AInsights
Unveiling hidden
threats

Why **AInsights**

Traditional access control systems are burdened by millions of logs, operational complexity, and misconfiguration, making it nearly impossible for security teams to extract meaningful insights or maintain proactive defenses. As a result, security operations often become reactive, leading to inefficiencies, increased risks, and gaps in compliance, with threats being addressed only after incidents occur.

IDCUBE AInsights transforms access control management by introducing AI-driven security intelligence through a comprehensive suite of analytical techniques, including machine learning, behavioral analytics, predictive modeling, time series analysis, prescriptive analytics, headcount, footfall tracking, and occupancy matrices. By consolidating data from multiple access control systems into a unified data lake, **AInsights** provides a holistic security overview and generates actionable insights through nine dashboards, 55 intelligence modules, and 184 dimensions.

With 46 sentinels dedicated to vulnerability and threat analysis, **AInsights** generates overall security scores for facility-wise comparative analysis, enabling organizations to proactively address risks and operational inefficiencies before they escalate.

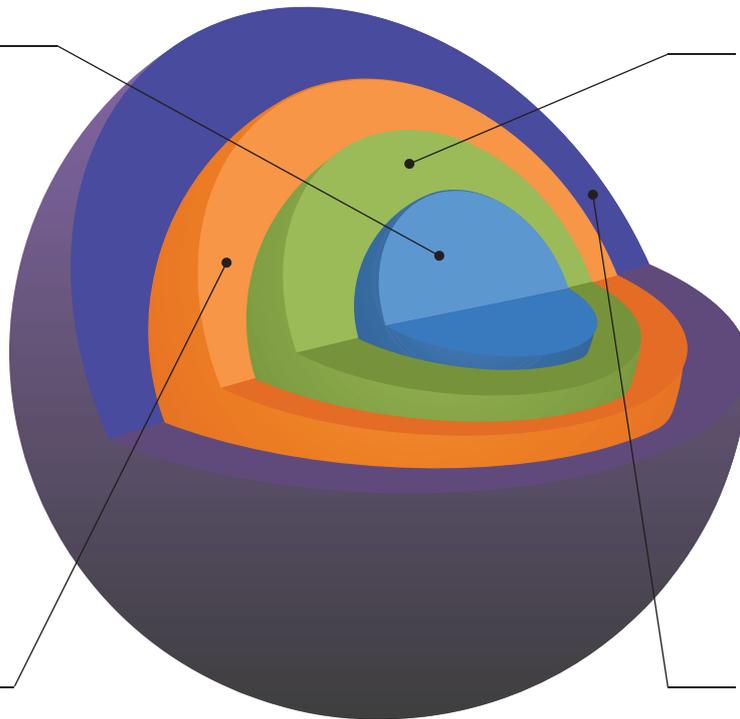|	
9 Dashboards	**55** Intelligence Modules
184 Dimensions	**46** Risk Assessment Sentinels

World's 1st AI-powered

Platform to Quantify Physical Security for comparative analysis, vulnerability and anomaly detection

Access Control Systems

Virtualization

Intelligence

Communication

Access Control Systems

Siemens | IDCUBE | LenelS2
Honeywell | JCI | Genetec | Milestone

Virtualization

Cloud-based data-lake
Virtual identities – NFC/BLE/M-Wallets/Dy.
QR codes

Intelligence

Proprietary ML Algorithms Gen. AI-powered
Analysis Security Intelligence Resource
Optimization

Communication

Dashboards
AI-Chatbots(Gen-AI)
APIs and Adapters

RiskVision **AI**

Insider **Threat**

AI-powered insider threat analysis enhances security by continuously monitoring user interactions within the access control system. By employing advanced behavioural analytics, it identifies deviations from normal patterns by comparing individual behaviours against historical trends and peer activity. Unusual access patterns and critical alerts linked to individuals contribute to their risk evaluation. The system dynamically assesses these risks, helping security teams detect and prioritize high-risk personnel. Interactive dashboards highlight potential threats in real time, enabling management to take proactive measures to mitigate insider threats and bolster the organisation's overall security posture.
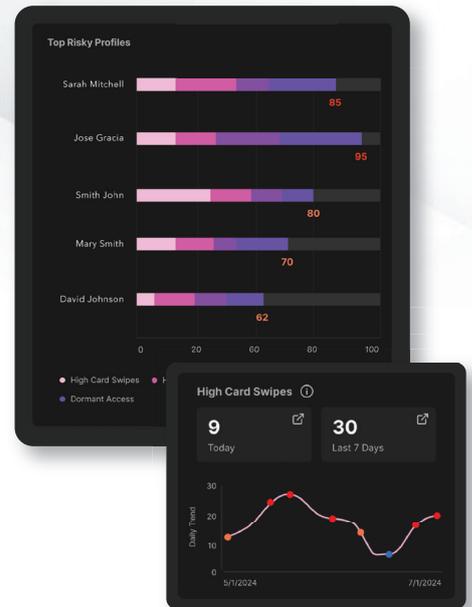
Vulnerability **Detection**

