Ambient.ai

CLEARED IS NOT SECURED: THE DISTANCE BETWEEN PACS ALARMS AND A SECURE PERIMETER

Inside Agentic Access Control with Ambient Access Intelligence

EXECUTIVE SUMMARY

For most security teams, the daily reality of access control is alarm fatigue. Physical Access Control Systems (PACS) generate a constant stream of alarms, the overwhelming majority of them false or routine, and operators clear them one by one with no context to tell the real ones apart. Legacy systems cannot fix this, because they were built to report alarms, not to interpret them. Ambient Access Intelligence interprets them, and the result is a step change no conventional access control or alarm tool delivers: up to 95% fewer PACS alarms reaching an operator.

That reduction is not a baseline the industry has reached and moved past. It comes from reasoning over video and access data together, the capability that defines Agentic Physical Security, the category Ambient.ai created. It is also the most important of three things access command requires, and the other two are easy to miss precisely because a low alarm count looks so reassuring.

The first layer is the noise itself: identical, context-free PACS alarms, almost none of which need a human. The second is the one a clean queue hides best: a cleared alarm is not a secured door. PACS record that an alarm was acknowledged, not that the door physically closed. On average, unsecured access-controlled doors stay physically open 14.5 hours a week, a perimeter exposure no alarm count will ever show. The third is chronic alarm sources: access points that generate noise because the hardware behind them is broken.

Ambient Access Intelligence is built to close all three, and it does so for more than one role. SOC operators get Doors Unsecured to see, in real time, which doors are actually open. Security administrators get Doors with Issues to find and repair the broken access points.

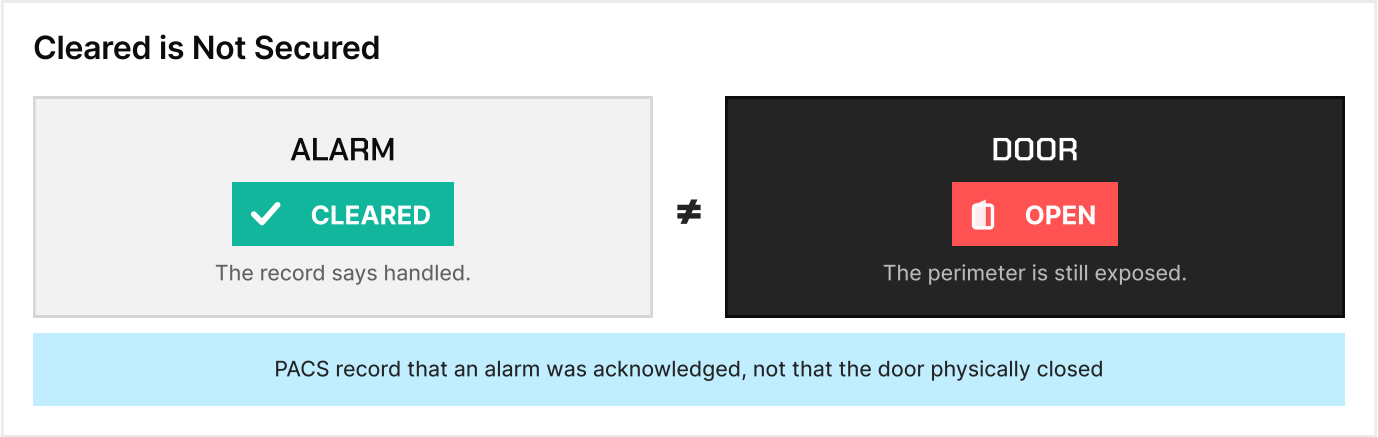
In the Path to Agentic Physical Security, this is Stage 3, Agentic Access Control. It is where a security team stops clearing alarms one at a time and starts seeing and commanding the true state of its perimeter.

THE THREE-LAYER PACS PROBLEM

Access programs stay stuck because they treat one symptom, alarm volume, as if it were the whole disease. Underneath the noise sit three separate failures, each with its own cause, its own symptom, and its own fix. Conflating them into a single complaint about too many alarms is the reason they never get solved, because a remedy aimed at the volume cannot reach the things actually generating it.

