Genetec

White Paper

Optimizing Video and Access Control Integration with A Next-Generation Security Platform

Table of Contents

Executive Summary

Nowadays, video surveillance and access control systems require a certain level of synergy. Yet the security industry has continued to provide disparate systems, with limited communication between systems. Even today, with all the technologies available, the industry is struggling to fully succeed at building security solutions that fulfill the users' true needs—a cohesive video and access control system that is efficient, non-proprietary, and cost effective. With the recent advancements in software technologies, and the ongoing discussions between manufacturers, integration has become a popular substitute for traditional interfacing. However, even integration has its limits. The answer can be found in a single software that manages access control, intrusion and video through non-proprietary security appliances. This next-generation security platform provides unity between video, access and intrusion systems with built-in reporting and alarm management functionalities. It goes above and beyond the basic functionalities of interfacing, integration and even PSIMs, offering end-users an efficient, flexible and cost-effective option to system unification.

Addressing the Security Industry's Hidden Flaw: Interfacing

Video and access control have always been seen as two separate industries. For the longest time, there were separate manufacturers building different products, each with their own specialized engineering teams. Even if end users always requested synergy between the two products, the reality was to buy video surveillance from one supplier and access control from another.

In one of his articles, Rich Anderson, president of Phare Consulting, previously VP of Marketing for GE Security and the VP of Engineering for CASI-RUSCO, illustrated the problem: "We have known for many years that the integration of access control systems and video systems produces real benefits. Yet, somehow we have managed to continue to build integrated systems the same way we did 15 years ago—one interface at a time."[1]

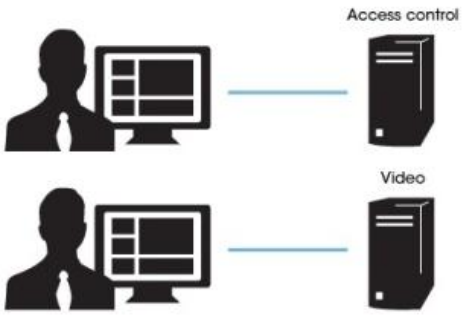

Figure 1 - Non-integrated system

The very first examples of interfacing access control and video products were characterized by the use of relays. At the time, what were considered sophisticated access control products were able to switch cameras on a matrix using commands over serial ports. A lot of these systems are still in operation today. To properly perform their work-related tasks, users were forced to master various independent systems, including DVR/VCR systems, CCTV keyboard equipment, access control software, intrusion systems, etc.

Shedding Light on What The End Users Really Want

Even today, with all the technologies available, the industry is struggling to fully succeed at building security solutions that fulfill the users' true needs—a cohesive video and access control system that is:

- Efficient
- Non-proprietary
- Cost effective

It is important to recognize that without these basic criteria, a unified video and access control system may not seem advantageous to customers and thus, not generate enough demand for manufacturers to justify developing such a product.

Efficiency Gains Matter

Any security staff, regardless of which market sector they come from, should spend their time on performing their core tasks such as monitoring, investigating and reacting to low and high-priority situations, and not on managing technology. In other words, the security technologies they use should help them be more efficient and not slow them down.

Again, Anderson clearly illustrates the common problem in today's disparate systems with the following statement: "Access control systems in particular generate alarms such as invalid badges, door-forced and door-held events. Those events need to be investigated, but the task of doing so with a standalone surveillance system is painful. Receive an alarm on one system, and your operator has to move to another completely different system to investigate. This surveillance system has a different user interface and so he/she has to "switch gears." Then, which camera do you call up to view the scene? An experienced operator will know, but that "experience" costs you a lot in terms of training." [2]

[1] Video and Access Control Integration, SecurityInfoWatch.com, Rich Anderson, 03-25-2009

[2] Video and Access Control Integration, SecurityInfoWatch.com, Rich Anderson, 03-25-2009

Interoperability Means Anything They Want

The PC industry has succeeded in building interoperable products. Anyone can buy a PC today, and down the line, add new hardware like a printer, web cam, gaming devices, or even install a new hard drive that processes information two times as fast as the previous one. Almost anything can be done without changing the entire PC or operating system.

However, the same cannot be said or done in the security industry. A user cannot simply decide to buy the latest high-tech wireless door controller and add it to an existing access control system. Or buy the latest and greatest IP cameras and connect them to a video management system (VMS) without first verifying that the specific model is supported. For these and many other reasons, the security industry is far behind the PC industry.

In fact, it might never be possible to achieve what the PC industry has in terms of interoperability.. Making a commitment to proprietary technology can be a costly decision. When a new technology emerges, the option to incorporate it becomes more of a question about whether or not to forgo existing investments and start over from scratch.

On the other hand, having the ability to mix best-of-breed products from different manufacturers, and having the option to incorporate the latest advancements in technology into their system, provides more flexibility and the added assurance that their investment, for the most part, is future-proof.

