INTELLIGENCE REPORT · 2026

State of the Verticals Benchmark Report 2026

Cross-vertical trends, regional benchmarks, and strategic intelligence across Education, Healthcare, and Financial Institutions.

This is the kind of report I have been arguing the industry needs more of for years. Honored to be part of it and add my thoughts.

~ Lee Odess

acre

The Access Control Collective

Commissioned by Acre Security ·Authored by The Access Control Collective

2026

About This Report

The State of the Verticals Benchmark Report provides cross-vertical trends, regional benchmarks, and strategic intelligence across three priority sectors: Education (K-12 and higher education), Healthcare, and Financial Institutions.

This report is the foundation of a yearlong program that blends market intelligence, thought leadership, storytelling, and in-person experiences designed to drive executive visibility across important verticals.

Methodology

This benchmark synthesizes intelligence across four primary sources:

- Direct conversations with vertical subject matter experts, end users, integrators, and specifiers
- Public reporting, media coverage, and regulatory developments observable across each vertical
- Technology deployment patterns visible across manufacturer roadmaps, integrator bid activity, and procurement signals
- Industry discussions and leadership priorities from the PhySec Collective community and The Access Control Collective's ongoing research into platform transformation

This is analytical intelligence, not statistical sampling. Insights are grounded in what is observable, defensible, and confirmed across multiple independent sources.

THREE PRIORITY SECTORS

Education

K-12 and higher education institutions navigating mandates, mobile credentials, and campus safety investment

Healthcare

Health systems managing identity fragmentation, workplace violence risk, and clinical system integration

Financial Institutions

Banks and financial services firms consolidating physical security governance across complex global estates

INTELLIGENCE APPROACH

The findings, framing, and conclusions reflect independent analysis and practitioner interviews — observable, defensible, and confirmed across multiple independent sources.

Analytical intelligence is underrated in our industry. We say statistical sampling is all that matters but the right call for a market this fragmented is also to include analytical intelligence, because the truth also lives in the conversations practitioners have when no one is selling them anything.

DISCLOSURE

This report was commissioned by Acre Security and authored independently by The Access Control Collective. The findings, framing, and conclusions reflect independent analysis and practitioner interviews, not the views or positions of Acre Security.

PART I

Cross-Vertical Benchmark

The report covers three sectors, three buyer profiles, and three sets of regulatory pressures. Underneath the surface differences, a single structural transformation is underway across all of them. Physical access control is no longer a door hardware problem. It is an identity infrastructure problem, and every organization in education, healthcare, and financial services is encountering that reality at different speeds, with different resources, and with different consequences when they get it wrong.

1	2	3	4	5
PLATFORM SHIFT	IDENTITY CONVERGENCE	CREDENTIAL LIFECYCLE	REGIONAL DIFFERENTIATION	COMPLIANCE DRIVER

THEME 1

The Platform Shift — From Products to Identity Infrastructure

The defining transition across all three verticals is the same: organizations are moving, at different speeds, from treating physical access control as isolated door hardware to treating it as identity infrastructure that connects physical and digital operations.

The language is shifting in observable ways. RFPs that once specified hardware are beginning to specify outcomes. Budget ownership is migrating from facilities to IT and security operations. Integration requirements are moving from optional add-ons to core selection criteria.

This shift is not uniform. Large enterprises in each vertical are further along, while regional and community organizations are lagging. The gap between what is possible and what is deployed is widest in the middle market.

Education, healthcare, and financial services are all hitting the same wall at different speeds, which is exactly what you would expect when an industry is mid-transition from a $10 billion hardware business to a $100 billion software and identity business.

THEME 2

The Identity Convergence — Physical and Digital Security Are Merging

In every vertical, the siloes between physical security and cybersecurity are collapsing. The trigger differs by sector. In financial institutions it is fraud detection integration. In healthcare it is HIPAA enforcement extending to physical access. In education it is emergency notification and lockdown systems demanding unified identity across every access point.

The organizations managing this convergence well are those that have aligned physical security and IT under a common governance framework. Those that have not are carrying significant operational and compliance risk.

FINANCIAL
Fraud detection integration driving convergence

HEALTHCARE
HIPAA enforcement extending to physical access

EDUCATION
Lockdown systems demanding unified identity

THEME 3

The Credential Lifecycle Problem — Onboarding Is Managed. Offboarding Is a Risk.

