SwiftConnect

The Access Disconnect

Why Fragmentation Is Costing Enterprises More Than They Think

Contents

01 The Access Disconnect

02 The Hidden Tax of Fragmentation

03 What It's Costing IT and Security Teams

04 Why Fragmentation Persists

05 From Fragmentation to Control

1. The Access Disconnect

In today's enterprises, physical access generally works. Employees badge in, doors unlock, offices stay secure.

But here's the catch: all the pieces of the access puzzle work separately. Badges, provisioning systems, building controllers – yes, they all function. But they don't operate as one. That fragmentation creates a subtle yet persistent drag on productivity, security, and cost.

> Portfolios and enterprises often have various access control systems, directories, mobile credentials, and building management tools – none of them designed from the ground up to operate as a unified access layer.

Instead, IT and security teams find themselves manually stitching together workflows, juggling provisioning across multiple systems, dealing with lost or stale credentials, and scrambling to deprovision access when someone leaves or changes roles.

The result is slower onboarding and offboarding, higher credential-costs, overlooked access changes, and increased risk exposure. Worse, every minute spent managing this complexity is time not spent advancing initiatives that matter: hybrid work enablement, real-time identity-based access, seamless experiences from street to seat.

This guide will help you quantify the cost of the access disconnect. We bring together data on manual provisioning, lost credentials, siloed systems and their impact – and show how unification, not just replacement, can help regain control.

2. The Hidden Tax of Fragmentation

Here are a few stats that should give any leader pause:

$250 per badge — the estimated total cost of replacing a lost or stolen access badge, including admin time and material fees.

10% of badges are lost annually in organizations with over 1,000 employees, leading to significant recurring costs and security gaps.

$4.45 million — the average cost of a data breach globally, with compromised credentials being a top attack vector.

328 days — the average time it takes to identify and contain a breach involving stolen or compromised credentials.

$3.78 million per year — what organizations spend (on average) due to inefficiencies in managing multiple identity systems.

34% of former employees retain access to systems or data after leaving a company, exposing organizations to ongoing risk.

These numbers reflect a common reality: managing access across fragmented systems is slow, expensive, and error-prone.

> When credentials are lost, badges need replacing, or user roles change, the process of updating access typically spans multiple tools and teams. Provisioning often happens manually. Offboarding is inconsistent. Changes fall through the cracks.

None of this is unusual. In fact, it’s the norm. But it adds up: in labor hours, in security risk, in mounting administrative workload.

And because the work is buried in everyday processes, its cost rarely shows up on a balance sheet. It’s a drain that hides in plain sight.

This is the hidden tax of fragmentation. Most organizations are paying it. But few realize how much.

3. What It's Costing IT and Security Teams

Even when access "works," the day-to-day cost of fragmentation falls squarely on IT and Security teams. Manual workflows, disconnected systems, and unclear ownership lead to inefficiencies that drain time, resources, and focus from higher-priority initiatives.

Here's how the damage typically breaks down:

Team	Impact of Fragmentation	Examples
IT Operations	High ticket volume, manual provisioning/deprovisioning, time wasted on badge management.	Resetting access for rehires, chasing down lost badges, bulk provisioning across systems.
Security	Increased risk exposure, slower response to access changes, audit gaps.	Delayed revocation after terminations, inconsistent access policies across PACS environments.
Identity & IAM	Difficulty syncing entitlements, misalignment between IdP and physical access.	Identity changes not reflected in building access, leading to overpermissioning.
Facilities	Reliance on IT for access control support, inefficient badge printing, limited visibility.	Managing building access manually via spreadsheets and work orders.
Help Desk / Support	Constant user issues tied to credentials, access delays, and badge loss.	"I can't get into the office" tickets, long lines at facilities desks for badge re-issues.

These challenges rarely make headlines, but they take a daily toll. Every lost hour, delayed deprovisioning, or misaligned entitlement chips away at efficiency — and puts added pressure on teams already stretched thin.

Over time, this doesn't just affect operations. It affects morale, retention, and the ability to focus on strategic work that actually moves the business forward.

4. Why Fragmentation Persists

Most enterprises didn't set out to build fragmented access systems. They arrived there gradually — through acquisitions, shifting real estate footprints, evolving IT stacks, and the natural sprawl that comes with growth.

Identity systems, access control systems , mobile credentials, tenant platforms, and badge printers all entered the picture at different times, often driven by local needs or short-term decisions. One building uses a LenelS2 access control system, another uses an AMAG system. One site relies on plastic badges, another is trialing mobile. Facilities teams manage one set of rules, IT manages another. Everything functions — but nothing is connected.

Because each piece works independently, integration was always something to deal with "later." In many organizations, that "later" never came.

> To cope with fragmentation, teams built workarounds. Spreadsheets to track badge status. Shared inboxes for provisioning requests. An interface to sync identity changes. Workflows that depend more on memory than documentation. Much of this complexity is held together by institutional knowledge — the kind that walks out the door when key people leave.

Over time, the access environment starts to feel more fragile than flexible. Every change requires double-checking multiple systems. Every onboarding or offboarding step becomes a potential gap. What should be a simple process — assigning or revoking access — turns into a coordination exercise across departments and platforms.

This isn't about legacy tech in the traditional sense. Most of the systems in place are still actively supported. The issue is that they were never built to operate in concert. There's no shared language between them, no common identity layer, no orchestration.

