

ACTatek & AMS

Competitor Comparison

A verified marketing comparison of leading access control and physical security platforms

People

Security

Environment

Energy

Unified Edge AI IoT Solution

Research standard

Every competitor statement in this report is tied to an official manufacturer source. Where a function was not found in the official core-product material reviewed, the report states “Not publicly evidenced” instead of assuming that it is unavailable.

Prepared for marketing and customer discussions
Official-source review completed 2 August 2026

1. Executive Summary

ACTAtek is positioned as a unified operational platform, not only an access control system.

PEOPLE Workforce management, shifts, visitor workflows, guard tour and healthcare functions.	SECURITY Biometric and RFID access, occupancy, alerts, roll call, video and intercom workflows.	ENVIRONMENT Environmental sensors, air-quality monitoring and hazard detection through AMS and IoT controllers.	ENERGY Direct control of lighting, HVAC, ventilation and appliances using occupancy, schedules and sensor data.
--	---	---	---

Verified positioning statement

ACTAtek combines intelligent edge terminals, AMS central management, IoT controllers and sensors in one architecture. The strongest verified differentiator is the direct connection between authenticated identity and occupancy data, environmental sensing, and automated control of building systems. [Source](#)

What the comparison shows
Several competitors provide excellent access control, video, visitor management, cloud operations or biometric hardware. ACTAtek differs by combining these security functions with workforce applications and direct environmental and energy automation in the same AMS ecosystem.

Products compared

- ZKTeco ZKBio CVSecurity / ZKBio software portfolio
- Suprema BioStar 2, with BioStar Air noted as the separate cloud platform
- Invixium IXM WEB and licensed IXM modules
- Brivo Security Suite
- Verkada Command access control, Guest and air-quality products
- LenelS2 OnGuard 8.4 / OnGuard Cloud
- Honeywell Pro-Watch 6.5.1

2. How to Read the Comparison

The report separates core capability from optional modules and integrations.

Native / Core Function is part of the reviewed platform or its documented core ecosystem.	Licensed / Add-on Available through an optional module, edition or licence.	Separate Product Available from the vendor, but not the same software product.	Integration-based Delivered through APIs, partner products or third-party systems.	Not publicly evidenced Not found in the reviewed official core-product sources; not an absolute “No”.
---	---	--	--	---

Scope controls

- Only official manufacturer websites, official support pages and current ACTatek project documentation were used.
- A feature is not marked “Native” merely because the vendor offers it somewhere else in its product portfolio.
- Hardware capabilities are described as model-dependent where a software platform supports multiple terminal or reader models.
- Capacity limits and licence quantities are excluded unless the same definition is publicly documented for all compared products.
- The unidentified “SecureID” entry in the supplied comparison is omitted because the manufacturer and exact product could not be verified.

Marketing-safe interpretation

Use this report to explain product positioning. For a formal tender, convert each requirement into Comply / Partially Comply / Does Not Comply against the exact quoted software edition, licence, device model and integration scope.

3. Comparison with Biometric and Workforce Platforms

ACTatek compared with ZKTeco, Suprema and Invixium.