Across all three verticals, the provisioning of access credentials is imperfect but improving. The revocation of credentials, particularly for contractors, temporary staff, and travelers, remains a significant operational and security vulnerability.

The organizations that have solved this problem have done so through full lifecycle credentialing integrated with HR and identity governance systems. The majority have not, and they are still relying on manual badge return and hope.

> *"Once the contractors finish their job they just hand their badge back in and then hope that somebody turns off their rights."*
>
> CIAN BOLGER, DIRECTOR OF SALES, ACRE SECURITY

The identity convergence point is where the Nokia moment happens for legacy vendors, and I have not seen most of them prepare for it seriously.

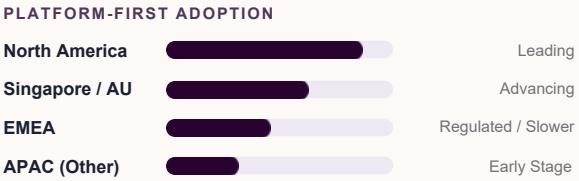
THEME 4

Regional Differentiation — North America Leads. Europe Fragments. APAC Varies.

Platform-first thinking is most advanced in North America across all three verticals. The drivers are consistent: a more innovative enterprise culture, standardized deployment models, and faster cloud adoption.

EMEA operates within stricter regulatory frameworks, particularly around identity and data privacy. GDPR creates friction for mobile credential adoption, and the result is more complex architecture and slower platform consolidation.

APAC presents the widest internal variation of any region. Singapore and Australia are leading, while the Middle East and parts of Southeast Asia are at earlier stages. Country-level decisions, not regional ones, drive outcomes here.



REGIONAL OPPORTUNITY

The regional variation in platform-first adoption creates a significant first-mover opportunity. Organizations in EMEA and APAC that are beginning their platform consolidation journeys need a vendor with both the global footprint and the vertical depth to guide that transition.

THEME 5

The Compliance Driver — Regulation Sets the Floor. Incidents Set the Ceiling.

In every vertical, regulation establishes baseline requirements, but regulatory compliance alone rarely drives significant capital investment. The real budget trigger is an incident, an audit finding, a merger, or a public failure.

This pattern is consistent across all three verticals. In education, the Va. Tech incident created a trigger moment. In healthcare, workplace violence incidents are driving investment. In financial services, audit findings and M&A due diligence expose vulnerabilities that drive procurement cycles.

The strategic implication is clear. Selling to compliance requirements is a floor strategy. Selling to risk reduction and operational outcomes is a ceiling strategy.

The credential lifecycle problem is the unglamorous truth of this industry, and Cian's quote about handing badges back and hoping is saying the part we whisper as an industry out loud.

PART II — VERTICAL SPOTLIGHT

Education

K-12 and higher education · Mandates, mobile credentials & campus safety investment

Education is the most emotionally charged vertical in physical security. The stakes are visible, the communities are vocal, the funding is complicated, and the technology gap between what is possible and what is deployed is significant.

The sector is moving. Mandates are arriving, mobile credentials are gaining traction, and institutions that once treated access control as a facilities budget item are beginning to treat it as a safety infrastructure investment.

MARKET CONDITIONS

Education operates on two parallel tracks. New construction is establishing modern standards while existing buildings are being retrofitted with whatever the budget allows. More activity is happening in existing infrastructure than in new construction, and that pattern will continue for the foreseeable future.

One Card providers have dominated higher education for years. The shift from those legacy architectures toward more open platforms is underway, driven by IT departments demanding interoperability and security teams demanding unified visibility.

Large urban districts are leading on platform consolidation. They have the scale to standardize across many sites and the budget to build toward a single pane of glass. Smaller and more rural districts are moving faster on mandates, particularly when targeted grant funding is attached. The driver differs; the destination is the same.

PROCUREMENT DRIVERS

- Bond measures & state grants
- Federal safety funding
- State mandate compliance
- Community & parent advocacy

Education is where the Sailing Ship Syndrome — the tendency of incumbent technologies to accelerate improvement just as disruption makes them obsolete — is most visible, because One Card providers built the dominant architecture for a previous era and IT departments are now forcing the platform conversation whether the security team is ready or not.