Layer one: alarms without context. PACS report that something happened at a door, but never what. Roughly 95% of the alarms they raise need no human action, and the operator has no way to tell which 5% do, because every alarm looks identical: a line in a queue, a door name, a timestamp, and no video attached. The operator can investigate all of them, which is impossible, or acknowledge them blindly, which defeats the purpose. Volume is the visible problem, but the missing context is the real one.

Layer two: cleared is not secured. This failure hides inside a clean queue, which is what makes it dangerous. PACS record alarm states, not physical door states. When an operator clears a Door Held Open alarm, the system logs that the alarm was acknowledged. It does not confirm that anyone closed the door. The alarm and the door are two different facts, and PACS track only the first. On average, unsecured access-controlled doors stay physically open 14.5 hours every week: an open perimeter accumulating in plain sight while the record reads as resolved.



Layer three: chronic alarm sources. Many alarms have nothing to do with people. They come from access points where something is physically wrong: a door that no longer latches, a strike drifted out of alignment, a sensor that misreports its state, a reader mapped to the wrong camera. On an average campus, 34% of access points carry an infrastructure issue that generates alarms day after day. These are not events to clear but faults to repair, and until they are repaired they produce noise on a schedule.

Two common event types show how little an alarm reveals on its own. A Door Forced Open alarm fires when a door opens without a valid credential. It is meant to signal an intrusion, but far more often it is a person leaving through the door, someone handling it from the inside, or a duplicate firing from the same reader. A Door Held Open alarm fires when a door stays open past its allowed time. It is meant to flag a propped or blocked door, but far more often it is a delivery, a door held briefly for a colleague, or an alarm raised after the door had already closed on its own. The alarm is real and the threat is not, and the operator cannot tell the two apart without the video PACS do not capture.

These are three different problems wearing the same uniform. You cannot fix what you have not separated, and an alarm count separates nothing.

The Scale of the Problem

~95	14.5 HRS	34%
of PACS alarms need no human action	a week that unsecured doors stay physically open (average)	of access points carry a chronic infrastructure issue (average)

Three separate failures a low alarm count hides.

WHY TUNING PACS WILL NEVER QUIET THE NOISE

Faced with too many alarms, most teams reach for the controls they already have: sensitivity settings, schedules, clearing workflows, the monthly audit. None of it quiets the noise, and the reason is structural. PACS were built to record that an alarm occurred, not to interpret what happened at the door. Every legacy remedy is therefore aimed at the symptom, because the system has no way to reach the cause.

PACS record events, not meaning. They know a contact opened or a timer expired. They do not know whether a person forced the door or the wind moved it, because they never see the door. Recording is the limit of their design.

Sensitivity tuning trades one failure for another. Loosen the thresholds and real alarms slip through. Tighten them and the queue fills with more noise. Either way the operator still gets a context-free line in a queue, because tuning changes how many alarms fire, never what any of them mean.

Manual vulnerability assessments are stale on arrival. Walking the campus once a month to find broken doors produces a snapshot that is already out of date by the time it is written up. Faults come and go on their own schedule, and a monthly pass cannot see the ones in between.

