remote oversight.

In retail, store managers need access to their branch, but head office needs visibility and control across the network. Managing access to staff-only areas, stock rooms, and storage **without a full server setup is key.**

With BioStar Air:

- Credentials can be assigned by corporate HR or regional managers.
- Access schedules align with store hours or delivery windows.
- Doors can be locked or unlocked remotely for late-night deliveries.
- Biometric and mobile onboarding can be done **from anywhere in the world**.



Schools & campuses with timed access needs.

Academic facilities operate on shifting schedules, **across buildings and roles**. From teachers and maintenance crews to students and temporary guests, flexibility is key.

BioStar Air allows education institutions to:

- Schedule access rights based on class hours or user roles.
- Use mobile credentials for students and biometric for staff.
- Track attendance and door activity from a central view.
- Assign QR or app-less access for temporary event guests.

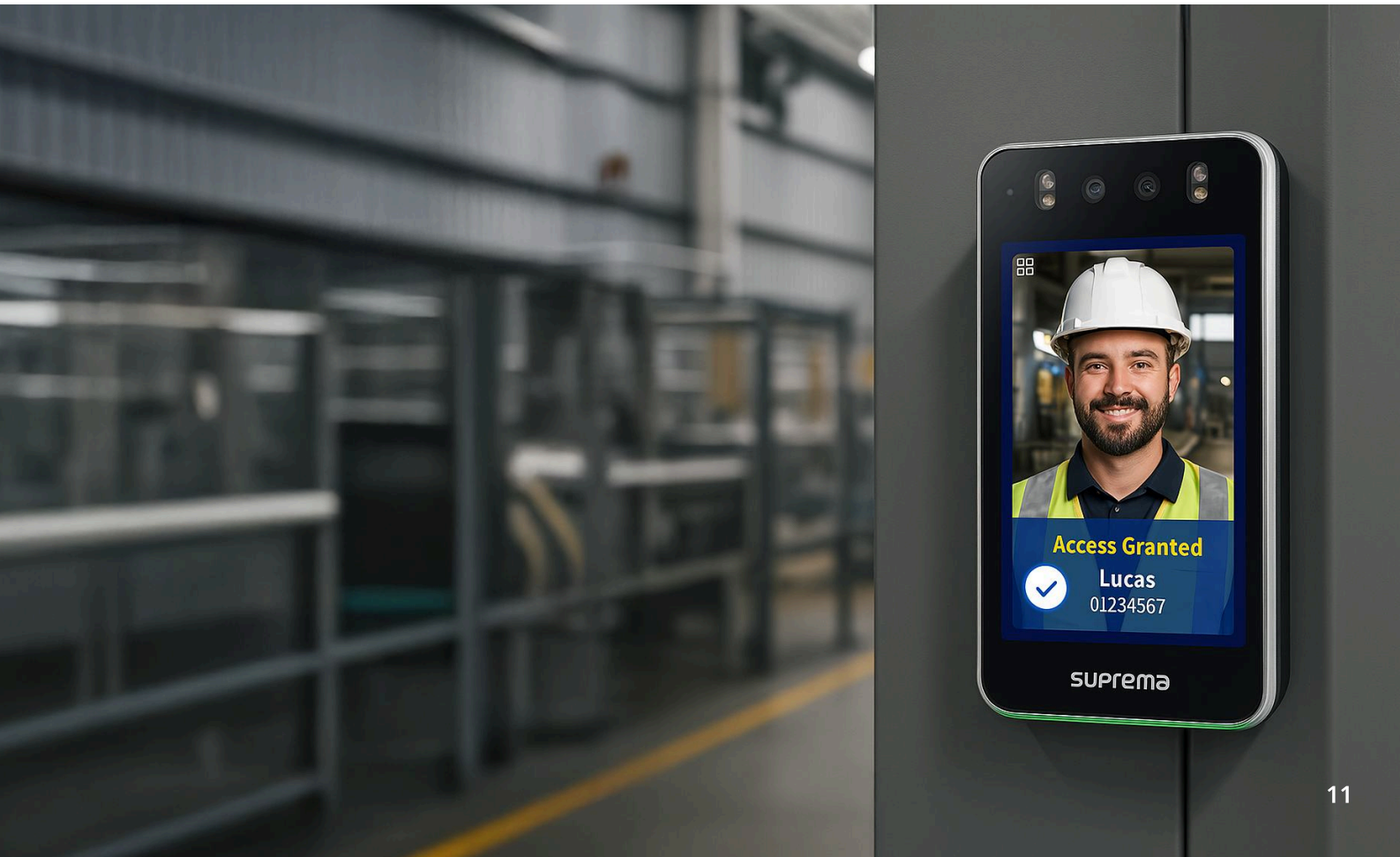
In summary, cloud-native access control solutions do not just work in theory, it’s designed for the day-to-day reality of modern businesses. Whether it’s automating onboarding, reducing IT overhead, or unlocking access remotely, BioStar Air wins where it matters most: in the field.