Access control is the first line of defense of an organization. Various access control vulnerabilities make the system vulnerable to potential security breaches. The timely identification of these vulnerabilities prevents security breaches from happening. The **IDCUBE's AInsights** identifies the system vulnerabilities on the following counts:
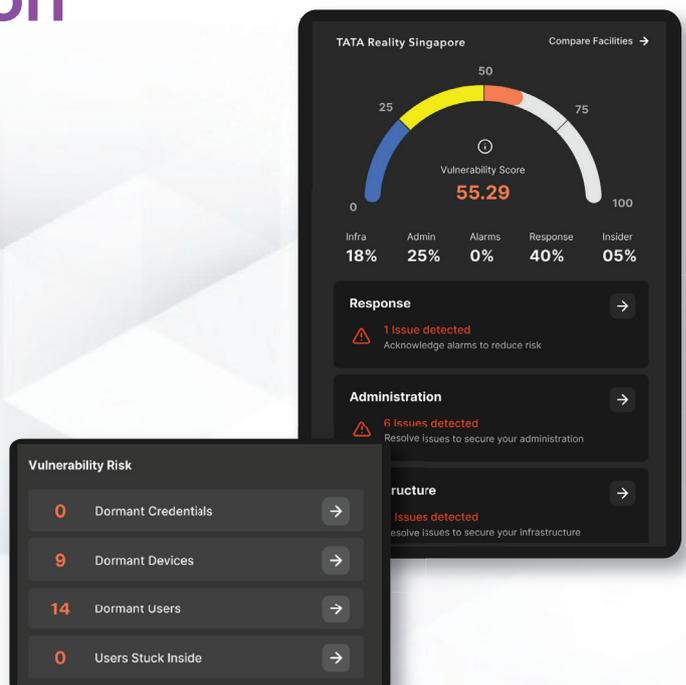
Administration

Administrative weaknesses like inactive accounts, outdated credentials, and excessive permissions pose security risks. **AInsights** detects and analyzes these threats in real time, providing actionable insights. By addressing them promptly, organisations can enhance security, prevent breaches, and maintain a well-managed access control system.
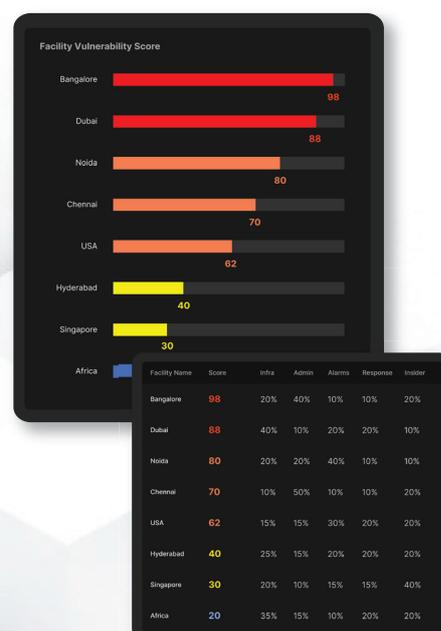
Infrastructure

Infrastructure flaws like weak authentication, unsecured data, and misconfigured access controls invite security threats. **AInsights** detects and flags these risks in real time, empowering security teams with actionable insights. Proactive mitigation strengthens access control, enhances resilience, and ensures compliance.

Events and Alarm

Events & alarms are analyzed using AI and predictive analytics to detect anomalies and potential threats. **AInsights** continuously monitors access logs, compares global trends, and conducts root cause analysis, providing actionable insights. This enables security teams to mitigate risks, enhance response times, and

Response

Response vulnerabilities arise from failing to acknowledge critical alarms, risking security threats and operational disruptions. Timely acknowledgment and resolution of alarms are essential for a secure environment. **AInsights** identifies gaps in alarm responses, ensuring no critical alert is missed.

Facility Security **Scores**

Facility security scores provide a quantifiable measure of the overall effectiveness of an organization's access control system. Based on 46 sentinels categorised into key sections, these scores comprehensively evaluate security infrastructure, policies, administration, alarm patterns, and response mechanisms. Security directors can objectively assess and compare facility security levels, identifying strengths and vulnerabilities across locations. This enables targeted interventions, policy enhancements, and resource allocation to fortify weak points. This quantification approach ensures continuous security improvement.