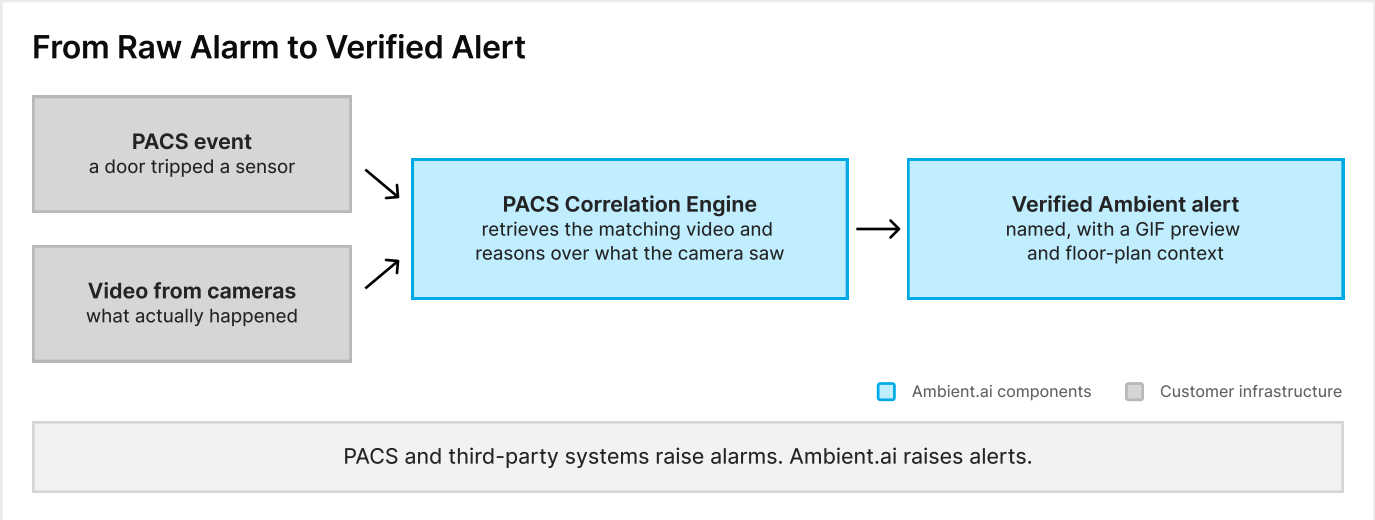
Clearing workflows confirm acknowledgment, not closure. A cleaner queue feels like progress, but clearing an alarm records only that an operator saw it. It says nothing about whether the door is shut. The workflow tidies the record and leaves the perimeter exactly where it was.

Alarm-orchestration platforms deserve a fair word, because they do real work. They route alarms, group them, and manage how they reach an operator, and for teams buried in volume that coordination has value. What they do not do is adjudicate. Routing an alarm faster still delivers a raw alarm; it does not decide whether the alarm was true. The difference that matters is between consuming raw alarms more efficiently and generating a verified signal in the first place.

That is the whole problem in a sentence: noise is not a volume problem to be managed but an interpretation problem, and PACS cannot interpret.

GIVING EVERY DOOR A WITNESS

Interpretation is what Ambient Intelligence adds. One of its enabling components, the PACS Correlation Engine, supplies that interpretation for access control. Operators never open it or configure it; it runs beneath Ambient Access Intelligence, and it is the reason every capability in the next section can tell a true alarm from a false one.



The engine does one thing, and does it on every PACS event. The moment a door reports an alarm, the engine retrieves the matching window of video from the indexed archive, reasons over what the camera actually saw, and returns a verdict with the supporting evidence. This happens in real time, before the event would ever reach an operator. The reasoning core behind each verdict is Ambient Pulsar, which interprets access data and video as one picture rather than two: not the door contact alone, and not the footage alone, but what they mean together. This fusion of video and access-control signal is patented.

The result is a change of kind, not degree. A raw PACS alarm goes in, and a verified Ambient alert comes out. This is the distinction the industry blurs and the one this paper insists on. PACS and third-party systems raise alarms, which are raw signals that something tripped a sensor. Ambient.ai raises alerts. An alert is an alarm that Ambient Intelligence has contextualized, by correlating it with the video of what happened and reasoning over it, into a verified, high-fidelity signal an operator can act on. PACS report that a door opened; the engine determines whether that was a person exiting, a sensor fault, or a genuine unauthorized entry, and says so.

In the language of the Agentic loop, this is the assess step applied to the access point. The reasoning that evaluates a live scene now evaluates a door event in context, and it does so for every alarm, continuously, without anyone asking.

What an operator and an administrator do with that verified signal is what Agentic Access Control delivers day to day, where the same engine also surfaces which doors are open and which access points are broken.

