VICON

VIDEO MANAGEMENT SOFTWARE

Superior Security Begins with a Single Pane of Glass

NOVEMBER 2022 | WHITEPAPER

Introduction

Open APIs have made it easy for leading VMS platforms to link video to instances of doors being propped open, LPR events, and other security incidents. The added value of integrated solutions makes them the norm for today's enterprise systems, and common in small to medium-sized installations. However, in most integrations, the VMS is not the dominant interface for viewing video with its associated data. Instead, users click on an event of interest within their access control software, for example, to see a short video clip captured by a nearby camera. Then, to search for more related clips, they turn to the VMS interface. While such integrations are better than no integration, the operator experience is clumsy and inefficient for use as a core security management platform.

A video-centric platform allows security personnel to remain within the VMS interface to view and manage events from integrated solutions – like access control, LPR, vape detection, and more – all through a single pane of glass. To explain its inherent superiority, let's begin with a hypothetical security threat and envision how such a system would facilitate a response.

A video-centric platform allows security personnel to remain within the VMS interface to view and manage events from integrated solutions - like access control, LPR, vape detection, and more - all through a single pane of glass.

Imagine This

Larry was terminated from his job last week. Today, he drives to his former workplace. A security officer monitoring the property sees live video from a parking lot camera pop up within the VMS interface. On the same screen, data from an integrated License Plate Recognition (LPR) system shows that the vehicle belongs to Larry Larkin, former employee.

Larry's plate is not on security's "forbidden on property" list, but the officer is curious whether Larry's visit is expected. He checks his list of approved visitors for the day and sees that Larry has an appointment with HR to finalize severance paperwork. Therefore, there's no need to dispatch an officer to the parking lot.

Larry heads to the employee entrance instead of the main entrance. As he approaches the door, a nearby camera's motion detection analytic pushes video to the officer's screen again. In addition, the VMS displays a facility map pinpointing the location of the active camera. Larry is in the wrong place, as he is no longer an employee.

From within the VMS screen, the officer opens a 2-way communication channel with the intercom mounted next to the employee door. He plans to instruct Larry to use the main entrance, where he must sign in and be met by someone from HR.

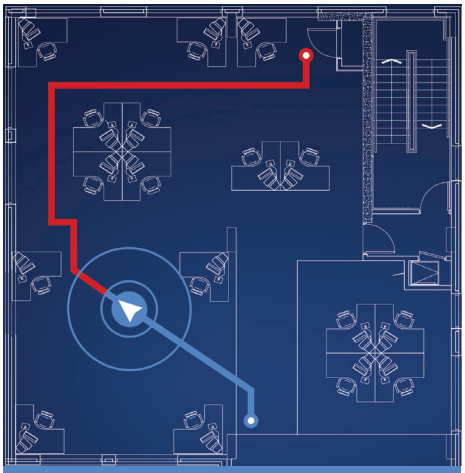
Just then, a staff member arrives at the employee door, swipes in, and improperly permits Larry to follow her through the entrance. Her name and department display next to the video.

The officer follows Larry's movement through the facility via surveillance cameras, instructs another officer to intercept him, and alerts HR that Larry is approaching their department unescorted. Furthermore, as a precaution, the officer calls up the status of door to the HR department and confirms that it is locked.

The episode ends without incident. Larry's use of the employee entrance was an honest mistake driven by habit. HR greets him at the door and allows him to enter the office area, where he meets with a benefits representative as planned.

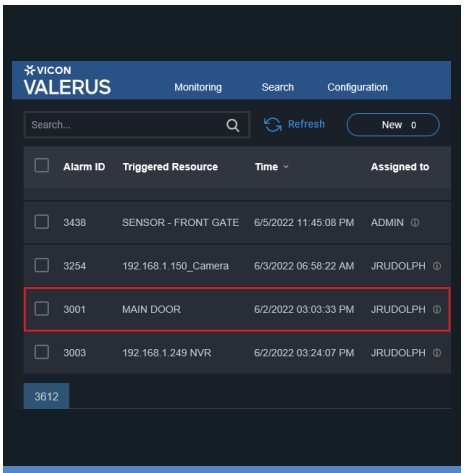
To summarize, within the VMS, the officer was able to:

Identify Larry's car by his license plate



Track his movements via a visual site map

Connect to an intercom system



Identify the employee who mistakenly let Larry into the building

Confirm that the HR door was locked so that Larry could not enter without permission

And, if it was not secure, he could have locked it remotely

This example is purely hypothetical, but it illustrates the advantages of a centralized video platform presenting disparate systems within a single pane of glass. Capabilities will vary by VMS manufacturer and the integrations they offer, but in all cases, system operators, administrators, onsite workers, and visitors benefit. Let's dig deeper.

Enhanced Situational Awareness and Actionable Intelligence

Video is much more meaningful when supported by live, corresponding data. When security officers are trying to understand the nuances of a security event, having all relevant information presented and seamlessly accessible is ideal.