BUYER MOTIVATIONS

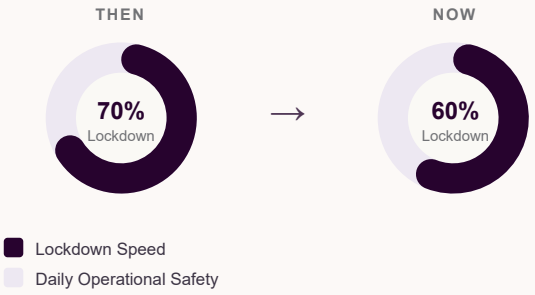
Active shooters are the loudest drivers in K-12. It shapes RFPs, bond measure language, school board conversations, and parent advocacy. It has the written workflows and the drills behind it. The most frequent security failure in practice, however, is unauthorized access, and daily operational safety is rapidly closing the gap on lockdown speed as the dominant investment priority.

Experts in the industry we spoke with describe a measurable shift in where the conversation is centered. A few years ago, lockdown speed dominated at roughly 70-30 or higher over daily operational concerns. Those same experts also reported that the ratio has moved to closer to 60-40 in favor of daily operational safety. The shift reflects a maturing understanding of how security systems actually perform: a system that works well on a regular Tuesday will also work on the worst day. Lockdown capability that exists inside a system nobody uses correctly the rest of the time is not a security program. It is a drill.

Higher education is bridging the gap between security and convenience. Mobile credentials are gaining traction precisely because students already carry phones. The economics are straightforward: reduce lost-card reissuance costs, improve student experience, and tighten access control simultaneously.

> *"The big buzz in higher education is mobile and around being more secured. It bridges the gap of security and convenience."*
>
> LARRY NIENABER, BUSINESS DEVELOPMENT MANAGER — HIGHER EDUCATION, ACRE SECURITY

INVESTMENT PRIORITY SHIFT



Community pressure has reached a critical mass point. Practitioners across the sector consistently report that staff safety concerns have intensified significantly over the past five years, with school safety ranking as the top community issue in district after district. Visible security progress is in high demand, and that pressure is understandable. The strongest districts are pairing visible upgrades with operational KPIs. They are pairing things like door compliance, response time, and drill performance, rather than allowing visible security to stand on its own.

The 70-30 to 60-40 shift toward daily operational safety is one of the most important data points in this entire report, because it reframes the K-12 conversation from a moment in time to an everyday operational system.

TECHNOLOGY ADOPTION PATTERNS

Mobile credentials are the most significant technology shift in higher education access control right now. The economics are compelling: eliminating the cost of reissuing physical cards for a population that loses them constantly is a straightforward return on investment argument.

The integration challenge is the deeper problem. Most institutions are managing access control, video surveillance, emergency notification, visitor management, and intercom as separate systems with separate applications. During an emergency, staff are switching between multiple screens. A door-force alarm triggers with no corresponding camera feed and no quick way to verify whether the incident is real. That is not a security program. That is a liability.

The districts building for the next 20 years are building toward a single incident workflow (one operational pane of glass) rather than a pile of mismatched devices. The rest are still patching, because funding is episodic and rip-and-replace across dozens of buildings at once is rarely possible.

ALYSSA'S LAW IMPACT

State mandates are creating standardization pressure in K-12. Alyssa's Law, which requires silent panic alarms in schools across multiple states, is a leading indicator of the regulatory direction. More mandates will follow. Institutions that build interoperable platforms now will be positioned to absorb future requirements without full system replacement. Mandates only raise the floor, however, not the ceiling. They work when states fund the full lifecycle: hardware, software, training, and ongoing support. Without consistent funding, districts end up cycling through whatever fits the current year's budget.

FRAGMENTED SYSTEM REALITY

- 📷 Video Surveillance
- 🔒 Access Control
- 📢 Emergency Notification
- 👥 Visitor Management
- 📞 Intercom Systems

Each running as a separate application, requiring staff to switch between multiple screens during emergencies.

THE GOAL: SINGLE PANE OF GLASS

One operational workflow for every incident, credential, and access event — replacing the pile of mismatched devices with unified incident response.

Alyssa's Law is exactly the kind of mandate that raises the floor without funding the ceiling, which is why interoperable platforms matter more than compliance checkboxes.

