acre

Security

WHITEPAPER

Modernize Without Compromise: The Strategic Imperative for Open-Architecture Cloud Access Control

Table of Contents

Executive Summary: The “Third Way” in Enterprise Security	03
The Crisis of Legacy Infrastructure & Technical Debt	04
Acre Access Control: The Architecture of Freedom	08
Cybersecurity: Secure by Design, Default, and Deployment	11
Programmability and Automation: The FITS Engine	14
Financial Analysis: The ROI of Open Cloud	16
Operational Agility: Mobile and Visitor Management	19
Case Studies and Sector-Specific Applications	20
Future Trends and Innovation Readiness	22
Conclusion: The Strategic Pivot	24
Strategic Recommendations for Implementation	25
Works cited	26

Chapter 1:

Executive Summary: The "Third Way" in Enterprise Security

In the evolving narrative of physical security, enterprise leaders have long been presented with a false dichotomy: a choice between the robust, controllable, yet stagnant reliability of on-premise legacy systems, and the agile, feature-rich, yet restrictive nature of proprietary cloud "walled gardens." This binary choice has forced Chief Security Officers (CSOs) and IT Directors into a posture of compromise. They must either sacrifice innovation to maintain control over their hardware infrastructure or sacrifice hardware independence to gain the benefits of the cloud.

This white paper articulates a compelling thesis for a "Third Way": Open-Architecture Cloud Access Control. It posits that the future of enterprise security lies in a decoupled architecture where cloud-native software drives innovation while open-standard hardware ensures investment protection and operational resilience. Acre Access Control (formerly Feenics) serves as the primary case study for this paradigm shift. By leveraging non-proprietary Mercury Security hardware combined with a programmable, cloud-native infrastructure built on Amazon Web Services (AWS), organizations can achieve the "Modernize Without Compromise" ideal.

The urgency for this shift is driven by a convergence of critical factors in 2025: the escalating costs of technical debt in legacy systems, the stringent demands of new cybersecurity regulations like the EU's NIS2 Directive, and the operational necessity for programmable automation in hybrid work environments. This report provides a forensic analysis of these market drivers, a technical deep dive into the Acre architecture, and a rigorous financial model demonstrating the superior Total Cost of Ownership (TCO) of open systems. It is designed as a strategic roadmap for security leaders tasked with future-proofing their organizations against both physical threats and digital obsolescence.

Chapter 2:

The Crisis of Legacy Infrastructure and Technical Debt

To appreciate the strategic value of the Acre Access Control solution, one must first quantify the liabilities inherent in the status quo. The physical security industry is currently grappling with a massive accumulation of “technical debt” – the implied cost of future reworking required when choosing an easy solution now instead of using a better approach that would take longer. In the context of access control, this debt is not merely a metaphor; it is a tangible financial and operational burden manifesting in aging servers, unpatched firmware, and disconnected data silos.

The Crisis of the Status Quo

The Legacy Debt Spiral

30%

Of IT time spent on routine server maintenance, not innovation.

$300k+

The average cost per hour of IT downtime for enterprises.

The Proprietary Cloud Trap

100%

"Rip-and-Replace" liability when changing software providers.

Vendor lock-in holds your hardware investment hostage, creating extreme exit costs and vulnerability to supply chain fragility.

2.1 The Hidden Costs of On-Premise Systems

Legacy systems, defined by local servers and thick-client software, create a false sense of economic stability. While the initial capital expenditure (CapEx) for these systems may have been amortized years ago, the operational expenditure (OpEx) required to keep them viable is rising exponentially. This phenomenon, often described as the "maintenance spiral," diverts critical resources away from innovation and toward mere sustenance.

Legacy systems create a **false sense of economic stability.** While CapEx may be amortized, **OpEx is rising exponentially**, driven by ongoing maintenance demands.

2.1.1 The Maintenance Spiral and Resource Drain

Maintaining on-premise access control takes a sizable IT footprint, often with duplicate staff roles and overlapping maintenance tasks. But that operational redundancy doesn't mean the system itself is resilient. Most legacy systems still lack built-in failover, leaving them exposed if servers go down.

IT teams must also manage the full lifecycle of the hardware – from patching operating systems like Windows Server to maintaining SQL databases. These routine tasks consume time and energy but rarely move the business forward.

- **IT Resource Allocation:** Research indicates that IT teams in organizations with heavy on-premise footprints spend up to 30% of their time on routine maintenance tasks – patching, backups, and hardware checks – rather than strategic initiatives that drive business value. This opportunity cost is invisible on the balance sheet but crippling to organizational agility.[1]
- **Downtime Economics:** Legacy systems often rely on a single site server, with no native redundancy. If that server fails, access control may default to degraded modes, or local administration becomes impossible until the hardware is replaced. The average cost of IT downtime for enterprises can exceed $300,000 per hour—and in large organizations; this figure can reach over $1 million per hour. These costs include both lost productivity and increased risk exposure during security lapses.[3]

2.1.2 The Cybersecurity "Patch Gap"

Perhaps the most critical aspect of technical debt is the widening security gap. Legacy systems were designed in an era before the proliferation of IoT threats and sophisticated state-sponsored cyberattacks. The architecture of on-premise systems creates a structural vulnerability known as the "patch gap."

- **Manual Patching Latency:** In on-premise environments, firmware and software updates are manual processes. A security integrator must physically visit a site or remotely access a server to apply patches. This creates extended periods – weeks or even months – where known vulnerabilities remain unaddressed because scheduling and budget constraints delay the necessary maintenance.[2]

- **Legacy Protocol Vulnerabilities:** Many legacy controllers still communicate via unencrypted Wiegand protocols or use outdated encryption standards (TLS 1.0/1.1). These protocols are susceptible to "man-in-the-middle" attacks, where an adversary can intercept card data between the reader and the controller.

2.2 The Proprietary Cloud Trap: A New Form of Debt

As organizations seek to escape the constraints of legacy systems, many pivot toward cloud solutions. However, this migration often leads them into a different but equally dangerous trap: the "Proprietary Cloud." A significant portion of the ACaaS market, including competitors like Verkada, Brivo, and Openpath (Avigilon Alta), utilizes proprietary hardware architectures. While these solutions offer the benefits of cloud management, they introduce "Vendor Lock-In".[8]

2.2.1 The Economics of Vendor Lock-In

Proprietary cloud systems function as "walled gardens." The hardware (readers and controllers) communicates only with the manufacturer's specific cloud platform. This creates a situation where the customer effectively rents their security infrastructure rather than owning it.

