Decoding the Security Stack

Ella Ortenberg, HiveWatch

Physical security comes with a lot of assumed knowledge. Acronyms like VMS, ACS, PSIM, and CV are thrown around like everyone's supposed to know what they mean. There's no official glossary and figuring out how these systems work together (spoiler: they often don't) takes time.

If you are new to security, coming from another field, or tired of nodding along in meetings while frantically Googling later, here's the breakdown

The Foundation: Video Management Systems (VMS)

Let's start with the most visible piece of security infrastructure. A Video Management System pulls together video feeds from multiple cameras into one place where you can monitor, record, and search footage. Think of it as mission control for your cameras.

Most organizations already have a VMS when you walk in the door. It's often the first major security technology investment a company makes, and it becomes the anchor point for everything else.

The thing nobody tells you about VMS platforms is that they generate an overwhelming amount of data. A single camera can produce terabytes of footage over time. Multiply that across dozens or hundreds of cameras, and you've got a storage and searchability problem that's bigger than most people realize.

Access Control Systems (ACS): Who Gets In

Access Control Systems manage who can enter which spaces and when. They handle badge readers, door locks, turnstiles, and the logic that decides whether someone's credentials are valid.

ACS platforms connect physical hardware (the readers and locks) to a database of users and permissions. When someone badges in, the system checks their credentials against access rules and either grants or denies entry, creating a log of the attempt either way.

What makes ACS tricky is that access rules get complicated fast. You're not just managing "can this person open this door?" You're managing time-based access, temporary credentials for visitors or contractors, integration with HR systems for automatic provisioning and deprovisioning, and compliance requirements around audit trails.

Computer Vision (CV): Teaching Cameras to Understand

Computer Vision is AI that analyzes camera feeds to detect specific objects, behaviors, or conditions. Instead of a human watching monitors and trying to catch something unusual, CV algorithms can identify things like weapons, unattended bags, people entering restricted areas, or vehicles without proper permits.

CV runs analysis on existing camera infrastructure. Technology has gotten significantly better in the past few years, but it's still not magic. CV is only as good as its training data, and it works best when it's looking for specific, well-defined things rather than vague concepts like "suspicious behavior."

The practical reality of CV is that it reduces the needle-in-a-haystack problem. Instead of scrubbing through hours of footage looking for a specific incident, CV can flag moments that match your criteria. It won't catch everything, and it will occasionally flag things that aren't threats, but it makes monitoring at scale feasible in ways that weren't possible when you needed human eyes on every camera.

Visitor Management Systems (VMS... Yes, Same Acronym)

Visitor Management Systems track who's coming onsite, when they arrive, and where they're authorized to go. These platforms have become more sophisticated than the old paper sign-in sheets, now handling pre-registration, badge printing, host notifications, and integration with access control.

Modern visitor management isn't just about knowing who's in your building. It's about compliance (who accessed sensitive areas), emergency response (who needs to be accounted for during an evacuation), and operational efficiency (reducing friction at reception while maintaining security).

Intrusion Detection Systems (IDS): The Sensor Network

Intrusion Detection Systems use sensors like motion detectors, glass break sensors, and door contacts to alert when someone enters a space they shouldn't. These are the systems that trigger alarms when a perimeter is breached after hours.

IDS platforms are often the oldest technology in a security stack because they've been around longer than modern video or access control systems. They're reliable but limited. They tell you something that happened, but not necessarily what happened or who was involved.

The integration challenge with IDS is getting alerts from these sensors to trigger actions in other systems, like having a motion detector automatically pull up the nearest camera feed or unlock an exit door during an emergency.

Physical Security Information Management (PSIM): The Aggregation Layer

This is where things get interesting. PSIM platforms try to solve the fundamental problem with everything I've described so far: all these systems live in separate silos.

A PSIM connects information from multiple sensors and systems, correlates events, and presents a unified view of what's happening. Instead of monitoring five different dashboards, security teams get one interface that shows alerts from VMS, ACS, IDS, and other sources together.

The theory is great. Execution is often messy. PSIM implementations require significant configuration, ongoing maintenance, and they're only as good as the integrations they can establish with your existing systems. But when done well, PSIM transforms how security operations work by reducing the cognitive load on operators and helping them understand the full context of an incident.

Weapons Detection: Hardware and Software Approaches

Weapons Detection can be handled through dedicated hardware scanners or through Computer Vision analysis of camera feeds. The hardware approach uses devices like airport metal detectors but designed to be faster and less intrusive. The CV approach analyzes video to identify weapons visually.

The technology here varies wildly in capability and accuracy. Hardware detection is generally more reliable but requires people to pass through specific checkpoints. CV detection can cover more area but has higher false positive rates and works better in controlled lighting conditions.

This is an area where vendor claims often outpace actual performance, so testing in your specific environment is critical before making decisions.

Mass Communication (Mass Comms): Getting the Word Out

Mass Communication platforms send emergency notifications to large groups quickly. During an active incident, you need to alert occupants, coordinate response teams, and communicate with law enforcement.

These platforms integrate with security systems so that an event detected by your IDS or CV system can automatically trigger communications. The challenge is balancing speed (getting alerts out immediately) with accuracy (not creating panic over false alarms).

Good mass communication systems handle multiple channels including text, email, app notifications, and overhead speakers. They also track who received and acknowledged messages, which matters during emergency accountability.

Open Source Intelligence (OSINT): Looking Beyond Your Perimeter

OSINT platforms scrape the web and social media to identify potential threats before they reach your physical space. These systems monitor for location-tagged posts, threat keywords, and patterns that might indicate planned incidents.

OSINT has become more relevant as potential threats increasingly announce themselves online before taking physical action. Technology can provide early warning, but it also raises privacy questions and requires careful policy around how information is collected and acted upon.

Case and Incident Management: Tracking Response

Case Management Platforms help investigation teams document incidents, track evidence, and manage research workflows. Incident Management Platforms help teams log and respond to security events in real time.

The distinction matters because case management is about the investigation after an incident (think detective work), while incident management is about the operational response during an event (think dispatch and coordination). Many organizations need both but start with incident management because it addresses immediate operational needs.

Why This All Matters

Understanding the security stack isn't just about knowing definitions. It's about recognizing that physical security infrastructure is fundamentally a data integration problem. Each system generates information, but the value comes from connecting those data points into actionable intelligence.

When your access control system shows someone badged into a restricted area, your VMS should automatically pull up the camera feed from that location. When an intrusion sensor triggers, your PSIM should correlate that with recent access attempts and video evidence. When a weapon is detected, your mass communication system should alert the right people immediately.

That's the theory. The reality is that most security stacks are held together with integrations that break, manual processes that create delays, and operators who are managing complexity that shouldn't exist.

The industry is moving toward more unified platforms that reduce the number of separate systems, and AI is helping bridge gaps between systems that can't directly integrate. But we're not there yet. Most security teams are still managing a collection of point solutions that require significant effort to make work together.

If you're early in your security career, learning how these systems work and how they're supposed to integrate will make you significantly more valuable. If you're evaluating new technology, understanding the full stack helps you ask better questions about how solutions will fit into your existing infrastructure.

And if you're just trying to keep up in meetings, now you've got the glossary nobody gave you on day one.