PROCUREMENT AND BUDGETING CYCLES

K-12 procurement is driven by bond measures, state grants, and federal safety funding. The cycle is long, community approval is required, and visible security improvements feature prominently in bond measure marketing. Visible security spend remains massive, and the challenge is that visible security without an operational workflow still leaves districts without a better system for managing what they now have.

Higher education procurement is more direct but still complex. IT, facilities, and security operations each have a claim on the budget and the decision, and successful vendors navigate all three stakeholders.

THE SILENT TAX

The operational burden of managing exceptions, lost credentials, and manual overrides consumes significant staff time across the sector. Pierce Mayfield calls this the silent tax, and the framing is precise. Districts are dedicating entire staff positions to a single function: unlocking doors for vendors, issuing temporary badges, and resolving credential issues on a loop. The cost never shows up on a security budget line because it lives in headcount and lost hours, which makes it easy to overlook and hard to justify fixing. When that dedicated person is out sick, the system stops. When they leave, institutional knowledge walks out with them. Mobile credentials address the lost-card portion of the burden directly, and the ROI argument — eliminate reissuance costs, reduce manual intervention, improve staff time allocation — is the conversation that moves procurement decisions at the district level.

INTEGRATION AND ECOSYSTEM

The highest-priority integration need in education is a unified incident workflow connecting access control, video, and emergency notification. The breakdown is not in any single system, but in the gap between them. A door-force event with no correlated camera feed is a workflow failure, not a technology failure.

Visitor and contractor management is the second-priority operational gap. Student and staff access is a scale problem, manageable with the right system. Visitor and contractor access is a variability problem: someone shows up 30 minutes early, they are not on the list, and someone opens the door. Variability is what breaks processes, and variability is hardest to systematize.

INTEGRATION PRIORITIES

1. Unified incident workflow: access control, video & emergency notification
2. Visitor and contractor management
3. Credential lifecycle: issuance, verification & revocation

The silent tax framing from Pierce is spot on in the education section, because the cost of fragmentation hides in headcount and lost hours rather than on a security budget line.

WHAT BUYERS ARE SELECTING FOR

The differentiating factor in education is not a single product capability. It is the ability to serve as the integration anchor for a school's full security infrastructure. You go from door hardware through identity management to emergency response workflow. Systems that carry an advantage in this vertical can address the full lifecycle: new construction standards, legacy retrofits, mobile credential migration, and platform consolidation. That breadth is rare, as most vendors in the market address one piece of the stack and leave the integration burden to the district.

New Construction Standards | **Legacy Retrofits** | **Mobile Credential Migration** | **Platform Consolidation**

WHAT WINNING LOOKS LIKE IN EDUCATION

The single-pane-of-glass model (again one workflow for every incident, every credential, every access event) is the frame that resonates with education buyers. School boards approve bond measures for outcomes: keeping students safe, reducing response times, and simplifying daily operations. Systems that position around those outcomes, with technology as the supporting evidence rather than the lead, are the ones that win the conversation and the contract.

K-12 BUYER GOAL
Keeping students safe, reducing response times, and simplifying daily operations

HIGHER ED BUYER GOAL
Mobile-first credentials, reduced reissuance costs, and tightened access across campus

VENDOR ADVANTAGE
Integration breadth across the full security stack, not a single point solution

School boards approve outcomes, not features, and the systems that lead with safety outcomes and treat technology as supporting evidence are the ones that win bond measure conversations.

PART III — VERTICAL SPOTLIGHT

Healthcare

Clinical operations, identity governance & workplace violence prevention

Healthcare is the most complex vertical in physical security. It operates at the intersection of clinical operations, IT governance, facilities management, regulatory compliance, and patient experience, and it is changing faster than it has in years.

The conversations happening now are different from those of even three years ago. The awareness is different. The people being hired into security leadership roles are more technology-forward. The ramp of change over the past 36 months is unlike anything the sector has seen before.

MARKET CONDITIONS

Physical access control in healthcare is no longer a facilities problem. It is a clinical operations problem. The budget is owned by security, IT is increasingly involved because most systems are IP-connected and threat-exposed, and the days of facilities managing access control in isolation are gone.