The Three-Layer PACS Problem

LAYER	CAUSE	SYMPTOM	FIX (AMBIENT)
Alarms without context	PACS report that an event happened, never what happened	About 95% of alarms are false, and every one looks identical	**Alarm Auto Clearing**
Cleared is not secured	PACS log alarm state, not physical door state	Doors stay open 14.5 hours a week, invisible to a clean queue	**Doors Unsecured**
Chronic alarm sources	Broken hardware at the access point	34% of access points generate noise on a schedule	**Doors with Issues**

Each layer is a different failure with its own fix. An alarm count separates none of them.

AGENTIC ACCESS CONTROL IN PRACTICE

Alarm Auto Clearing

Alarm Auto Clearing is the capability the other tools build on, and it serves everyone who touches the system. As each PACS alarm arrives, the PACS Correlation Engine has already reasoned over the matching video and reached a verdict, so false alarms clear automatically before they ever reach a person. Up to 95% of alarms resolve this way. The few that survive are the ones that earned attention, and each surfaces as a contextualized Ambient alert rather than a generic queue entry: named for what it is, with a short GIF preview of what the camera saw and a floor-plan view of where it happened. The operator opens an alert already knowing what it is and where to look, instead of opening a blank line and starting from nothing. The daily work changes from clearing alarms to acting on verified events.

Doors Unsecured

Doors Unsecured is built for the SOC operator and security manager on a live shift, and it answers the question Alarm Auto Clearing cannot answer on its own: which doors are open right now. It presents a real-time video wall of every physically unsecured door across every connected site, and it holds each door on screen until the door-restored signal from the PACS confirms the door has actually closed. Seeing the whole perimeter at once changes how a team responds. Instead of reacting to one alarm, dispatching a guard, and waiting for the next, an operator can direct a single coordinated sweep across the doors that remain open. This is the tool that closes the gap between an alarm cleared and a door secured, turning the physical state of the perimeter into something a person can watch in real time.

Doors With Issues

Doors with Issues is built for a different person: the security administrator responsible for keeping the access infrastructure healthy. It is a diagnostic, not an alert feed: a periodic, prioritized view of the access points generating alarms because something is broken. It sorts root causes into three categories: door and alarm behavior, such as a door registering as unsecured while it is visually closed; camera health, such as a feed that has gone dark or blurry; and camera-reader mapping, such as a camera that does not cover the access point it is tied to. Each finding arrives with the visual evidence behind it and is ready to route as a maintenance ticket. Instead of clearing the same alarm every day, the administrator fixes the door that keeps raising it.

PACS Analytics

Alongside the three operational capabilities sits a reporting layer. PACS Analytics turns the same correlated data into management views: Door Alarm Analysis to see where alarms concentrate, the PACS Alarm Reduction Breakdown to quantify how much noise has been removed and where, and Top Offenders tables to rank the doors and sites generating the most work. This is how a security leader measures the program and decides where to invest next.

How the Four Work Together

Each capability answers a different need, and together they give a security team command of the whole picture. Alarm Auto Clearing removes the noise so operators see only what is real. Doors Unsecured confirms which doors are physically open so perimeter state is never assumed. Doors with Issues removes the sources of the noise so the same faults stop recurring. PACS Analytics keeps the whole program measurable. Together they turn a stream of alarms into a perimeter a security leader can actually call secure.

Four Capabilities, One Command of the Perimeter

Alarm Auto Clearing	Doors Unsecured
EVERYONE Clears up to 95% of false alarms before they reach a person	SOC OPERATOR / SECURITY MANAGER A real-time view of every door physically open right now
Doors with Issues	**PACS Analytics**
SECURITY ADMINISTRATOR Finds and routes the broken access points for repair	SECURITY LEADER Measures the program and shows where to invest next

FROM NOISE REDUCTION TO PERIMETER COMMAND

The outcomes of Agentic Access Control line up with the three layers, which is the point. This is not a list of features that each save a little time. It is one system retiring three distinct failures, and the results read that way.

Layer one, the noise, falls away. Up to 95% of PACS alarms resolve before they reach an operator, returning thousands of hours to the team. No legacy approach comes close to that reduction, which is why it is the foundation the other two layers build on.