Industrial sites with harsh environments.

Dust, dirt, shocks, gloves, **these conditions break most systems.** Industrial environments need rugged access control that doesn’t rely on cards or keypads.

Suprema’s biometric readers offer:

- Face authentication that works even with coal dust or PPE.
- Offline fallback modes for remote areas.
- On-device AI for fast, accurate recognition in < 0.2 seconds.
- Cloud sync that doesn’t require local server rooms.
- Readers built to last, even outdoor (IK08 and IP67 standards).



5. Smarter monitoring with entry-centric design.

Traditional video systems are often built for broad surveillance, managed by separate teams, powered by complex software, and integrated with access control in ways that feel more like duct tape than synergy.

BioStar Air takes a different approach.

It doesn’t try to replace a full-fledged VMS, and it doesn’t need to. Instead, it focuses where it matters most: the door. By embedding smart, event-based video directly into the access control workflow, BioStar Air delivers just the right level of visibility, **without the complexity, cost, or infrastructure of a full CCTV system.**

With BioStar Air, video becomes a native part of your access control flow: simple, integrated, and responsive.

Real-time video + alerts where it matters most.

Traditional camera systems are built to monitor everything. But not every organization needs a full-blown surveillance grid.

- BioStar Air focuses on what matters most: **the door**.
- Receive instant alerts when unauthorized access is attempted.
- View a real-time video feed of the reader and entry point.
- Match access logs with live or recorded footage, directly within the platform

Whether you're managing a coworking space, a school, or a multi-branch operation, this door-level focus provides just the right amount of visibility, without overwhelming your system or your team.

No complex VMS or CCTV system required.

Unlike many platforms that require expensive cloud video subscriptions or proprietary VMS integration, BioStar Air is built for practical, plug-and-play visibility:

- Native ONVIF camera support (G or S profiles).
- Cameras connect through Suprema’s smart readers on the same network.
- No NVRs, local servers, or separate video licenses needed.
- No storage limitations, just access events and matching footage when you need it, directly from the camera’s SD card.

This is video designed for lean teams, remote admins, and smart buildings, not surveillance operators.

Event logs that tell the full story.

Seeing when a door was accessed isn’t always enough. You also want to know who entered, how, and what happened next.

With BioStar Air, you are not just logging events, you are tying them together.

- Access events (badge, face, PIN, etc.)
- Matching video clips
- Alerts triggered by exceptions (denied access, forced entry, etc.)
- A video timeline that reconstructs the sequence of actions at a glance

Instant visibility. Remote response.