Acquisitions are the single largest driver of fragmentation in healthcare. Every acquired facility arrives with its own access control system, and the result across the average large health network is 6 to 12 or more disparate identity systems.

> *"Painting over the mold versus mold removal. Acquisitions are driving fragmentation no matter what. They are all seen as insecure."*
>
> KUMAR SOKKA, CEO, ACRE SECURITY

FRAGMENTATION REALITY

6–12+

DISPARATE IDENTITY SYSTEMS PER LARGE HEALTH NETWORK

Every acquired facility arrives with its own access control system — and the result is a compounding governance and compliance burden.

The market is moving toward unified identity platforms, but it is early. Demand is building, and the North American Southeast and Midwest are seeing the most change, driven primarily by leadership changes and the hiring of more technology-forward security executives.

The 6 to 12 disparate identity systems number is conservative in my experience, and "painting over the mold" is exactly what most health networks have been doing for a decade.

BUYER MOTIVATIONS

Workplace violence is the dominant investment driver in healthcare security. It is driving capital allocation, technology selection, and organizational attention in a way that no other threat scenario is.

Employee net promoter score, specifically the question of whether staff feel safe on campus, has become a talent retention metric. Hospitals that cannot answer that question affirmatively are losing nurses and clinical staff to competitors who can. Security is now a workforce issue, not just a safety issue.

THE TRUST TAX

Healthcare operates on a trust economy in a way that most industries do not. Patients choose hospitals based on reputation. Clinicians choose employers based on safety and culture. A single high-profile security failure (a workplace violence incident that reaches the news, a patient safety event tied to access control breakdown) does not just create a liability. It erodes the foundation the institution depends on for revenue, staffing, and community standing. Jeffrey Stout frames this as the trust tax: the ongoing cost of maintaining security at a level that protects institutional trust is real and significant, but it is manageable and predictable. The cost of a failure is neither. Organizations that treat physical security investment as a trust maintenance budget rather than a compliance cost make different procurement decisions, and they make them faster.

TECHNOLOGY ADOPTION PATTERNS

The healthcare access control market has entered an inflection period. The IAHSS is seeing narrative changes, organizations are asking different questions, and vendors are having different conversations than they were even two or three years ago.

SECURITY IS NOW A WORKFORCE ISSUE

Talent Retention
Staff feel-safe scores are now tracked as employee NPS, with hospitals losing nurses to safer competitors

Trust Economy
A security failure is not just a liability — it erodes the institutional trust that drives patient choice and staffing

Capital Allocation
Workplace violence drives technology selection and organizational attention above all other threat scenarios

The integration pathway gaining the most momentum connects access control with clinical systems. Epic is integrating with security systems, tagging patient records with behavioral risk attributes so that the clinical team and security team share real-time awareness. Axon's Fusus is enabling situational awareness centers that blend video, access, and clinical data. These are early signals of where the market is heading.

Today, healthcare security is still primarily reactive. Reporting dominates, and real-time response capability is emerging but is not yet standard. The gap between reporting and response is the technology opportunity.

The trust tax framing is great, because it moves physical security investment from a compliance line item to an institutional trust maintenance budget.

PROCUREMENT AND BUDGETING CYCLES

Healthcare security procurement is owned by the security function in most organizations, but IT is at the table in a way it was not five years ago. Vendors that cannot speak both languages of operational security and IT infrastructure are losing deals.

The highest-value procurement trigger is not a regulatory requirement. It is an audit finding or a merger, both of which expose vulnerabilities in ways that generate immediate budget authority.

Platform consolidation projects are long-cycle, high-value opportunities. They require executive alignment across security, IT, and facilities, and the vendors who win them are those who can manage stakeholder complexity, not just technical complexity.

STAKEHOLDER ALIGNMENT REQUIRED

- Security Function
- IT Leadership
- Facilities
- Clinical Ops

INTEGRATION AND ECOSYSTEM

Healthcare security professionals have largely stopped asking for more integrations. They are asking for interoperability: the ability to see the health of multiple systems from a single pane of glass without requiring every system to be replaced.

The emergency department is the highest-friction access point in any hospital. It is open, it attracts emotionally taxed individuals, and it is a primary target for bad actors seeking pharmaceutical access or information.