And while the inefficiencies are well understood, fixing them often feels too risky or time-consuming to justify. Integrations are seen as complex. Upgrades are delayed because the current setup is "good enough." So the organization lives with the friction — not because it's invisible, but because it's familiar.

The result is an access environment that looks modern on the surface, but runs on manual work, patchwork process, and systems that were never meant to scale together.

5. How Fragmentation Happens

HQ adopts first access control system (e.g., LenelS2)
"It works for us — no need to connect anything yet."

Company expands to new region with different access control system
"Let's just keep what the landlord already uses."

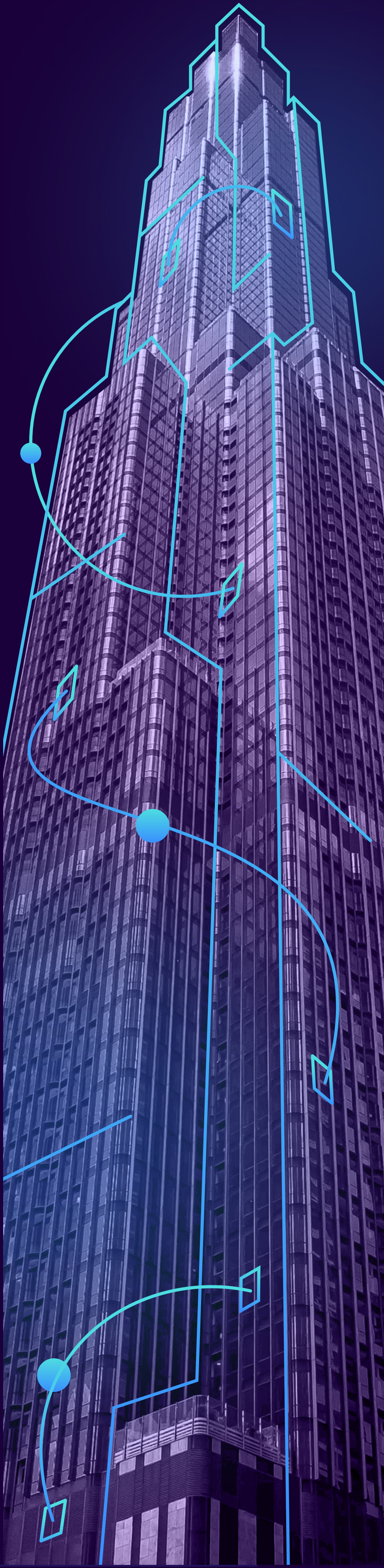
Introduction of mobile credentials at a flagship site
"We'll pilot mobile here — see how it goes."

New identity provider rolled out globally
"Eventually we'll sync access to identity. For now, let's keep both systems."

Acquires another company with its own access stack
"We'll deal with integration later. For now, just issue separate badges."

Hybrid work demands access flexibility across multiple sites
"Let's create a shared inbox for provisioning. It's messy, but it works."

Teams depend on manual process to bridge systems that were never meant to work together
"It's stable enough... but we all know it's not sustainable."



6. From Fragmentation to Control

Access challenges aren't necessarily the result of failed systems — they're the result of disconnected ones. Most of the components in place across today's enterprise environments do exactly what they're supposed to do. The issue is that they were never built to work together. As a result, control gets fragmented right along with the infrastructure.

When every building has its own access control system, every team has its own process, and every access decision is managed in isolation, there's no clear source of truth. Identity systems might reflect a user's role, but that information doesn't always make it to the physical layer. Changes in permissions lag. Offboarding is inconsistent. Teams get stuck acting as go-betweens — reconciling what should already be in sync.

> SwiftConnect addresses these challenges by introducing a unified access layer — one that bridges the gap between identity and physical space. We connect the infrastructure already in place: access control systems, identity providers, mobile platforms, and workflow tools.

This connectivity enables access decisions to be made in real time, based on a person's role and what they're authorized to do — no spreadsheets, no email chains, no duplicated effort.

This isn't a replacement for your existing tools. It's the connective layer they've been missing. With SwiftConnect, identity becomes the single source of truth for physical access — across every building, system, and team. People get the access they need, when they need it. And IT and Security regain visibility and control without taking on more complexity.

That shift doesn't happen all at once. But it doesn't have to. SwiftConnect integrates with what you already have, ensuring organizations have freedom of choice to adopt new technologies quickly and evolve as the landscape shifts. This empowers you to move from fragmentation to control at your own pace — one integration, one site, one use case at a time.

Comparing the Current State vs. a Unified Model

Fragmented Access Today	SwiftConnect Unified Access
Manual provisioning across multiple systems	Real-time provisioning based on identity
Separate access control system per building or landlord	Connected access network across locations
High volume of access-related help desk tickets	Reduced ticket volume through lifecycle automation
Lost badges trigger delays and reissuance effort	Mobile credentials issued over the air
Offboarding depends on email chains or spreadsheets	Access revoked automatically when identity changes
Inconsistent user experience across sites	Seamless access across every space, system, and resource
Limited visibility into who has access where	Centralized control and real-time access visibility
Vendor lock-in and siloed tools	Open, flexible platform using existing infrastructure

Ready to see for yourself? Get in touch for a personalized demo.

LEARN MORE

🌐 www.swiftconnect.com | ✉ info@swiftconnect.com