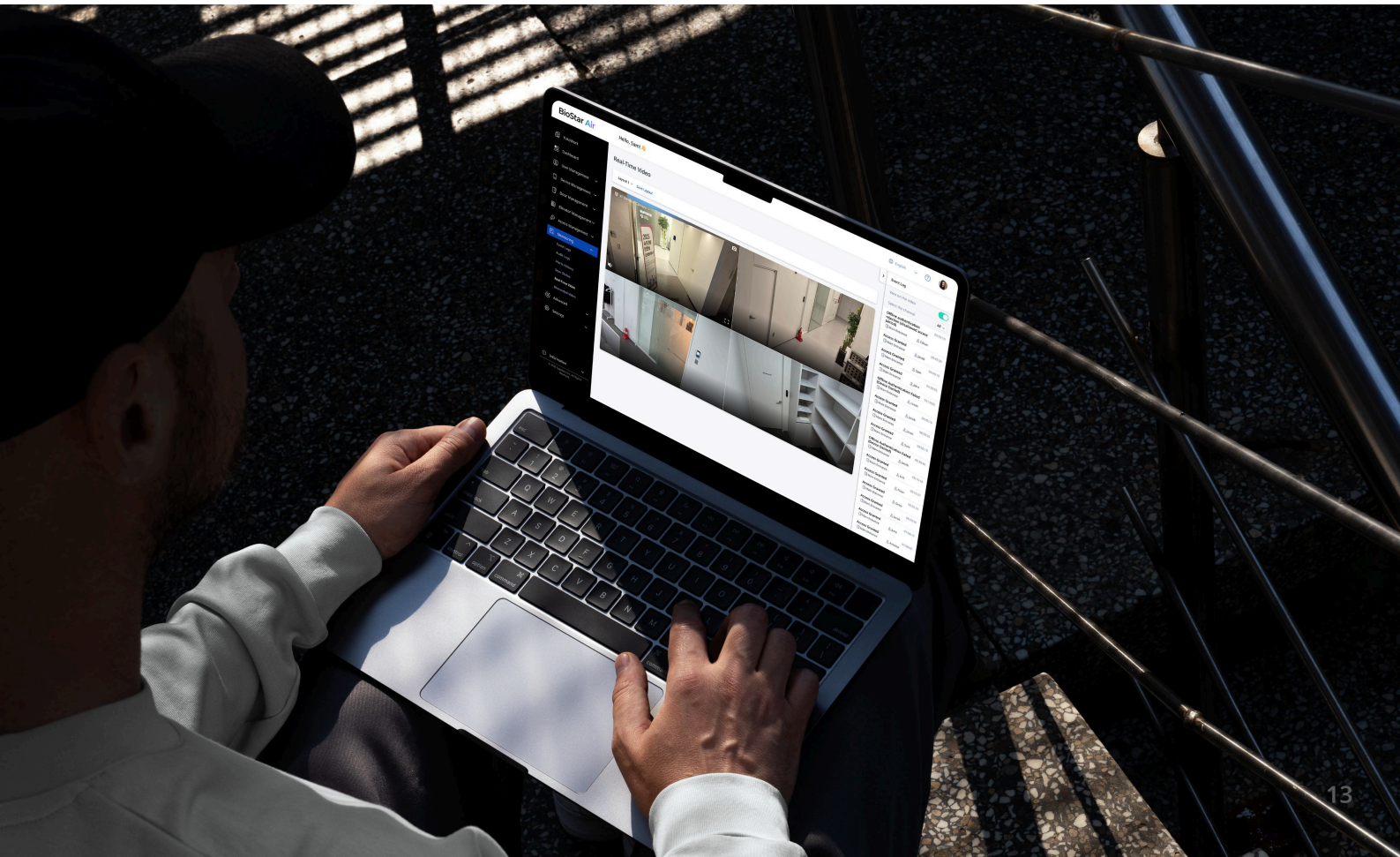
When something goes wrong, you shouldn’t have to call the front desk, or wait until morning to respond.

With BioStar Air, **security becomes proactive**, not reactive:

- Alerts appear in real time, in your mobile or desktop dashboard
- Video shows exactly what’s happening at the door
- You can remotely unlock or disable access from wherever you are

Security isn’t just about keeping people out, it’s about knowing what’s happening and being able to respond. With BioStar Air’s entry-centric monitoring, you gain video-enhanced awareness without the bulk of traditional surveillance systems.

It's smarter monitoring, built into your access control, not bolted next to it.



6. Cloud access control showdown: How leading platforms compare.

The market for cloud access control has matured significantly, with a wide range of solutions now available. While many providers offer cloud-based features, not all platforms are built the same—and the differences can have a big impact on deployment, usability, and scalability.

In the following pages, we'll compare some of the most common platforms across key areas like credential versatility, biometric integration, architecture, and video capabilities. Whether you're evaluating solutions for your business or helping clients make the right decision, this guide is designed to provide a clear, practical overview of what each approach can offer.

Multi-credential flexibility.