- **Rip-and-Replace Liability:** If a customer becomes dissatisfied with the vendor's software pricing, support, or feature set, they cannot simply switch software providers. They must physically rip out every controller and reader in their facility and replace them with new hardware. This switching cost is often prohibitive, effectively holding the customer hostage to the vendor's roadmap and pricing model.[10]
- **Supply Chain Fragility:** Proprietary systems rely on a single supply chain. If the vendor experiences manufacturing delays or discontinues a product line, the customer has no alternative sources for replacement parts. This risk was starkly highlighted during recent global chip shortages, where open-architecture systems allowed integrators to source compatible hardware from multiple vendors, while proprietary users were left waiting.[11]

Feature	Open Architecture (e.g., Acre/Mercury)	ProprietaryArchitecture (e.g., Verkada, Brivo)	Strategic Implication
Hardware Compatibility	Broad support for third-party readers, locks, and sensors.	Restricted to manufacturer-specific devices.	**Flexibility:** Ability to choose best-of-breed peripherals.
Migration Path	Software can be changed without ripping out controllers.	Switching software requires full hardware replacement.	**Agility:** Protection against vendor price gouging or decline.
Supply Chain Risk	Multiple sources for hardware components (OEMs).	Single source; vulnerability to vendor-specific shortages.	**Continuity:** Reduced risk of project delays due to hardware availability.
Long-Term TCO	Lower; competitive bidding for maintenance and software.	Higher; vendor dictates pricing for hardware and licensing.	**Control:** Customer retains leverage in renewal negotiations.

The “Modernize Without Compromise” thesis argues that true modernization requires avoiding both the stagnation of on-premise legacy systems and the handcuffs of proprietary cloud systems. Acre Access Control represents the “Third Way” by combining the scalability of the cloud with the freedom of open hardware.

The "Third Way": The Acre Open Architecture

Cloud-Native Scalability (AWS)

Built on a multi-tenant, microservices architecture, Acre leverages 3+ AWS Availability Zones for resilience. A customer PoC proved massive scalability:

2M/hr Transactions Processed
(at 1.8ms avg)

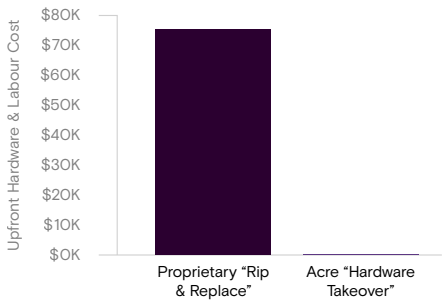
<2 sec Database Failover
(Zero throughput loss)

15M+ Cardholders
(Proven customer scale)

Open Hardware Freedom (Mercury)

Acre's "Hardware Takeover" capability allows migration from legacy systems by simply flashing existing Mercury controllers, eliminating "rip-and-replace" costs.

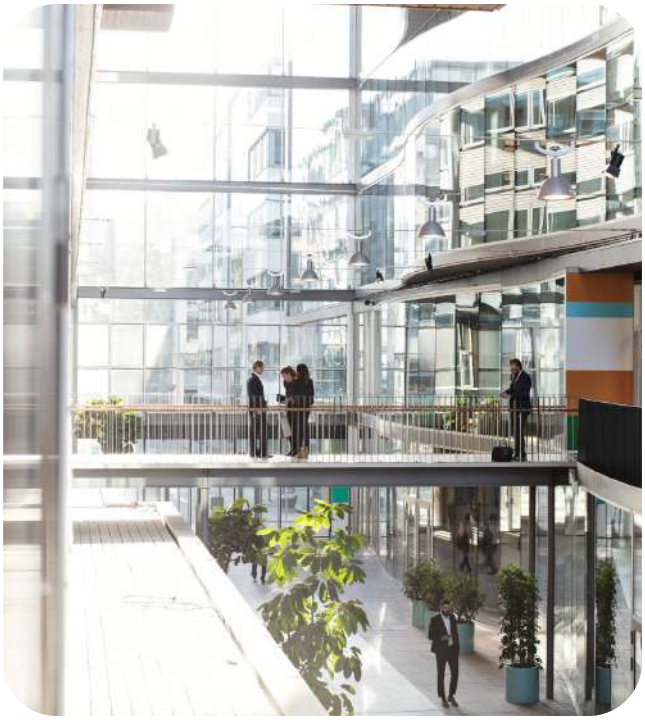
50-Door Migration Cost Example:



Chapter 3:

Acre Access Control: The Architecture of Freedom

Acre Access Control (formerly Feenics) addresses the market's dual need for cloud agility and hardware independence through a meticulously designed architecture. Unlike "cloud-masked" solutions – which essentially host legacy, single-tenant software instances on a remote virtual machine – Acre is architected as a true, multi-tenant Access Control as a Service (ACaaS) solution. This platform utilizes a cloud-native infrastructure built on Amazon Web Services (AWS) while maintaining strict compatibility with non-proprietary Mercury Security hardware.[13]



3.1 Cloud-Native Infrastructure on AWS

The decision to build on AWS provides Acre with an infrastructure that is inherently scalable, resilient, and secure. This cloud-native approach distinguishes it from competitors who may run their own data centers or use less robust hosting environments.

3.1.1 Horizontal Scalability and Microservices

The platform utilizes a microservices architecture, allowing individual components of the system (API, communications, database) to scale independently based on real-time demand.

- **Auto-Scaling Groups:** During high-traffic events – such as a shift change at a large manufacturing plant, a university campus lockdown, or a global audit of cardholder data – the system automatically provisions additional compute resources to handle the load. This ensures that user experience remains snappy and critical alarms are processed instantly, regardless of system load.[13]

Acre Access Control is a true cloud-native, multi-tenant ACaaS platform on AWS, delivering scalable performance with hardware independence.