INTEGRATION PRIORITIES BY OPERATIONAL IMPACT

1. Access control to EHR for patient identity and behavioral risk
2. Access control to emergency notification for code response
3. Access control to pharmacy security for medication management
4. Access control to visitor management for contractor and vendor credentialing

The shift from asking for more integrations to asking for interoperability is the maturity signal I have been watching for in this vertical, because it means buyers have moved past the feature checklist and into systems thinking. More please.

WHAT BUYERS ARE SELECTING FOR

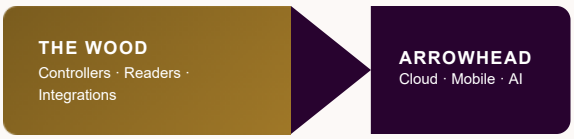
Healthcare buyers are not selecting innovation. They are selecting on consolidation credibility. A health system that has accumulated 6 to 12 or more disparate identity systems through a decade of acquisitions, a number practitioners in this vertical cite consistently as representative of the typical large network, is not looking for a new tool. It is looking for a way out of the fragmentation it already has, without ripping out every system simultaneously.

The procurement question that surfaces in mature healthcare security evaluations is not “what does this system do?” It is “what can this system connect to, and what can we stop managing separately once it does?”

Understanding what separates vendors that win these evaluations from those that lose requires a simple analogy. Think of an arrow. The arrowhead is what people see — sharp, specialized, and designed to hit the target. In access control, the arrowheads are the capabilities that draw initial attention and open the conversation: cloud management, mobile credentials, and AI-enabled configuration. They are new, they feel innovative, and they get the glory. The wood is the part no one celebrates but everyone depends on. It is the controllers, the readers, and the integrations that hold a complex multi-site environment together, give the arrow its length, balance, and strength, and make the platform indispensable over time.

Legacy vendors tend to be all wood. All wood is represented by deep infrastructure, proven reliability, but little visible innovation at the surface. Newer entrants tend to be all arrowhead. Arrowheads are sharp, modern, and exciting, but without the foundational depth to hold a complex enterprise environment together across years and acquisitions. The systems that win platform consolidation projects in healthcare are the ones that have both: enough wood to be trusted across a fragmented estate, and enough arrowheads to be chosen over the competition in the first place.

THE ARROW ANALOGY



WOOD
Deep infrastructure, proven reliability across years and acquisitions. The foundation that holds everything together.

ARROWHEAD
Modern, innovative capabilities that draw initial attention and open the procurement conversation.

WHAT WINNING LOOKS LIKE IN HEALTHCARE

Health systems are not looking for new tools. They are looking for fewer tools that do more, and vendors that can integrate with what already exists rather than requiring full replacement are the ones that win platform consolidation projects. The vendors who lose are those who arrive with a point solution and no credible path toward unified identity management across the full estate.

The systems that win consolidation projects have both wood and arrowheads, and that combination is rare enough that it is a defensible position for the vendors who have built it.

PART IV — VERTICAL SPOTLIGHT

Financial Institutions

Enterprise banks, regional institutions & the governance-first procurement model

Financial institutions are further along the platform-first transition than most of the industry realizes. Large national and global banks have been running standardized access control deployments for years, and the McDonald's model, defined as picking a solution and rolling it out everywhere, is real and common at the enterprise level.

Beneath that surface uniformity, however, there is significant complexity. Regional and community banks are lagging, mergers and acquisitions have created fragmented architectures across institutions of every size, and the convergence of physical security with cybersecurity and fraud detection is still in its early stages.

MARKET CONDITIONS

The financial services sector is undergoing two simultaneous structural changes: digitalization and branch evolution, and both have direct implications for physical access control.

Large institutions are digitally transforming their operations and treating identity governance as infrastructure. Mobile credential adoption is stronger in North America than in any other region or sector, and cloud platforms are being deployed for governance and management.

At the regional and community bank level, the gap is wide. The hardware was not built for modern platforms, and the systems are fragmented across acquisitions.

> *"Large institutes are changing: identity governance is adding value. But regional banks are lagging behind. The conversations are there but the infrastructure is not."*
>
> CIAN BOLGER, DIRECTOR OF SALES, ACRE SECURITY

Cian's quote captures the bifurcation perfectly, where the conversations are happening at the regional level but the infrastructure is not ready for what those conversations imply.