Biometric and workforce platform comparison

Capability	ACTatek AMS	ZKTeco	Suprema	Invixium
Primary platform scope	Native: access, workforce, visitor, guard tour, healthcare, IoT and video workflows. Source	Core: web-based integrated security and biometric/computer-vision platform. Source	Core: web-based access control platform with time attendance, visitor and video-log options. Source	Core: centralized biometric device management, access, monitoring and reporting. Source
Time attendance and shifts	Native: time attendance, multi-shift management, overtime, alerts and reports. Source	Available through ZKBio Time and attendance functions in the ZKTeco software portfolio. Source	Licensed add-on: BioStar 2 TA module. Source	Licensed add-on: IXM TIME with shifts, leave, payroll-ready reports and notifications. Source
Visitor management	Native: pre-registration, ID/photo capture, temporary QR or card credentials and auto-expiry. Source	Available in ZKTeco platforms; ZKBio Zlink documents integrated access, attendance and visitor functions. Source	Licensed visitor-management function within the BioStar 2 ecosystem. Source	Licensed add-on: IXM VISITOR with pre-registration, walk-in and online registration. Source
Guard tour / patrol management	Native: routes, schedules, live monitoring and performance reports using biometric, RFID, QR or PIN checkpoints. Source	Not publicly evidenced in the reviewed ZKBio core-product pages. Source	Not publicly evidenced in the reviewed BioStar 2 core-product page. Source	Not publicly evidenced in the reviewed IXM WEB core-product page. Source
Health and risk workflows	Native: body-temperature screening, contact tracing, capacity control and configurable risk assessments. Source	Device-based temperature and mask options exist; an AMS-equivalent health workflow was not evidenced in the reviewed core platform pages. Source	Device-based thermal and mask functions exist; broader healthcare workflow is not presented as a core BioStar 2 module. Source	Licensed add-on: IXM Health supports temperature monitoring, screening workflows and health instructions. Source
Environmental and energy control	Native: sensors plus direct lighting, HVAC, ventilation and appliance control through the IoT Controller. Source	Not publicly evidenced as a native ZKBio CVSecurity building-automation function. Source	Not publicly evidenced as a native BioStar 2 building-automation function. Source	Not publicly evidenced as a native IXM WEB building-automation function. Source
Deployment choice	Native choice: on-premises, SaaS or hybrid deployment. Source	On-premises ZKBio CVSecurity; ZKBio Zlink is a separate SaaS product. Source	On-premises BioStar 2; BioStar Air is a separate cloud platform. Source	On-premises IXM WEB; no vendor-hosted SaaS edition was evidenced in the reviewed source. Source
Integration	Native SOAP and REST APIs; SQL Server, MySQL, Oracle and Azure SQL options for on-premises AMS. Source	ZKBio CVSecurity API provides third-party data connection; HA is a separate product. Source	Open API and SDK integration are documented. Source	IXM SDK and licensed IXM Link synchronize with leading access-control platforms. Source
Public cybersecurity position	TLS 1.3, VAPT, hardened Linux and IP-range restriction are documented for the ACTatek ecosystem. Source	ZKBio CVSecurity and ZKBio Time received Safe-to-Host certifications; ZKTeco also publishes security bulletins. Source	AES-256, ISO 27001/27701, Secure Element and Secure Boot are documented. Source	Updated encryption, vulnerability assessment and penetration testing are documented for IXM WEB. Source

Note: “Not publicly evidenced” means that the feature was not found in the official product pages reviewed. It may still be possible through customization, another product or a regional offering.

4. Comparison with Enterprise and Cloud Physical Security Platforms

ACTatek compared with Brivo, Verkada, LenelS2 OnGuard and Honeywell Pro-Watch.

Enterprise and cloud physical security comparison

Capability	ACTatek AMS	Brivo	Verkada	LenelS2 OnGuard	Honeywell Pro-Watch
Primary platform scope	Native: access, workforce, visitor, guard tour, healthcare, IoT and video workflows. Source	Core: cloud-native access, video intelligence, visitor, intrusion and sensors. Source	Core: cloud-managed access, video, alarms, intercom, Guest and environmental sensors. Source	Core: enterprise access control with integrated video and broad third-party integration. Source	Core: global access control, video surveillance and intrusion detection in one view. Source
Workforce and time attendance	Native: shifts, attendance, overtime, leave, job costing, reports and alerts. Source	Not a workforce time-and-attendance platform in the reviewed Security Suite source. Source	Attendance analytics uses access data; payroll, shifts and workforce rules are not presented as core access functions. Source	Not publicly evidenced as a core OnGuard workforce time-and-attendance module. Source	Not publicly evidenced as a core Pro-Watch workforce time-and-attendance module. Source
Visitor management	Native: visitor lifecycle, credentials, host alerts and full visitor records. Source	Available in Brivo Security Suite; current visitor offering is integrated into the cloud platform. Source	Separate Command product: Verkada Guest with screenings, workflows and temporary credentials. Source	Add-on browser client: OnGuard Visitor. Source	The official Pro-Watch Visitor Management 3.0 page is marked discontinued; verify current alternative before quoting. Source
Emergency roll call / mustering	Native: fire and emergency roll call with occupancy and evacuation reporting. Source	Not explicitly evidenced as a native muster function in the reviewed Brivo product overview. Source	Native roll-call reports list users and visitors currently within a site. Source	Integration-based: AllClear integration provides mustering and emergency response. Source	Not publicly evidenced in the reviewed Pro-Watch core-product page. Source
Environmental monitoring	Native: AMS manages environmental sensors and combines readings with occupancy data. Source	Available: sensors are part of the cloud security ecosystem. Source	Native separate product family: cloud-managed air-quality and environmental sensors. Source	Integration-based through the open enterprise ecosystem; not shown as a native sensor product in OnGuard. Source	Integration-based through the broader building and security ecosystem. Source
Direct HVAC, lighting and appliance control	Native: direct relay and scene control using occupancy, schedules and sensor thresholds. Source	Integration-based through APIs and smart-building connections; direct appliance control is not stated as a core Security Suite function. Source	Monitoring and alerts are native; direct HVAC or lighting control is not stated as a core sensor function. Source	Integration-based through building-system and partner integrations. Source	Integration-based through Honeywell building and third-party systems. Source
Deployment model	Native choice: on-premises, SaaS or hybrid. Source	Cloud-native SaaS. Source	Hybrid-cloud: local controllers with centralized Command management; no local management server. Source	On-premises OnGuard plus a separate single-tenant OnGuard Cloud offering hosted on AWS. Source	Primarily on-premises enterprise software with web clients and cloud-connected ecosystem functions. Source
Open integration	SOAP and REST APIs plus multiple customer-selected database engines. Source	Open API platform and integration marketplace. Source	APIs support door and scenario workflows; broader integrations are available in Command. Source	Open, customizable platform with a broad integration ecosystem. Source	Integrates Honeywell and third-party access and video systems; interface scope depends on the quoted solution. Source
Public cybersecurity position	TLS 1.3 device-to-platform communication, VAPT and hardened Linux are documented. Source	SOC 2 Type II, ISO/IEC 27001:2022 and TLS support are documented. Source	TLS 1.2 or greater in transit and encryption at rest are documented. Source	OnGuard 8.4 documents cryptographic modules and capability for FIPS 140-3 compliance. Source	Honeywell publishes product security patch testing notices; exact transport protocol depends on the deployed architecture. Source