- **Proof of Concept Validation:** Acre validated this scalability in a rigorous customer proof-of-concept (PoC). The test environment mimicked a massive deployment with 200 sites, 2,000 intelligent controllers, and 400,000 cardholders. The system was subjected to a transaction load of 10x the customer's heaviest day. The results were definitive: API servers processed 2 million transactions per hour with transaction times averaging 1.8ms, proving the platform's ability to handle enterprise-scale throughput without latency.[13]

3.1.2 High Availability and Geographic Redundancy

Reliability is the currency of trust in physical security. Acre leverages AWS Availability Zones (AZs) to ensure continuous uptime and disaster recovery.

- **Multi-AZ Deployment:** The solution runs on a minimum of three independent Availability Zones within a region (e.g., US East, Canada Central, EU West). An AZ is a discrete data center with redundant power, networking, and connectivity. If one AZ goes offline due to a power failure, fire, or natural disaster, traffic is seamlessly rerouted to the remaining healthy AZs without service interruption.[13]
- **Database Resilience:** The system utilizes MongoDB replica set distributed across these AZs. In failure simulations during the PoC, terminating the primary database server resulted in zero throughput loss, with failover to a secondary server occurring in less than 2 seconds. This level of resilience is virtually impossible to achieve with traditional on-premise SQL clusters without massive investment in hardware and licensing.[13]

Manual Patching Latency

- **Zero-Downtime Reliability:** Multi-AZ AWS setup ensures uninterrupted operations
- **Fast Failover:** Sub-2-second database failover with no performance impact.
- **Cost-Saving Migration:** Reuse Mercury hardware with a simple firmware flash, accelerating ROI.

3.2 The Mercury Security Advantage

The strategic decision to build upon Mercury Security hardware is a core differentiator for Acre. Mercury controllers (specifically the MP series) are the de facto open standard in the industry, supported by over 20 different OEM software partners[14] This "Open Architecture" is the physical embodiment of the "Modernize Without Compromise" philosophy.

3.2.1 Investment Protection via Hardware Takeover

For organizations with existing systems based on platforms like LenelS2 OnGuard, Genetec Synergis, or older RS2 deployments, moving to Acre Access Control often requires **no hardware replacement.**

- **The "Flash" Migration:** Integrators can simply "flash" the firmware of existing Mercury boards to communicate with the Acre cloud. This capability drastically reduces the upfront capital cost of migration. For a large enterprise with hundreds of doors, this "Hardware Takeover" can save hundreds of thousands of dollars in hardware procurement and labor costs, accelerating the Return on Investment (ROI) significantly.[16]

- **Future-Proofing Strategy:** This architecture also provides an exit strategy. If an organization becomes dissatisfied with Acre's software in the future, they retain the freedom to switch to another Mercury-partnered platform without discarding their hardware investment. This keeps the software vendor (Acre) accountable and focused on continuous innovation, as they cannot rely on hardware lock-in to retain customers.[9]

3.2.2 Edge Intelligence and Offline Survivability

While the cloud provides centralized management and analytics, the Mercury hardware ensures local survivability. The system's intelligence (access rules, cardholder databases, schedules, triggers and procedures, holidays, etc.) is pushed down to the local controllers.

- **Offline Operation:** If the internet connection to the site is severed, the local Mercury controllers continue to make access decisions, log events, and execute schedules autonomously. They do not default to a "locked" or "open" state but continue to function based on the last known configuration. Once connectivity is restored, all buffered events (up to 50,000 transactions on standard boards like the MP1502) are automatically synchronized to the cloud database, ensuring no data loss.[18]
- **Mercury MP Series Capabilities:** Acre supports the latest Mercury MP series controllers, which feature enhanced cybersecurity protections (including crypto chips for secure key storage) and support for advanced OSDP (Open Supervised Device Protocol) features. This ensures that the hardware layer remains as modern and secure as the software layer.[19]

Chapter 4:

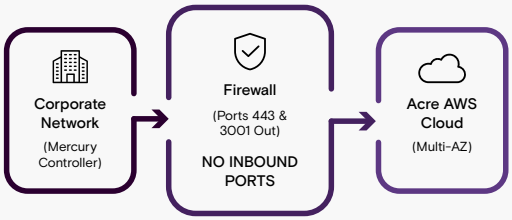
Cybersecurity: Secure by Design, Default, and Deployment

In 2025, physical security systems are no longer just door locks; they are IoT endpoints on the corporate network, making them prime targets for cybercriminals. A breach in an access control system can serve as a gateway to the wider corporate network or result in the theft of sensitive biometric and identity data. Acre Access Control employs a "Secure by Design" philosophy, explicitly adhering to the Microsoft SD3+C model (Secure by Design, Secure by Default, Secure in Deployment, and Communications).[13]

Secure by Design, Default, and Deployment

Outbound-Only Network Security

Acre eliminates the #1 network vulnerability of on-premise systems: open inbound firewall ports. Controllers only make outbound connections, drastically reducing the attack surface.



Enterprise-Grade Protections

End-to-End Encryption

TLS 1.3 encryption for data in transit and AES-256 for data at rest, managed via AWS Key Management Service.

Identity & Access Management

Enforce Multi-Factor Authentication (MFA) and integrate with SAML 2.0 providers (Okta, Azure AD) for Single Sign-On (SSO).

Verified & Compliant

Audited to ISO 27001:2022 standards and regularly pen-tested by third-party firms like Bishop Fox to meet NIS2 and GDPR requirements.

4.1 Encryption and Data Protection Architecture

Data security within the Acre ecosystem is enforced at three critical stages: in transit, at rest, and in use. This defense-in-depth strategy ensures that data remains protected even if one layer of defense is compromised.

Acre Access Control is **built Secure by Design**, using TLS 1.3 and AES-256 encryption to protect access data across the network, cloud, and devices.

4.1.1 TLS 1.3 and AES-256 Encryption

- **Communication Encryption:** All data moving between the Mercury controllers and the cloud is encrypted using TLS 1.2 or 1.3 (depending on the specific controller generation, with MP series supporting 1.3). This prevents eavesdropping and replay attacks where an attacker might capture a “door open” command and replay it later. Unlike legacy systems that often rely on proprietary, obfuscated protocols, Acre uses standard, globally vetted cryptographic protocols.[13]
- **Data at Rest:** Data stored within the AWS MongoDB clusters is protected by AES-256 bit encryption. Acre utilizes the AWS Key Management Service (KMS) to create and manage cryptographic keys. This ensures that keys are rotated regularly and that data remains protected.