BRANCH EVOLUTION AND PHYSICAL SECURITY

Tier 1 institutions are consolidating branches, and where they are not consolidating, they are converting branches into second spaces, such as experience centers and advisory locations rather than transactional banking floors. This model introduces new security risk, as the visitors are less predictable and visitor management becomes a priority.

Regional banks are expanding. The physical branch is a brand signal, and these institutions are investing in new hardware and security infrastructure as they open locations.

EMEA is relatively stagnant in branch investment, while APAC is actively investing in new hardware for future-proofing, particularly in Singapore and Australia.

BRANCH INVESTMENT BY REGION

North America	Consolidating + Converting
APAC (SG / AU)	Actively Investing
EMEA	Relatively Stagnant

BUYER MOTIVATIONS

The dominant threat narrative in financial institutions has evolved from external robbery toward insider threat and fraud. At the largest institutions, a physical security failure that enables a data breach is a media event, and the reputational consequence of that outcome is the primary driver of senior executive attention.

The real budget trigger is not regulatory pressure, though that exists. It is an audit finding or a merger, both of which expose vulnerabilities in a way that bypasses the normal budget process and creates immediate authorization for investment.

THE AUDIT FINDING TRIGGER

Regulatory frameworks in financial services are well-established, and most institutions have a compliance foundation in place. That foundation, however, rarely generates the kind of budget authority required for a platform-level investment. What does generate it is an audit finding or an M&A transaction. Both expose vulnerabilities that the normal annual budget cycle would not surface and cannot address quickly enough. An audit finding creates an immediate remediation obligation with board visibility. An M&A transaction exposes the acquiring institution to every security gap in the acquired entity's estate, often revealing fragmentation that was invisible from the outside. Cian Bolger frames the vendor conversation correctly: stop leading with the cost of implementation, and start leading with the operational cost of managing what the institution already has, such as the staff hours, the governance gaps, the liability exposure, plus what happens if there is an incident before the next renewal cycle. That reframe is the one that moves the conversation from procurement to investment.

TECHNOLOGY ADOPTION PATTERNS

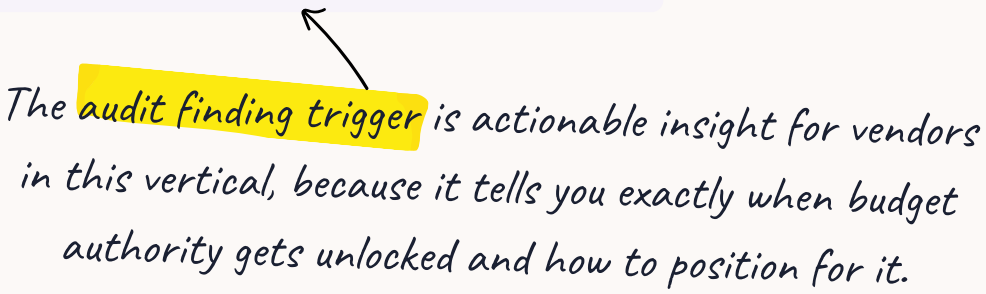
Financial institutions are moving away from proprietary vendor lock-in. Open hardware and open APIs are being requested with increasing frequency, driven by the convergence of IT and physical security governance.

Trust is being redefined in the process. The historical comfort with proprietary systems came from the trust in the vendor relationship. Open ecosystems require a different kind of trust. Trust in standards, in interoperability, and in the vendor's commitment to the ecosystem rather than to lock-in.

The credential lifecycle problem is most acute in financial institutions because the workforce includes a large contractor and third-party population with variable tenure. Offboarding failures, where contractors retain active credentials after engagement ends, are a persistent vulnerability.

TRUST REDEFINED

- Proprietary systems: trust in the vendor relationship
- Open ecosystems: trust in standards and interoperability
- Vendor commitment to the ecosystem, not to lock-in



PROCUREMENT AND BUDGETING CYCLES

Enterprise financial institutions procure access control through a centralized, standardized approach: one vendor, one platform, global rollout. This creates large, high-value contracts and long relationship tenure, and it also creates high switching costs, which is why platform selection decisions at this level are slow and deliberate.