Layer two, the perimeter, becomes visible. Real-time door state, confirmed rather than assumed, closes the 14.5-hour-a-week gap between alarms that read as handled and doors that are actually open. For the first time the security leader can report not that the alarms are cleared, but that the perimeter is secured.

Layer three, the sources, are eliminated. Because Doors with Issues finds and routes the broken access points, the 34% of doors quietly manufacturing alarms get repaired instead of re-cleared. The slow, stale monthly audit is replaced by a continuous diagnosis that catches faults as they appear.

The clearest proof comes from ServiceNow, which runs Ambient Access Intelligence across its access control environment. The platform processed more than 240,000 PACS alarms and auto-cleared 94% of them, saving the team over 15,000 labor hours and avoiding more than $500K in costs, the measured result of solving all three layers at once.

Proof: ServiceNow

240K+	94%	15,000+	$500K+
PACS alarms processed	auto-cleared	labor hours saved	in costs avoided

> 240K+ alarms processed, 94% auto-cleared, saving over 15,000 labor hours and $500K+ in avoided costs.
>
> BRIAN K. TUSKAN,
> Chief Security Officer, ServiceNow

These outcomes are best read as a system rather than a set of separate wins. The 95% reduction is not a single customer's high-water mark either; it is an average Ambient.ai has verified across its enterprise customers, with ServiceNow's 94% sitting right beside it. What makes the case is not the size of any one number, but that noise, perimeter state, and sources are solved together, which is the only way access command holds.

WORKING WITH THE PACS YOU ALREADY RUN

Ambient Access Intelligence is designed to work with the PACS a team already runs, not to replace it. It builds on Ambient Foundation, the base layer of the Ambient Platform, and it is infrastructure-agnostic: it integrates with the leading PACS platforms in enterprise use today, so a team augments what it already owns rather than starting over.

ALLEGION	AVIGILON	brivo	genea	Genetec
Honeywell Pro-Watch®	KASTLE	LENEL:S2 by Honeywell	milestone	C-CURE 9000

Like any integration, this takes real work. Connecting to the PACS, mapping doors to the right cameras, and validating the correlation should all be scoped at the start. But it is not a replacement program. The doors, readers, controllers, and cameras already in place stay in place, and Ambient Access Intelligence adds reasoning on top of them.

FROM VERIFIED ACCESS TO ANTICIPATED THREAT

A verified access event is not just a cleaner alarm. It is a higher-quality input to everything that comes after it. Once the platform can say with confidence that a door event was a real unauthorized entry rather than a delivery, that judgment becomes a signal that threat reasoning can build on.

That is the link to Stage 4. The same fusion of video and access data that turns a raw alarm into a verified alert also feeds the threat detection that depends on access context, so the work done here strengthens the stage that follows. Verifying what happened at a door and assessing whether it signals a threat are the same kind of reasoning, applied at two points on the platform.

It holds together because it runs in one place. Access and threat operate inside the same Cloud SOC, on the same reasoning core, so a verified access event and a threat assessment are not two systems trading data but one system applying its judgment to two questions.

Where that judgment turns from verifying access to anticipating threats is the subject of the next paper, on Agentic Threat Detection and Response.

CONCLUSION: CLEARED IS NOT SECURED

The distance between a cleared alarm and a secure perimeter is where access programs quietly fail. A clean alarm queue can sit on top of an open perimeter, and across much of the industry it does, because the tools were built to manage alarms rather than to verify doors.

Closing that distance means solving three problems, not one. The noise has to fall, through Alarm Auto Clearing. The real state of the perimeter has to be visible, through Doors Unsecured. The sources of the noise have to be repaired, through Doors with Issues. Each layer needs its own tool because each is a different failure, and only reasoning over video and PACS data together can address all three. A cleared alarm is a record that someone looked. A secure perimeter is the outcome that matters, and they are not the same thing.

Agentic Access Control is Stage 3 of the Path to Agentic Physical Security, and it stands on its own. A team can adopt it to command its perimeter without committing to anything beyond it.

An access program should be judged not by how many alarms it cleared but by whether its perimeter is secure, and that is the certainty Agentic Access Control is built to deliver.