4.1.2 Outbound-Only Communication Architecture

One of the most significant security advantages of Acre’s cloud architecture is its elimination of inbound firewall ports. Traditional on-premise systems often require IT departments to open inbound ports on the corporate firewall to allow for remote access or mobile app connectivity. This practice creates “holes” in the perimeter that can be exploited by attackers (e.g., via Shodan scans).

- **Port 443 & 3001:** Acre Access Control utilizes an outbound-only communication model. Mercury controllers initiate an outbound connection to the Acre cloud over standard ports (HTTPS Port 443 and Port 3001). The firewall permits this outbound traffic while blocking all unsolicited inbound connection attempts. This architecture eliminates the need for port forwarding, VPNs, or static public IP addresses for controllers, significantly reducing the network attack surface.[13]

4.2 Identity and Access Management (IAM)

The platform incorporates enterprise-grade IAM features to prevent unauthorized system access, addressing the "human element" of security risk.

- **Multi-Factor Authentication (MFA):** MFA is not just an option but a strongly encouraged standard for all users. Acre supports time-based one-time passwords (TOTP) generated by standard authenticator apps like Google Authenticator, Duo, or Microsoft Authenticator. This ensures that a stolen password alone is insufficient for an attacker to gain access to the system.[13]
- **Single Sign-On (SSO):** Integration with SAML 2.0 identity providers (such as Okta, Azure AD, or Ping Identity) allows organizations to centralize user lifecycle management. When an employee leaves the company and their Active Directory account is disabled by HR/IT, their access to the Acre administration portal is immediately and automatically revoked. This eliminates the risk of "orphan accounts"—former employees retaining access to security systems simply because an administrator forgot to manually delete their user account.[22]

Identity & Access Management

- **Strong User Security:** MFA with authenticator apps prevents access from stolen passwords.
- **Centralized Access Control:** SSO via SAML 2.0 integrates with enterprise identity providers.
- **Zero Orphan Accounts:** Automatic access revocation when employee accounts are disabled.

4.3 Regulatory Compliance: NIS2, GDPR, and SOC2

The regulatory landscape for physical security is shifting dramatically. The European Union's NIS2 Directive, effective October 2024, places stringent cybersecurity requirements on critical infrastructure entities, expanding the scope to include supply chain security and mandatory incident reporting.[23]

- **Supply Chain Vetting:** Acre's reliance on AWS (the largest cloud provider with extensive compliance certifications) and Mercury Security (proven, non-proprietary hardware) assists organizations in meeting NIS2's supply chain due diligence requirements. Customers inherit the security posture of these top-tier partners.
- **Incident Response Reporting:** The platform's centralized logging and health monitoring capabilities provide the visibility needed for the rapid incident reporting mandated by NIS2 (which requires an "early warning" within 24 hours of becoming aware of a significant incident). Acre's architecture allows for immediate detection of controller offline status or anomalous access patterns, enabling rapid compliance.[25]
- **Penetration Testing:** Acre engages third-party security firms to conduct regular penetration testing on the platform. This proactive approach identifies vulnerabilities before they can be exploited by malicious actors, ensuring that the software remains hardened against evolving threats.[13]

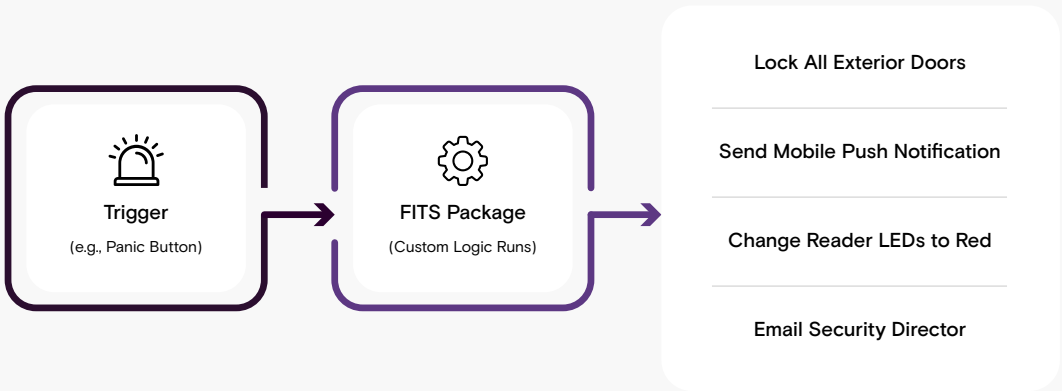
Chapter 5:

Programmability and Automation: The FITS Engine

One of the most distinct features of Acre Access Control, distinguishing it from commoditized access platforms, is the **Functional Integration Toolkit Scripts (FITS)**. While most access control systems rely on rigid, pre-configured logic (e.g., "if door opens, trigger alarm"), FITS introduces a layer of programmable logic that allows for complex, bespoke workflows without the need for custom firmware development or manufacturer intervention.

Custom Workflows, Your Way

FITS packages make it easy to automate approvals, sync data, and create custom workflows that link access events to your broader operations - without changing your core system. Available in Gallery, the marketplace for FITS, they're ready to extend what Acre Access Control can do.



5.1 Advanced Logic Scenarios

- **Dynamic Threat Level Management:** A standard system might have a simple "lockdown" button. With FITS, a "Panic Button" input can trigger a sophisticated global lockdown script. This script could not only lock all exterior doors but also change reader LED colors to red to visually warn staff, send push notifications to all mobile app users, email the security director, and trigger a relay to cut power to automatic door operators—all executing instantly across multiple sites.
- **Environmental Integration:** FITS allows the access system to act on environmental data. A script can monitor a temperature sensor in a server room via an auxiliary input. If the temperature exceeds a critical limit, the system can automatically unlock the server room door for emergency ventilation (if safe) or trigger an integration with the Building Management System (BMS) to ramp up HVAC cooling.[29]

FITS turns rigid access control into intelligent, programmable workflows, enabling real-time, multi-system responses without custom firmware or vendor dependency

5.2 API-First Integration Strategy

Acre provides a comprehensive RESTful API, exposing every function of the system to third-party developers. This contrasts with competitors who often restrict API access to premium tiers or offer limited "partner-only" integration paths.