The McDonald's model works when the chosen platform can absorb M&A activity without requiring full system replacement at acquired entities. Platforms that cannot handle that complexity lose enterprise financial institution clients over time.

Regional bank procurement is more fragmented. Decisions are made locally, standards are often absent, and the opportunity for a vendor that can bring both the platform and the standardization framework is significant.

INTEGRATION AND ECOSYSTEM

The highest-cost fragmentation in financial institutions is not hardware fragmentation. It is governance fragmentation. Multiple systems across a global portfolio make it nearly impossible to implement consistent policies, report to the board on compliance status, or respond to audit findings with confidence.

Physical and digital security integration is still relatively rare but accelerating. The alignment between physical and IT security teams is happening at the policy level first, then at the technology level.

INTEGRATION PRIORITIES

1. Identity lifecycle management for provisioning and revocation
2. Governance and reporting across multi-site deployments
3. Cybersecurity integration for correlation of physical and digital access events
4. Visitor management in branch transformation contexts

WHAT BUYERS ARE SELECTING FOR

Financial institution buyers at the enterprise level are not selecting product features. They are selecting on governance capability, integration breadth, and the demonstrated ability to absorb change, specifically acquisitions, without creating new security liability.

The three questions that surface consistently in enterprise financial institution evaluations are: Can this platform produce a consolidated compliance report across every site in our global estate? Can it onboard an acquired entity's infrastructure without requiring full replacement? And can it support an audit response without requiring manual reconciliation across multiple systems?

Vendors that can answer all three credibly earn a place in the evaluation. Vendors that can answer only one or two are typically positioned as point solutions, regardless of how strong their individual capabilities are. The financial services buyer at the enterprise level has seen enough point solutions. What they are selecting for is a platform that reduces the number of systems they have to manage, increases the governance visibility they can demonstrate, and survives the next acquisition intact.

WHAT WINNING LOOKS LIKE IN FINANCIAL INSTITUTIONS

Financial institutions are not buying access control. They are buying the ability to report compliance status to their board, pass their next audit, and absorb their next acquisition without creating a new security liability. Systems that position around those three outcomes, rather than leading with product capability, are the ones that earn a seat at the enterprise procurement table.

Governance capability, integration breadth, and the ability to absorb acquisitions are the table stakes, and the buyers in this vertical have seen enough point solutions to know the difference.

The Moment That Is Here

EDUCATION
Accelerating
Driven by mandates, mobile credential adoption, and community pressure. Buying outcomes: safer campuses, simpler operations, resilient emergency response.

HEALTHCARE
Inflecting
Leadership changes and technology-forward security executives reshaping the conversation. Buying consolidation: fewer systems, unified visibility, path out of fragmentation.

FINANCIAL INSTITUTIONS
Bifurcating
Large enterprises further along the platform journey; regional organizations still beginning. Buying governance: report, audit, and absorb change without new liability.

What unites all three is the direction of travel. Physical access control is becoming identity infrastructure, and the organizations that treat it as such will build operational advantages, compliance resilience, and technology flexibility that their peers will not.

The systems positioned to win across all three verticals share a common profile. They offer portfolio depth that spans the full lifecycle rather than a single point on the stack. They bring integration capability that absorbs existing infrastructure rather than demanding full replacement. And they can operate across geographies and institution types without imposing a one-size-fits-all architecture on buyers with fundamentally different regulatory and operational environments.

The conversation each vertical needs to hear is different in its specifics but identical in its structure. Education buyers are buying outcomes: safer campuses, simpler operations, and more resilient emergency response. Healthcare buyers are buying consolidation: fewer systems, unified visibility, and a path out of fragmentation. Financial institution buyers are buying governance: the ability to report, audit, and absorb change without creating new liability. Systems that lead with those outcomes, and use technology as the supporting evidence rather than the headline, are the ones that earn trust and close at the enterprise level.

The State of the Verticals Benchmark Report is the intelligence foundation for those conversations. The vertical spotlight reports that follow are the tools that turn intelligence into action.

Education accelerating, healthcare inflecting, and financial institutions bifurcating is the correct read on the moment, and the structural commonality underneath is the identity infrastructure thesis playing out at three different speeds. It is time to lead with outcomes: safety, consolidation, or governance... and use the technology as support rather than the headline, which is the same lesson the rest of this industry is still learning the hard way.