This table compares the reviewed products as sold. A separate vendor product is not treated as a native function of the core platform.

5. Edge Device and System Architecture

The software comparison must be considered together with the hardware topology.

Hardware and edge architecture comparison

Architecture area	ACTatek	ZKTeco	Suprema	Invizium	Brivo	Verkada	OnGuard / Pro-Watch
Door-edge architecture	All-in-one intelligent terminal with local CPU, database, credentials and door relay. Source	Portfolio includes standalone biometric terminals and separate panel-reader architectures. Source	Intelligent biometric terminals and controller-based architectures are both supported. Source	Biometric terminals managed by IXM WEB; IXM Link connects them to third-party access panels. Source	Cloud platform with local access panels, readers, locks and sensors. Source	Command platform with local access controllers and connected readers; intercom and cameras are separate integrated devices. Source	Traditional enterprise controller/panel and reader architecture with a broad partner ecosystem. Source
Authentication options	Face, fingerprint, RFID, QR, OTP and PIN options in the ACTatek device family. Source	Broad biometric, card, QR and PIN options; exact credentials are device-dependent. Source	Face, fingerprint, card, mobile and PIN options; exact credentials are device-dependent. Source	Face, fingerprint, card and PIN options across the Invizium device portfolio. Source	Physical and mobile credentials with reader and lock options. Source	Physical badges, mobile devices and other supported credential types. Source	Credential and biometric support depends on the selected reader and partner hardware. Source
Network options at the edge	LAN, PoE, Wi-Fi and optional 4G/5G SIM are documented for ACTatek models. Source	Ethernet, PoE, Wi-Fi and cellular availability are model-dependent across the ZKTeco device portfolio. Source	BioStation 3 documents Ethernet, PoE+ and Wi-Fi. Source	Network and hardware options are model-dependent within the biometric device portfolio. Source	Panels connect readers and locks to the cloud service; exact network options vary by panel. Source	Controllers require power and internet; network architecture is centrally managed through Command. Source	Network options depend on the selected controller, panel and reader hardware. Source
Offline access continuity	Access decisions continue at the terminal; events are retained locally and synchronized later. Source	Standalone terminals are offered; exact offline behaviour is device- and configuration-dependent and should be verified. Source	Intelligent terminals can perform local authentication; architecture and device determine behaviour. Source	Exact offline access behaviour is not stated in the reviewed IXM WEB overview and should be verified by terminal model and integration. Source	Current panels document local credential and event storage for connectivity interruptions; capacity depends on panel model. Source	Local access controllers continue defined functions during internet outages. Source	Offline behaviour depends on the selected controller architecture and is not defined in the reviewed high-level product pages. Source
Camera and intercom at entry	Built-in event camera / RTSP and optional SIP intercom in the ACTatek family. Source	Available on selected terminals and separate video-intercom products. Source	BioStation 3 includes VoIP intercom and RTSP video monitoring. Source	Camera and display functions vary by biometric terminal; broad SIP intercom is not stated as a core IXM WEB function. Source	Video and entry products are integrated in the platform but generally separate from the reader. Source	Video intercom combines intercom, camera and access functions as a separate integrated device. Source	Video and intercom are delivered through native or partner systems rather than a universal built-in reader function. Source

Hardware functions vary by model. This table describes the documented architecture rather than claiming that every model from a vendor has every option.