Explore how top cloud access control systems support modern credential types, from mobile and QR to biometrics and Apple Wallet. See which platforms truly offer flexibility.

Credentials	BioStar Air	Comp. A	Comp. G	Comp. K	Comp. B	Comp. AA	Comp. S	Comp. V	Comp. G
Mobile	Yes	Yes	*3rd party*	Yes	Yes	No	Yes	Yes	Yes
Apple Wallet	Yes	No	*3rd party*	Yes	Yes	No	No	Yes	No
Android Wallet	No	No	*3rd party*	No	Yes	No	No	No	No
QR Code/Pass	Yes	No	Yes	Yes	No	Yes	No	No	No
Web Link/Pass	Yes	Yes	No	Yes	No	No	No	No	No
Face	Yes	No	No	No	Yes	Yes	No	No	No
RFID cards	Yes	Yes	Yes	Yes	Yes	*3rd party*	Yes	Yes	Yes
PIN	Yes	Yes	Yes	No	Yes	*3rd party*	Yes	Yes	Yes
Finger	*Coming soon*	No	No	No	No	No	No	No	No

Note: For the sake of neutrality and clarity, the names of third-party vendors have been anonymized in this comparison.

When it comes to credential flexibility, BioStar Air clearly leads the field. It's the only platform that checks nearly every box, supporting everything from mobile and Apple Wallet to facial authentication, PIN, and app-less QR/Link Passes.

Some competitors also offer strong mobile and RFID support, and some support PIN or face credentials. However, they often lack newer, user-centric features like Apple Wallet integration, app-less credentials, or multi-credential setups that streamline access without app fatigue.

Verdict: BioStar Air stands out for its depth and flexibility, especially in mixed-use environments where different users require different ways to access a site.

Biometrics in the cloud.

Not all biometric access control is created equal. Compare platforms with native facial and fingerprint recognition.

Features	BioStar Air	Comp. A	Comp. G	Comp. K	Comp. B	Comp. AA	Comp. S	Comp. V	Comp. G
Face support	Yes	No	No	No	Yes	Yes	No	No	No
Finger support	*Coming soon*	No	No	No	No	No	No	No	No
Onsite enrollment	Yes	n/a	n/a	n/a	No	Yes	n/a	n/a	n/a
Onsite enrl. speed	2 sec.	n/a	n/a	n/a	n/a	~30 sec.	n/a	n/a	n/a
Automatic enrl.	No	n/a	n/a	n/a	No	Yes	n/a	n/a	n/a
Remote enrl.	Yes	n/a	n/a	n/a	Yes	No	n/a	n/a	n/a
Matching speed	0.2 sec.	n/a	n/a	n/a	~0.5 sec.	1 sec.	n/a	n/a	n/a
Edge architecture	Yes	No	No	No	No	No	Yes	No	No
Anti-spoofing	Yes	n/a	n/a	n/a	Yes	Yes	n/a	n/a	n/a

BioStar Air delivers the most complete biometric experience in the cloud. It supports face and soon fingerprint, with fast 2-second onsite enrollment, enabling instant onboarding with high accuracy. It also features liveness detection, anti-spoofing, and the ability to authenticate users wearing , Biostar Air also bolsters a controller-free architecture, no separate door controller needed. This makes deployment faster, simpler, and more scalable.

Competitor AA delivers strong facial recognition with edge AI and effective liveness detection. However, the enrollment process is slower—typically requiring a 30-second scan—and while automatic enrollment is a promising feature, it takes multiple entries to calibrate properly, making onboarding less consistent. The system also depends on third-party readers and controllers, which adds integration complexity.

Competitor B supports cloud-based face recognition but lacks flexibility. There's no onsite enrollment, and setup requires admin-uploaded photos. It also needs a door controller, limiting deployment flexibility.

Verdict: BioStar Air leads in cloud-native biometric performance, with the fastest enrollment, broad credential support, and a tightly integrated platform designed for real-world use. Competitor AA is strong on facial recognition but comes with more hardware complexity. Competitor B offers entry-level biometrics but falls short on key features that matter for usability at scale.

Video in the cloud.

Video is an essential part of modern access control, helping you verify access events, investigate incidents, and monitor sites remotely. But not every platform handles video the same way.

