# BEHIND, *or just* UNFINISHED?

**Continuing the data center theme of this issue, Chris Meiter and Ed Evans from AMAG Technology and Eric Zei from Salient Systems examine why security gaps often stem from unfinished integration and unclear ownership, rather than outdated technology**

Data centers are going up faster than almost any other facility type, and the security problem inside them resembles nothing else. A large colocation site moves tens of thousands of people through its doors in a year, working for hundreds of separate tenant companies, most of whom the operator does not employ.

> **"An unfinished system is not a technology failure. It is a failure of ownership."**

Community opposition and organized protests are trying to reshape where these buildings go and how their perimeters get designed. Drones are a concern, though not for what they can see: everything in a data center comes back to cooling, and material dropped into an intake causes an operational event without anyone crossing the fence. Even video retention, a policy question in most buildings, is a contractual obligation with real money attached.

Salient Systems and AMAG Technology have worked on these buildings together since 2012. AMAG is among Salient's closest technology partners, and the work we do together concentrates in exactly this segment: the large operators running multi-tenant sites at scale. So, when an operator tells one of us that the security system isn't doing what they expected, we compare notes.

## What the access side decides about the video side

Comparing notes works because the two halves are not as separate as they look. Access control is often treated as finished technology: badge, reader, door. Visibility is treated as something happening on the video and analytics side. But that mistakes maturity for being solved. A protocol can

be decades old and entirely stable, yet still be poorly managed.

It is also backwards. Analytics are only ever as good as the access data they compare themselves against. Access events arrive in the video system with the cardholder attached to the alarm, which is what allows an operator to see who badged and to pull the recorded video by clicking the event rather than hunting for a camera and a time. The traffic runs both ways: video can trigger a lockdown, and a credential flagged as stolen can raise an alert with the right camera already attached to it.

> **"Analytics are only ever as good as the access data they compare themselves against."**

Video used to be evidence you went back for after somebody reported an incident. Now it is meant to raise the alarm while the incident is still underway. That only works if the access side is alerting personnel to something worth raising.

Tailgating is the clearest case. Access control records one valid swipe. Video, counting people, sees two bodies come through. Neither system flags anything alone, because the log says a valid credential was granted and video has no view on how many people should have passed. The alert exists only in the comparison. And in a data center, the second person is rarely an intruder. It is a colleague who did not badge, or a contractor's second technician on one credential, walking past cages that belong to somebody else.

## The two buildings behind one complaint

That is what the two systems do when they work. Far more often, what we hear is that they don't. The complaint is always the same sentence. What is causing it almost never is.

In one building the recording servers are eleven years old and the software ▸

is four versions behind. That is a budget conversation, and there is no clever way around it. In the other, everything is current and everything works. Nothing was ever finished: the detection zones are drawn so wide that somebody switched the alarms off, the cameras and the doors carry different names in each system, and the clocks drifted apart two years ago without anyone noticing. That one is an afternoon of work.

> **"An unfinished system is not a technology failure. It is a failure of ownership, and a data center project is structured in a way that almost produces it."**

From the operator's chair the two are indistinguishable. Ed Evans of AMAG Technology puts it at four out of five being the second kind, and suspects that estimate is generous. Neither got that way by accident, and the routes are different.

The first route is money. Hardware debt accumulates because security sits behind other IT in the funding order, and a department whose failures stay invisible is easy to defer. Nobody runs a laptop for eleven years. A recording server that has been writing continuously for eleven years draws no comment at all.

Version drift is quieter still. One operator can run a dozen sites on the same platform with eight different builds among them and never log it as a fault. That is why someone will watch a capability demonstrated at a trade show and insist their own system cannot do it. It can. Theirs is four versions back.

The second route is easier to travel because nothing along it announces itself. A detection zone, a door name, a drifted clock: none of it registers as an incident on its own. Collectively they are the distance between the system as designed and the system as installed, and almost nobody measures that distance. "The system does what it's told," Ed says. "It's just being told the wrong thing."