In the previous example, there were many times the guard received additional information within the VMS to explain what he was seeing. In a non-integrated solution, with only video immediately available, the officer would only know that someone had tailgated through an employee entrance. He would lack sufficient knowledge to assess the risk and respond appropriately. An overreaction by his security team could cause unnecessary stress and inconvenience to everyone in the building; a weak response could jeopardize their safety.

With a video-centric integrated solution, operators have the data they need to differentiate between "real" security threats and harmless situations. They can prioritize where to focus their attention and quickly understand when it's necessary to deploy additional resources.

A Faster, Better, More Informed Response

Without a single pane of glass, security guards must navigate several solutions, search for, and pull up, relevant data to stitch together and make sense of what they observe – a cumbersome process that's impossible to perform in real time.

Our example ended peacefully, but what if Larry was emotionally unstable and seeking revenge for what he perceived as wrongful termination? Imagine if HR had flagged him as a volatile individual who was not welcome on site? Or if the guard observed Larry removing a firearm from his car while in the parking lot? That guard could have initiated a lockdown immediately from within the VMS. These are ways in which a video-centric centralized solution facilitates a faster response.

A centralization solution also better equips officers who monitor security from their mobile devices. Patrolling guards can maintain situational awareness without toggling between apps. When officers in the field have access to the same information as those behind a desk, they can respond immediately and spontaneously to security risks, like a door propped open. They don't need to wait for dispatch orders.

Today's centralized solutions can initiate automated, complex responses driven by AI. There may be cameras all over a facility, but humans can only look at so many video streams at one time. Analytics can identify anomalous situations before humans can, issue real-time notifications, and trigger a series of proactive responses across all platforms while security professionals evaluate the next steps. The systemwide response is documented as a single event, presented through a centralized interface.

When non-video events can only be viewed from within their native platforms, operators must waste time navigating disparate systems as they seek to determine:

a. **What's happening?**
b. **Where else should they look for information?**
c. **What's the best plan of action?**

Systemwide Efficiencies and Cost-Savings

In a security operations center environment, multiple monitors typically appear side-by-side at each workstation, allowing operators to observe simultaneous events from separate systems in real-time – such as a card swipe and corresponding video. However, further investigation requires the officers to take their eyes off the surveillance video. When a threat is unfolding, that's a luxury they don't have. A larger team is needed to provide monitoring and response coordination.

Centralized platforms save money on staffing and technology. Fewer officers can manage many systems at once using fewer monitors and servers.

Companies also save on system training. With only one platform to learn, security teams can master its full range of features relatively quickly. By contrast, when operators are expected to manipulate many applications and interfaces, it is difficult for them to become proficient with any of them beyond a superficial level.

No Coding Required

When VMS systems *are designed to perform as a core platform*, integrators find that much of the work required for integrating access control and other solutions is already done. Manufacturers of open, video-centric VMS software sometimes create "integration frameworks" that require little more than entering the IP address of any server hosting a compatible third-party solution. After that, a drop-down list allows an administrator to associate cameras with access readers, LPR databases, or other devices. The integration is pre-built, requiring no programming by the integrator.

By contrast, systems not designed for centralized management through the VMS may make APIs available to programmers, but extensive effort and coding expertise are needed to create a functional solution. Depending on manufacturers, a custom-engineering video-centric solution may not even be possible.

Actionable Data for Investigations and Operations

When operators can derive intelligence from one searchable interface, they benefit from a more transparent audit trail that enables faster and deeper analysis.

For example, a security team might want to search every time a particular car entered the parking lot during specified days. A single search could find those time-stamped instances via the LPR database, subsequent access swipes at the parking lot gate, and correlated video. Was it the same person in all events? The centralized platform makes detective work more fruitful, as puzzle pieces come together with significantly less effort.

Analysis of aggregated data can also improve security and operational policies by helping to identify where gaps exist. For example, analyzing the frequency with which secure doors get propped open and by whom, or if tailgating is a chronic problem between 8:30 and 9:00 am, could drive security teams to update policies or consider new solutions.

You Have an Important Decision to Make

Stakeholders researching their company's next security upgrade often have non-negotiables that their VMS system-of-choice must deliver. Many insist it must be scalable. Feature an open platform. Have a robust mobile app. The VMS's ability to monitor and manage security from a core, centralized platform should top the list. Without it, any VMS will fall short.

Integrators who specialize in "single pane of glass" solutions differentiate themselves from the competition. They are no longer just camera or access control dealers. They are value-added problem solvers who deliver against a broader range of clients' security challenges.

Their customers benefit from superior situational awareness, response capabilities, ease of use, operational efficiencies, and forensic insights. But there's more. They also have a future-proof system that will accommodate advances in physical security technology. Video-centric, centralized platforms are not engineered in a VMS vacuum. They are designed within the context of the broader security market, with developers looking for ways to bring added functionality to users through synergistic integrations. Users can feel confident that the platform they purchase today has a roadmap of future integrations, ready to grow with their security needs.

In today's environment, VMS platforms that can only display video are limited from day one. They can—and should—do so much more. Centralized security management is fundamental to organizational safety. Choosing the right VMS is the easiest and most cost-effective means to get there.

vicon-security.com