Facility Vulnerability Score

Bangalore	98
Dubai	88
Noida	80
Chennai	70
USA	62
Hyderabad	40
Singapore	30
Africa	

Facility Name	Score	Infra	Admin	Alarms	Response	Insider
Bangalore	98	20%	40%	10%	10%	20%
Dubai	88	40%	10%	20%	20%	10%
Noida	80	20%	20%	40%	10%	10%
Chennai	70	10%	50%	10%	10%	20%
USA	62	15%	15%	30%	20%	20%
Hyderabad	40	25%	15%	20%	20%	20%
Singapore	30	20%	10%	15%	15%	40%
Africa	20	35%	15%	10%	20%	20%

Alarm **Vision**

Alarm Vision delivers a clear statistical and graphical view of alarms and events within the access control system. Powered by advanced analytics, it detects time-series patterns across 50+ dimensions. Structured into 8 intelligence modules, it offers intuitive, interactive, and filter-friendly visualisations. Each module provides deep data access for further filtering and analysis, enabling security teams to identify critical trends and prioritize high-risk sites. This real-time insight ensures swift intervention, enhances situational awareness, and strengthens overall security management, helping organisations proactively mitigate risks and maintain a secure environment.
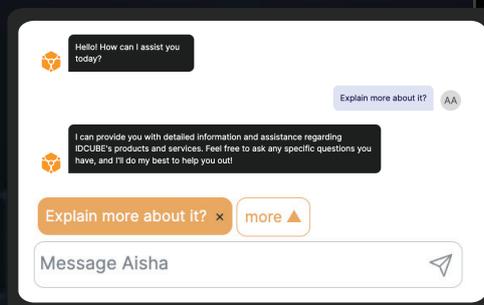
Flow **Vision**

Flow Vision provides key insights into people movement and space utilization. It analyzes occupancy and footfall trends over time across different areas and zones. This data helps optimize space management, reduce energy costs, improve resource planning, enhance cafeteria operations, and boost overall facility efficiency.

Gen-AI
AIsha

AIsha is an advanced chatbot designed to assist administrators, security directors, and senior management with natural language queries in the access control system. It simplifies tasks by answering how, what, and why queries related to the access control system and its software interfaces. Additionally, it aids in retrieving complex data insights instantly. Queries such as "How many people are absent today?" or "Who was in the facility after 7 PM?" are resolved swiftly, eliminating manual effort and enhancing decision-making efficiency, ultimately streamlining security operations and workforce management.

Other **Dashboards**

Guest Track

The Guest Track consolidates visitor trends, helping organizations monitor frequent visitors, requesters, overstayers, and unreturned cards. It provides time-based trend analysis and alerts authorities to potential risks. The data is displayed in a clear, filterable format, enabling security teams to identify patterns and enhance facility safety.

Chrono Vision

The Chrono Vision provides a clear view of employee turnout trends, tracking half-days, early-outs, leaves, late-ins, and missed punches. It highlights irregular patterns for quick identification. With time-based analysis and an easy-to-filter format, it simplifies reviews, ensuring critical attendance insights are readily available for decision-making.

Cred Vision

The Cred Vision delivers critical analytical insights into the management of credentials—the virtual keys to your facilities. Mismanagement of credentials can lead to significant security risks, making effective oversight essential. This dashboard highlights credentials that require immediate review, provides an overview of the distribution patterns, and analyses credential types across facilities.

People Vision

The People Vision offers a clear overview of all users in a facility, including headcount, active users, status, and departmental breakdowns. It provides security directors and management with a quick snapshot of workforce or resident profiles, enabling efficient personnel management and informed decision-making at a glance.

System Vision

The System Dashboard offers a comprehensive overview of all hardware components installed and configured within the facility. By providing a clear and centralised view, it empowers administrators to monitor and manage the infrastructure efficiently, ensuring optimal system performance and readiness.

Live Count

Live Headcount provides a real-time view of people present in a facility, categorised by occupants, visitors, teams, areas, and zones. This ensures organisations maintain full visibility of on-site personnel, enabling quick response during emergencies like fires or earthquakes, enhancing safety, and improving overall security management.

IDCUBE

We built the World's first AI-powered operating system for physical Access Control - **Access360**.

The OS provides comprehensive support for a wide range of physical identities, encompassing legacy credentials like smartcards and biometrics, as well as virtual ones such as mobile credentials and QR codes. This enables secure and agile authentication of diverse entities across various facilities.