6. Competitor-by-Competitor Marketing View

Fair positioning improves credibility and helps sales teams focus on genuine differences.

Competitor	Verified strength	ACTAtek positioning opportunity
ZKTeco	Strong biometric hardware range and broad access/time software portfolio. Source	ACTAtek can lead with one AMS ecosystem spanning guard tour, healthcare, IoT control, multiple deployment choices and direct energy automation.
Suprema	Strong biometric performance, mobile credentials, security certifications and open APIs. Source	ACTAtek can lead with broader operational modules and the direct link from occupancy and sensor data to lighting, HVAC and appliance control.
Invoxium	Strong biometric terminals plus licensed workforce, visitor and health modules. Source	ACTAtek can lead with native guard tour, broader central access functions, SaaS/on-premises choice and integrated IoT/environment/energy control.
Brivo	Strong cloud-native access, video, visitor, intrusion, mobile and IT integration. Source	ACTAtek can lead where customers need on-premises control, workforce/attendance functions, biometric edge terminals and direct building automation.
Verkada	Strong cloud-managed video, access, intercom, visitor and environmental monitoring. Source	ACTAtek can lead where customers require on-premises/hybrid choice, workforce management, healthcare workflows and direct local HVAC/lighting control.
LenelS2 OnGuard	Mature enterprise access platform with integrated video, browser clients and extensive partner integrations. Source	ACTAtek can lead with a simpler edge-terminal architecture and a wider native application scope across workforce, health, environment and energy.
Honeywell Pro-Watch	Mature global access, video and intrusion platform within the Honeywell building ecosystem. Source	ACTAtek can lead with all-in-one biometric edge devices, workforce functions, native guard tour/healthcare and direct IoT energy automation.

Key message: Do not claim that competitors lack cybersecurity, APIs, video or offline access. The credible ACTAtek advantage is the breadth of native operational applications combined with intelligent edge devices and direct IoT control.

7. Marketing Messages Supported by the Evidence

Recommended wording for presentations, proposals and landing pages.

Safe, supportable message	Wording to avoid unless project-specific evidence is available
• “One platform for People, Security, Environment and Energy.” • “Use verified identity and occupancy data to automate lighting, ventilation and HVAC.” • “Choose on-premises, SaaS or hybrid deployment according to data-sovereignty and IT requirements.” • “Operate at the edge during network interruptions and synchronize centrally when connectivity returns.” • “Integrate with enterprise systems through SOAP and REST APIs.” • “Reduce system fragmentation by combining access, workforce, visitor, guard tour, healthcare and IoT control.”	• “Competitors do not use TLS” or “competitors can easily be hacked.” • “All competitor devices are Android” or “all competitor devices can be rooted.” • “Every ACTatek installation has unlimited users or devices.” • “ACTatek is the only product with biometrics, cloud access, mobile credentials or offline operation.” • Fixed energy-saving percentages without a measured baseline and project calculation. • A universal “Yes” or “No” where the result depends on a licence, device model, integration or separate product.
Recommended headline ACTatek Unified Edge AI IoT Solution - one secure platform to manage People, Security, Environment and Energy.	

Recommended supporting copy

ACTatek connects intelligent biometric and RFID edge terminals with AMS central management, IoT controllers and environmental sensors. The result is a unified system that manages access and workforce operations while using real-time occupancy and sensor information to automate building responses. The platform can be deployed on-premises, as SaaS or in a hybrid model and integrates with third-party systems through open APIs. [Source](#)

8. Conclusion

The comparison supports a focused and defensible ACTatek value proposition.

ACTatek's strongest verified advantage

ACTatek is not simply another access control platform. It combines access, workforce, visitor, guard tour, healthcare, environmental monitoring and direct energy automation around the same real-time identity and occupancy data.

Best-fit customer situations

- Customers seeking one platform instead of separate access, attendance, visitor, health and IoT systems.
- Multi-site deployments requiring centralized control with edge operation during network interruption.
- Organizations that require on-premises data control, cloud convenience or a hybrid deployment model.
- Buildings that want to use verified occupancy and environmental measurements to control HVAC, lighting and appliances.
- Projects needing face, fingerprint, RFID, QR, OTP and PIN options with open enterprise integration.

Final qualification

This document is a marketing comparison, not a formal certification of competitor compliance. Product editions, licences and public documentation can change. Before a tender submission, confirm each requirement against the exact vendor quotation, device model, licence and current statement of compliance.

One System. Total Control.

People | Security | Environment | Energy [Source](#)