- **Ecosystem Connectivity:** The API facilitates seamless integration with core business systems such as HR platforms (Workday, SAP), Video Management Systems (Milestone, Avigilon, Hanwha), and visitor management platforms.
- **Automated Onboarding Example:** When a new employee is added to the corporate HR system, the API can automatically create their profile in Acre Access Control, assign access levels based on their department and location metadata, and email them a mobile credential invitation. This automation eliminates manual data entry errors and ensures that new hires have immediate, correct access on day one.[30]
- **The Gallery:** Acre has fostered a developer ecosystem through "The Gallery," a repository where partners, community members and Acre can share FITS packages and integrations. This allows organizations to leverage pre-built solutions for common problems (e.g., a specialized Bosch Intrusion panel integration package) rather than coding from scratch, accelerating deployment times.[29]

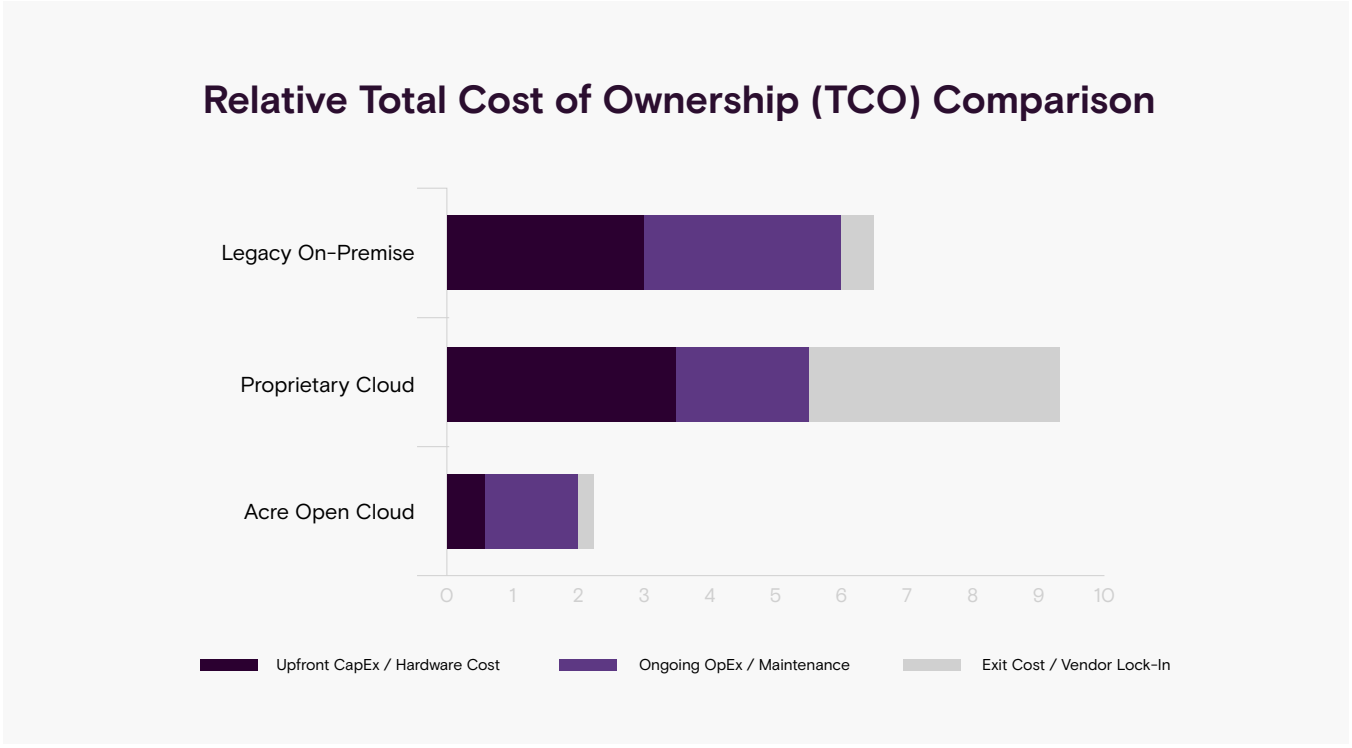
Chapter 6:

Financial Analysis: The ROI of Open Cloud

Transitioning to Acre Access Control is not merely a security decision; it is a strategic financial move. The shift from a CapEx-heavy model to an OpEx subscription model aligns with modern IT budgeting preferences, but the true financial advantage lies in the holistic Total Cost of Ownership (TCO) analysis over a 5-7 year lifecycle.

6.1 TCO Comparison: Cloud vs. On-Premise vs. Proprietary Cloud

To understand the economic impact, we must compare Acre against both legacy on-premise systems and proprietary cloud competitors.



6.1.1. Legacy On-Premise Model:

- **Upfront CapEx:** Heavy. Requires purchase of physical servers, OS licenses (Windows Server), database licenses (SQL), application software licenses, and proprietary controllers.
- **Hidden OpEx:** High maintenance costs. IT staff hours spent on patching, backups, and troubleshooting. Energy costs for running servers 24/7/365.
- **Depreciation:** Hardware depreciates rapidly, typically requiring a refresh cycle every 3-5 years.

Legacy systems create a **false sense of economic stability.** While CapEx may be amortized, **OpEx is rising exponentially**, driven by ongoing maintenance demands.

6.1.2 Proprietary Cloud Model (e.g., Brivo, Verkada):

- **Upfront CapEx:** Moderate to High. Requires purchasing new, proprietary cameras & controllers.
- **Migration Cost:** High. If switching from a legacy system, all existing hardware must be ripped out and replaced.
- **Exit Cost:** Extreme. If the customer leaves the vendor, the hardware becomes useless e-waste.

6.1.3 Acre ACaaS Model (Open Architecture):

- **Upfront CapEx:** Low. The primary cost is installation, labor and field hardware (readers/locks). If Mercury hardware exists, controller costs are near zero.
- **OpEx:** Predictable annual or monthly subscription fees based on the number of managed doors.
- **Financial Benefit:** This shifts security from a capital-intensive project to a predictable operating expense, improving cash flow visibility.[32]

6.2 The "Hardware Takeover" Savings: A Real-World Calculation

Consider a mid-sized facility with 50 doors currently utilizing a legacy Lenel system with Mercury controllers. The organization wants to migrate to the cloud.