Colocation multiplies everything that has to be told correctly. "The big thing colocation has to deal with that single-tenant and hyperscale rarely do, is keeping tenants separated from each other, not just keeping outsiders out," Ed adds. That one difference reaches into every part of the design. Segmentation has to go down to the cage and sometimes the cabinet. Every tenant runs its own authorized-personnel list, with its own churn. Audit evidence has to come out per tenant, PCI for one and HIPAA for the next. And a tailgate into the wrong cage is not an internal write-up. It is a contract problem with a paying customer.

## The step nobody owns

An unfinished system is not a technology failure. It is a failure of ownership, and a data center project is structured in a way that almost produces it. On paper, commissioning splits three ways:

- The consultant designs the system and often writes the acceptance test plan, then is rarely still involved at installation
- The integrator installs it, configures it and effectively certifies its own work
- The end user signs the acceptance without the technical depth to test whether an access-to-video integration behaves as designed

"Nobody is structurally incentivized to find the gaps," Ed says. Verification falls to whoever volunteers, and frequently nobody does. Operations inherit the same split. Physical security holds access control, IT or facilities holds video and the integration between them belongs to whoever installed it and has not been touched since. When a system underperforms in that arrangement, it is usually three teams each maintaining their piece, with nobody responsible for how the pieces fit together.

Contractor access is the everyday version. A credential is issued for one cage and one afternoon and is supposed to be revoked the same day, which depends on someone





**Chris Meiter,**
Vice President of Global Business Development for Video Solutions, AMAG Technology

Chris leads AMAG's global video strategy and supports the growth of its Symmetry CompleteView Video Management System. Before joining in November 2024, he spent approximately a decade at Salient Systems.



**Ed Evans,**
Vice President, Business Development - Global Data Center, AMAG Technology

Ed leads AMAG's growth with hyperscale, colocation, wholesale and enterprise data center operators worldwide. He has more than 13 years of experience in data centers, physical security and building technology.



**Eric Zei,**
VP of Sales - Enterprise for Salient Systems

Eric joined Salient in 2021 with 20+ years of experience in working with Integrators and Enterprise End Users on the deployment and support of integrated security systems. Eric has a proven history in a variety of vertical markets.

remembering. A tenant authorizes one company and that company sends a subcontractor nobody put in the system. Equipment fails overnight and the approval chain gets skipped just this once, and that exception has a way of becoming routine. Every one of those failures sits at a handoff between parties who do not fully trust each other, rather than inside one chain of command.

## How to tell which one you have

Ownership is the hard thing to fix. Working out which of the two problems you actually have is not, and on an existing site it costs almost nothing:

- Match the naming convention across both systems
- Redraw the detection zones somebody switched off
- Synchronize the clocks between access control and video
- Clear the credentials that should have expired
- Run a punch list against what the specification actually promised
- Check firmware, software version and warranty date at every site

If answering that last one requires sending a technician, you have already found something.

> **"Most operators are already paying for more support than they use."**

The same diagnosis should change what you buy next. If most of the gap is commissioning, ownership and lifecycle rather than capability, then comparing feature lists measures the wrong thing. Both platforms on a serious shortlist can probably do the work. What separates them is the support model.

Most operators are already paying for more support than they use. A software support agreement usually carries engineering time and a periodic review of whether the system still runs the way it was designed to. The capability is not missing. Nobody calls it in. So, three questions are worth real weight at procurement:

- Does the support agreement include engineering time and scheduled review, or is it version entitlement and a phone number?
- Is verification against the original specification somebody's named job, with a punch list attached?
- When the integration fails eighteen months from now, whose name is on the ticket?

Data centers will keep outrunning security design. What can change is how quickly someone works out which of the two problems is in front of them, and whether anyone owns the ground between the two systems once the project closes.

The integrator who wins the next project is the one who can walk a site and say which is which: this half needs replacing, this half needs two days of configuration and this integration was never tested against the drawings. To an operator that is worth more than a quote for the whole building. Half of it is not a sale at all. It is what earns the next one. ■