Features	BioStar Air	Comp. A	Comp. G	Comp. K	Comp. B	Comp. AA	Comp. S	Comp. V	Comp. G
Real-time video	Yes	Yes	Yes	No	Yes	Yes	No	Yes	Yes
Recorded video	Yes	Yes	Yes	No	Yes	No	No	Yes	No
Video logs	Yes	Yes	Yes	Yes	Yes	No	No	Yes	No
Video export	No	Yes	Yes	No	No	Yes	No	Yes	No
Video analysis	No	Yes	Yes	No	No	No	No	Yes	No
Video reports	No	Yes	Yes	No	No	No	No	Yes	No
Cloud storage	No	Yes	Yes	No	Yes	No	No	Yes	No
Video intercom	No	Yes	No	Yes	Yes	No	Yes	Yes	No
Person of interest	No	No	No	Yes	No	No	No	Yes	No
Floor heat map	No	No	No	No	No	No	No	Yes	No

BioStar Air doesn't aim to be a full VMS (Video Management System). Instead, it brings the most essential video tools right into your access control flow, without the complexity or licensing costs of full-scale surveillance platforms.

BioStar Air supports:

- Real-time digital video via ONVIF-compatible IP cameras
- Recorded video (on camera SD card) tied to access events
- Searchable video logs and clips
- Alerts and basic video reporting

Platforms like competitors V, G, and A offer deeper VMS functionality: analytics, cloud storage, AI-based person detection, and more. That makes them ideal for organizations with dedicated security operations and full-time monitoring needs.

But for leaner teams or those who want door-centric visibility without a full CCTV deployment, BioStar Air offers a clean, integrated, and easy-to-use solution.

Verdict: If you need heatmaps, AI tagging, and forensic search, go with a VMS-focused platform. But if your priority is quick visibility at the point of entry—tied to access events—BioStar Air delivers the right level of video integration without the overhead. It's a smart balance for coworking spaces, education, retail, and growing multi-site operations.

Overall.

Features	BioStar Air	Comp. A	Comp. G	Comp. K	Comp. B	Comp. AA	Comp. S	Comp. V	Comp. G
Multi-credential	*****	***	***	****	****	**	**	***	**
Native Biometrics	Yes	No	No	Yes	Yes	No	No	No	No
Edge Architecture	Yes	No	No	No	No	No	Yes	No	No
Video	**	****	****	**	***	**	**	*****	**
Alarm	No	Yes	Yes	Yes	No	No	No	Yes	Yes
API Integrations	Limited	Extensive	Extensive	Extensive	Extensive	Limited	Limited	Extensive	Absent

In a cloud market filled with similar claims, the real test comes down to execution, especially at the door. BioStar Air scores high where it counts: in credential flexibility, biometric readiness, and architectural simplicity.

While some competitors outperform on video or alarm management (like competitors V and G), most struggle with deeper biometric integration or edge-level innovation. BioStar Air stands out with native biometric support in the cloud, smart edge architecture, and support for app-less, mobile, and facial credentials, creating a user-first experience with lower infrastructure demands.

The tradeoff? BioStar Air's current video features are still lightweight (currently in beta), favoring door-centric simplicity over full-blown VMS capabilities. But for teams focused on access, not surveillance, that's often a strength, not a weakness.

Verdict: BioStar Air leads in modern, flexible access control, especially for environments where fast enrollment, cloud-native biometrics, and frictionless scaling matter most.

Conclusion

Cloud access control isn't just a trend, it's a shift in how businesses manage space, identity, and security. BioStar Air was designed to connects the world's most advanced biometric readers directly to the cloud. It eliminates the need for server closets and door controllers. It syncs credentials across sites in real-time. And it empowers you to manage access, enroll users, and respond to alerts from anywhere. Whether you're managing five doors or five hundred, building a coworking empire or upgrading your residential footprint, this is what cloud access control should look like.

It's time to unlock the next era of access control. It's time to think bigger, with less.

Suprema Inc.
17F Parkview Tower, 248, Jeongjail-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, 13554, Republic of Korea
T +82 31 783 4502 **W** www.supremainc.com

For more information visit our website below by scanning the QR code.
https://www.supremainc.com/en/about/contact-us.asp