6.2.1 Scenario A: Proprietary Cloud Migration (Rip-and-Replace)

- **New Controllers:** ~$1,500 per door (hardware + labor) x 50 doors = **$75,000.**
- **Disruption:** Significant downtime during rewiring and testing.
- **Total Hardware CapEx: $75,000.**

6.2.2 Scenario B: Acre / Mercury Takeover

- **New Controllers: $0** (Existing boards are reused).
- **Firmware Flash Labor**: **$0** labor for Acre / Mercury takeovers completed by Acre.
- **Disruption:** Minimal.
- **Total Hardware CapEx: $0**

Result:

The Acre solution delivers an immediate **capital avoidance of $75,000** in this scenario. This hardware savings can effectively subsidize the SaaS subscription costs for several years, accelerating the ROI significantly compared to closed competitors.[16]

6.3 The Cost of Downtime Comparison

- **Legacy System:** A server failure requires IT to procure new hardware, reinstall the OS and software, and restore from backups (if they exist). This can lead to days of downtime. At an estimated cost of even $10,000/hour for a mid-sized enterprise, a 24-hour outage costs **$240,000**.
- **Acre Cloud:** With 99.99% uptime SLAs and triple-redundancy in AWS, the risk of prolonged system-wide failure is negligible. The cost avoidance of a single major outage can justify the annual subscription cost of the platform.[35]

Chapter 7:

Operational Agility: Mobile and Visitor Management

The modern workforce is hybrid, mobile, and dynamic. Security tools must reflect this reality, moving beyond the static “badge and reader” model to interactive, user-centric experiences.

7.1 Acre Access Control Mobile App

The mobile application is designed to serve two distinct user groups: administrators & general users.

- **Admin on the Go:** Security managers can view real-time alarms, acknowledge events, and remotely unlock doors from their smartphones. This allows a security director to respond to a “Door Forced Open” alarm at a remote site immediately, verifying the situation via integrated video and resetting the alarm without needing to drive to a command center.[36]
- **Mobile Credentials:** The app supports Bluetooth Low Energy (BLE) and NFC, allowing users to unlock doors by presenting their phone or utilizing background scanning (keeping the phone in a pocket). This aligns with the “mobile-first” expectations of modern employees and reduces the recurring cost and environmental impact of issuing plastic cards.[37]

7.2 Visitor Management Integration

Acre offers native integration with Acre Visitor Management (and partners like Fast-Pass and Acre Identity by TDS), creating a seamless workflow for guest access.

- **The Workflow:** A host pre-registers a visitor in the web portal. The visitor receives a QR code via email with instructions. Upon arrival, they scan the code at a self-service kiosk, which captures their photo, prints a badge, and automatically activates their access rights for the specific duration of the meeting.
- **Security Impact:** This process eliminates the insecure “clipboard and pen” logbook, ensures that all visitors are screened against watchlists, & guarantees that visitor access rights expire automatically, preventing unauthorized re-entry.[38]

Chapter 8:

Case Studies and Sector-Specific Applications

Acre Access Control's flexibility makes it suitable for diverse verticals, but it excels in environments requiring complex segmentation, high availability, & scalability.

8.1 Media + Entertainment: Securing a Global Footprint in the Cloud

A global media and entertainment company chose Acre to modernize access across 150+ sites worldwide — from studio lots to offices to broadcast centers.[40]

- **The Challenge:** Years of creative expansion led to a patchwork of over 20 disconnected access systems. Security standards varied, scaling was slow, and evolving regulations like GDPR and CCPA were difficult to meet across such a fragmented landscape.
- **The Solution:** With Acre's cloud-native platform, the company began consolidating systems into a unified global architecture. A centralized cardholder database simplified identity management across sites. The platform's flexibility supported phased rollouts, while upcoming Dot Global features helped localize data by region for privacy compliance.
- **Scalability Feature:** Acre's cloud foundation enables remote updates, faster deployment across new sites, and seamless integrations with future technologies – offering a scalable, compliant, and future-ready foundation for security transformation at global scale.

8.2 Healthcare: Compliance and Continuity

In healthcare environments, system downtime can impact patient care, making reliability paramount.

- **High Availability:** The multi-AZ redundancy of the Acre platform ensures that access to sensitive areas like pharmacies, NICUs, and server rooms is never compromised by a single server failure.
- **Regulatory Compliance:** Granular reporting and immutable audit logs meet HIPAA requirements for tracking access to areas containing electronic protected health information (ePHI) and physical records. The system can prove exactly who entered a records room and when.[42]

8.3 Industrial and Manufacturing: The Specialist Steel Company

A specialized steel manufacturing company faced the challenge of replacing a 25-year-old legacy access control system that was becoming unmanageable.

- **The Challenge:** The aging infrastructure was a security risk and lacked remote management capabilities. The company needed a centralized view of multiple sites.
- **The Solution:** Partnering with OLS Limited, the company migrated to Acre's cloud-based solution (ACT365). This allowed them to centralize management of all sites into a single pane of glass.
- **The Result:** The migration streamlined operations, reduced the need for on-site IT maintenance, and provided the ability to integrate with their Time & Attendance software, improving payroll accuracy and operational efficiency.[44]

Chapter 9:

Future Trends and Innovation Readiness

The security industry is on the cusp of an AI and data revolution. Choosing a cloud-native platform like Acre positions organizations to capitalize on these trends rather than being left behind.

9.1 AI and Analytics

Cloud platforms are uniquely positioned to leverage Artificial Intelligence (AI) because they have access to vast amounts of compute power and data.

- **Anomaly Detection:** Acre can introduce algorithms that analyze access patterns to detect anomalies. For example, "Why is this user, who normally works 9-5, accessing the server room at 3 AM?" The system can flag this behavior for review, identifying potential insider threats that rule-based systems would miss.
- **Generative AI:** Acre is exploring the use of generative AI (via acquisitions like REKS) to simplify system interaction, potentially allowing operators to query the system using natural language (e.g., "Show me all access denied events at the North Gate last night").[45]

9.2 Mobile Wallet Evolution

As Apple Wallet and Google Wallet credentials become standard, cloud platforms can provision these credentials over-the-air instantly.

- **Acre One App:** The evolution of the Acre One app positions customers to adopt these technologies seamlessly. Unlike on-premise systems that might require server upgrades to support new credential formats, the cloud platform can support new wallet standards via a software update.[46]

9.3 Sustainability and ESG

Cloud migration contributes to corporate sustainability goals.

- **Energy Efficiency:** Moving workloads to hyperscale cloud providers like AWS (which is targeting 100% renewable energy usage) is significantly more carbon-efficient than running inefficient, cooling-intensive on-premise server rooms at every facility.
- **E-Waste Reduction:** The ability to reuse Mercury hardware prevents tons of electronic waste (plastic, silicon, heavy metals) from entering landfills, a key metric for corporate Environmental, Social, and Governance (ESG) reports.[47]

Cloud platforms enable instant Apple and Google Wallet credential provisioning, with Acre One adopting new standards via simple software updates—no server upgrades required.

Chapter 10:

Conclusion: The Strategic Pivot

The analysis presented in this report leads to a singular, robust conclusion: The traditional dichotomy between “secure on-premise” and “agile cloud” is false. The strategic choice facing enterprise leaders is between **closed architectures** that create technical debt and risk, and **open architectures** that create value and resilience.

Acre Access Control validates the “Modernize Without Compromise” thesis by delivering the operational velocity of the cloud while respecting the sovereignty of the customer’s hardware investment.

- For the **CSO**, it offers a “sleep-well-at-night” cybersecurity posture, backed by AWS resilience and Bishop Fox testing.
- For the **CFO**, it offers predictable costs, significant CapEx avoidance through hardware takeover, and asset preservation.
- For the **IT Director**, it eliminates the drudgery of server maintenance and empowers the organization with API-driven automation.

In a world defined by NIS2 compliance, dynamic cyber threats, and the need for operational efficiency, Acre Access Control is not just a tool for opening doors – It is a foundational element of the resilient, modern enterprise. The time to transition is now, before the hidden costs of legacy systems compound into critical failures. By choosing Acre, organizations secure not just their physical premises, but their future freedom of action.

Chapter 11:

Strategic Recommendations for Implementation

For organizations convinced by the data and ready to consider a migration to Acre Access Control, the following strategic steps are recommended to ensure a smooth transition:

- **Audit Existing Hardware:** Conduct a comprehensive site survey to identify existing Mercury controllers (EP, LP, or MP series). Document firmware versions to confirm compatibility and maximize "takeover" savings.
- **Define Automation Rules:** Before deployment, map out manual security processes (e.g., "disable access when employee is terminated," "unlock lobby for events"). Plan FITS scripts or API integrations to automate these workflows from Day 1.
- **Leverage the Cloud for Cyber-Resilience:** Utilize the migration as an opportunity to offload cyber risk. Ensure the security team reviews Acre's SOC 2 and ISO 27001 documentation to streamline internal compliance audits.
- **Plan for Mobile Adoption:** Roll out mobile credentials in phases, starting with high-frequency users (staff) to reduce the long-term cost of plastic card procurement and management.
- **Engage Certified Partners:** Work with certified Acre integrators who have specific experience with Mercury hardware takeovers to ensure a seamless cutover with minimal downtime.

By following this roadmap, organizations can execute a modernization strategy that delivers immediate value while laying the groundwork for a secure, adaptable future.

The Future is Within Reach.

By avoiding the "false dichotomy" of legacy vs. proprietary systems, Acre Access Control provides a clear path to modernize your security infrastructure without compromising on cost, flexibility, or cybersecurity.

To learn more, download the full white paper at: acresecurity.com/whitepapers-reports

Works cited

01 Understanding the differences in cloud vs on-premise server security - Kisi, accessed November 25, 2025, https://www.getkisi.com/blog/cloud-vs-server-on-premise-security

02 The Hidden Costs and Risks of Legacy Systems: Why Modernization Matters - Morphis Tech, accessed November 25, 2025, https://morphis-tech.com/blog/the-hidden-costs-and-risks-of-legacy-systems/

03 What is the cost of IT downtime for small businesses in 2025? - E-N Computers, accessed November 25, 2025, https://www.encomputers.com/2024/03/small-business-cost-of-downtime/

04 Calculating the cost of downtime | Atlassian, accessed November 25, 2025, https://www.atlassian.com/incident-management/kpis/cost-of-downtime

05 The Hidden Costs of Legacy Systems: Why It's Time to Modernize | CentralSquare, accessed November 25, 2025, https://www.centralsquare.com/resources/articles/the-hidden-costs-of-legacy-systems-why-its-time-to-modernize

06 Beyond Badge Readers: The True Cost of Legacy Access Control and the Pathway to True Digital Identity - Alcatraz AI, accessed November 25, 2025, https://rock.alcatraz.ai/blog/true-cost-of-legacy-access-control

07 The Vulnerability of Legacy Access Control Systems: Is Your Business at Risk?, accessed November 25, 2025 https://oliverfps.com/2023/11/the-vulnerability-of-legacy-access-control-systems-is-your-business-at-risk/

08 Evaluating Cloud-Based Commercial Access Control Systems | 2727 Coworking, accessed November 25, 2025, https://2727coworking.com/articles/commercial-access-control-systems

09 Open Access Control vs. Proprietary Access Control - Genea, accessed November 25, 2025, https://www.getgenea.com/blog/open-access-control-vs-proprietary-access-control/

10		The Risks of Proprietary Access Control Door Hardware - Genea, accessed November 25, 2025, https://www.getgenea.com/blog/the-risks-of-proprietary-access-control-door-hardware-for-commercial-buildings/
11		Cloud Migration Horror Stories | What Enterprises Can Learn from Real Failures, accessed November 25, 2025, https://articles.hashroot.com/cloud-migration-horror-stories-what-enterprises-can-learn-from-real-failures/
12		The Downsides to Proprietary Security Equipment, accessed November 25, 2025, https://www.vulcansecuritysystems.com/proprietary-security-equipment-downsides/
13		Whitepaper_Feenics-aAC white paper on Scalability in the Cloud.docx
14		Open Architecture for the new Mercury Controllers, accessed November 25, 2025, https://www.mercury-security.com/why-open-architecture-matters/
15		Total Cost of Ownership (TCO) for Access Control Systems | Dash Door, accessed November 25, 2025, https://www.dashdoor.com/wp-content/uploads/2014/03/RS2-Total-Cost-of-Ownership-for-Access-Control-Systems-13-0411.pdf
16		Access Control Access Control Takeover - Whitepaper - Genea, accessed November 25, 2025, https://www.getgenea.com/downloads/access-control-software-takeover/
17		Feenics Achieves Platinum Partner Status With Mercury Security - SDM Magazine, accessed November 25, 2025, https://www.sdmmag.com/articles/93627-feenics-achieves-platinum-partner-status-with-mercury-security
18		Overcoming the 5 Major Challenges in Access Control Systems with Feenics by Acre security, accessed November 25, 2025, https://www.acresecurity.com/blog/overcoming-the-5-major-challenges-in-access-control-systems-with-feenics-by-acre-security
19		New Mercury MP Controllers are Supercharging Security - Genea, accessed November 25, 2025, https://www.getgenea.com/blog/mercury-mp-controllers-are-supercharging-security/

20 Mercury Intelligent Access Controllers | Proven and Reliable, accessed November 25, 2025, https://www.mercury-security.com/controllers/

21 Acre Access Control Data Specs Sheet, accessed November 25, 2025, https://acre.my.site.com/knowledgearticles/s/article/Acre-Access-Control-Data-Specs-Sheet

22 Feenics Access Control: Overview & Guide (2024) - Safe and Sound Security, accessed November 25, 2025, https://getsafeandsound.com/blog/feenics-access-control/

23 NIS2 Requirements for Access Control: Is Your System Ready? - HID Global, accessed November 25, 2025, https://blog.hidglobal.com/your-physical-access-control-system-ready-nis2-heres-what-you-need-know

24 NIS2 Directive: securing network and information systems | Shaping Europe's digital future, accessed November 25, 2025, https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

25 Why NIS2 Makes Physical Infrastructure Security Non-Negotiable - Nlyte Software, accessed November 25, 2025, https://www.nlyte.com/blog/why-nis2-makes-physical-infrastructure-security-non-negotiable/

26 VB0155 - Acre Security Our Commitment to EU NIS2 Directive Compliance and Supporting Your Requirements, accessed November 25, 2025, https://23532239.fs1.hubspotusercontent-na1.net/hubfs/23532239/Legal%20documents/VB0155%20-%20Acre%20Security%20Our%20Commitment%20to%20EU%20NIS2%20Directive%20Compliance%20and%20Supporting%20Your%20Requirements.pdf

27 Welcome to the New Era of Access Control Technology with Acre, accessed November 25, 2025, https://www.acresecurity.com/blog/welcome-to-the-new-era-of-access-control-technology-with-acre

28 Why Access Control Needs an Upgrade — And How FITS Is Leading the Way - YouTube, accessed November 25, 2025, https://m.youtube.com/shorts/45aNza0hyqE

29 Introducing the Acre Gallery - Acre Security, accessed November 25, 2025, https://acresecurity.com/blog/introducing-the-acre-gallery

30 Enterprise Identity Management: Why Your Business Needs It - Acre Security, accessed November 25, 2025, https://acresecurity.com/blog/enterprise-identity-management-why-your-business-needs-it

31 Mastering Gallery: acre's App Store for Smarter Access Control - YouTube, accessed November 25, 2025, https://www.youtube.com/watch?v=i2RZIxXg668

32 Compare Cloud-Based vs. On-Premise Access Control Security Systems, accessed November 25, 2025, https://www.acresecurity.com/blog/cloud-vs-on-prem

33 Key differences between on-premise and cloud-based access control systems - Security 101, accessed November 25, 2025, https://www.security101.com/blog/sanfrancisco/key-differences-between-on-premise-and-cloud-based-access-control-systems

34 Proprietary vs. Open Hardware - Open Access Control System - Genea, accessed November 25, 2025, https://www.getgenea.com/blog/proprietary-vs-open-hardware/

35 Access Control Solutions | Acre Security, accessed November 25, 2025, https://www.acresecurity.com/en-gb/access-control

36 acre Access Control Mobile - App Store, accessed November 25, 2025, https://apps.apple.com/us/app/acre-access-control-mobile/id1288737717

37 Discover the Future of Security with Mobile Access Control Systems, accessed November 25, 2025, https://www.acresecurity.com/blog/discover-the-future-of-security-with-acre-mobile-access-control-systems

38 Acre Security Announces New Partnership between Feenics and FAST-PASS for Enhanced Visitor Management and Access Control Solutions, accessed November 25, 2025, https://acresecurity.com/blog/acre-security-announces-new-partnership-with-fast-pass-for-enhanced-visitor-management

39 Acre Security Elevates Access Control with Seamless Integration of its Enterprise Visitor Management Solution and Feenics Access Control, accessed November 25, 2025, https://www.acresecurity.com/blog/acre-security-elevates-access-control-with-seamless-integration-of-its-enterprise-visitor-management-solution-and-feenics-access-control

40 Acre Security Safeguards 69,000 Students Across Three Major Universities Following Campus-Wide Access Control Deployment, accessed November 25, 2025, https://www.acresecurity.com/blog/campus-wide-access-control-deployment

41 Three U.S. Universities Install Acre Security Access Control Platform -- Spaces4Learning, accessed November 25, 2025, https://spaces4learning.com/articles/2025/08/21/acre-security-access-control-platform.aspx

42 Healthcare Security. Acre Solutions., accessed November 25, 2025, https://www.acresecurity.com/industries/healthcare

43 Hospital Access Control: How to Ensure Safety in Healthcare Facilities - Acre Security, accessed November 25, 2025, https://www.acresecurity.com/blog/hospital-access-control-how-to-ensure-safety-in-healthcare-facilities

44 Streamlining Access Control Processes through Cloud Migration at a Specialist Steel Company - Acre Security, accessed November 25, 2025, https://acresecurity.com/case-study/streamlining-access-control-processes-through-cloud-migration-at-a-specialist-steel-company

45 ACRE news | Security news - SourceSecurity.com, accessed November 25, 2025, https://www.sourcesecurity.com/news/co/acre.html

46 ACRE launches the Feenics One Mobile App - International Security Journal, accessed November 25, 2025, https://internationalsecurityjournal.com/feenics-one-mobile-app/

47 The Hidden Costs of E-Waste - West Coast Computer Recycler, accessed November 25, 2025, https://www.wcrecycler.com/blog/the-hidden-costs-of-e-waste

acre

Security

Talk to our team here.

Press inquiries? Reach us at press@acresecurity.com