Every Penny Counts

A solution that is entirely customized to fit with all existing business processes and infrastructure might be very efficient and attractive, but as with any customization it will likely be expensive as well. Take for example ERP systems (enterprise resource planning) deployed by many companies. An ERP system can be customized to adapt to virtually any business model and environment by specialized ERP system integrators. Although the cost of customizing such a system is very high, there is usually a significant productivity gain realized after deployment to justify this investment.

In similar respects, investments in security departments and equipment are always considered an expense and it is unlikely that security systems could be adapted to every internal process. Since these systems rarely generate revenue, budgets are tightly controlled. Completely overhauling a system, regardless of the technology employed, is entirely dependent on budget availability and management's buy-in. Often, even discussions of upgrading or replacing a system occur out of pure necessity (eg., aging system or security flaw) and the process itself of sourcing and implementing a system could span months, if not, years.

Therefore, it is crucial, more than any other factor, that the total cost of ownership of a cohesive video and access control system be justified.

After Simple Interfacing Comes Integration

With the recent advancements in technologies, and the ongoing discussions between manufacturers, integration has become a popular substitute for traditional interfacing.

Integrated Systems

A step beyond the outdated practice of interfacing is systems integration.

"In information technology, systems integration is the process of linking together different computing systems and software applications physically or functionally." [3]

Specifically in the security industry, the most popular integration methods are network protocols and software development kits (SDK).

Network protocols are very powerful as they support a mix of operating systems and it is real-time. However, integrating two systems through a network protocol requires more time than an SDK or a shared database between two systems. Network protocols are popular for edge-device integrations like IP cameras or door controllers but are even more commonly used between two software applications. Network protocols are simply deemed more effective.

An SDK also referred to as application programming interface (API) consists of a DLL package created and distributed by software manufacturers to allow other software developers to integrate their system.

[3] Systems Integration Course Syllabus, Georgia State University, webpage, retrieved June 27, 2007

SDKs simplify the integration by hiding all the complex mechanisms from developers such as authentication, decoding video, complex network protocols etc. Because it simplifies software integrator's task, most DVR, NVR and access control manufacturers offer an SDK or API instead of a network protocol.

The majority of video surveillance manufacturers offer an SDK that can be used to integrate live and playback video within any application. For example, some access control manufacturers use the SDK from some DVR vendors to attach an access control alarm to the associated video for quick playback. The majority of access control software manufacturers also offer an SDK so VMSs can receive access control events from their system. Some access control vendors even allow video manufacturers to integrate some of their functionality inside the access control system's user interface.

Regardless of the method of integration that is chosen, integrated systems definitely start to give users the tools to become more efficient. It is very common for an integrated access control and video solution to display live or playback video associated with an access control event from the access control user interface.

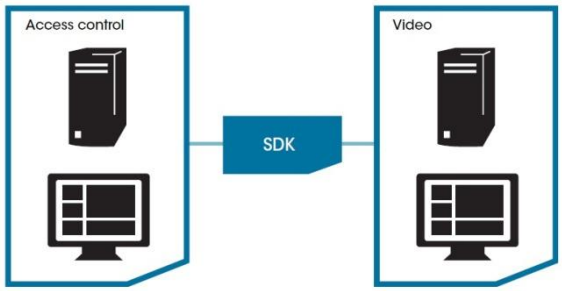

Figure 2 - Integrated solutions

Also, integrated solutions offer another advantage for users: not having to rely on a single manufacturer for the entire security system. In some cases, it might be beneficial to deal with two independent vendors with each having multiple technology partners of their own. In this case, users who do not like their current video surveillance solution might be able to switch to another manufacturer, as long as it is compatible with the access control system.

Although lowering end user switching costs and using an SDK or API to achieve a deeper level of integration amongst products has its benefits, integration also carries a few pitfalls as well.

Most of these integrations still require operators to use two systems in parallel because neither the video nor the access control system offers all the required functionalities in one user interface.

Examples of limitations:

- The access control system doesn't support camera sequences.
- Not easy to search through all recorded video recording with access control.
- No motion search capabilities in the access control system.
- Pan-tilt and zoom (PTZ) functionalities are limited in access control as compared to the video system.

Another common drawback to consider with an integrated system emerges from future maintenance and configuration of said system. Since the administrator has two or three independent systems to configure and keep synchronized, maintenance of these multiple systems will require more time.

Also, many of these configurations are redundant, causing the administrator to repeat the same work on all systems. Here are a few examples:

- Independent alarm management configurations
- User management: for each operator, the security manager must create two accounts and specify privileges in two systems.
- Each new camera requires configurations in two independent systems.

Finally, conducting upgrades and getting support for an integrated system can be challenging. Russ Gager, once Senior Editor for SDM magazine, raised a valid point about upgrades: "Two systems from different companies may be successfully integrated, but if one of the companies comes out with a newer version of its software, then the integration may not work with the other company's software." [4]

Manufacturers constantly change their software to support new functionalities and with that, might also change the way existing integrations work, especially when they change their SDK or API.

Considering an upgrade to the latest software version of one system that is part of an integrated solution may impact the

[4] How to improve your Integrated System Projects, SDM Magazine, Russ Gager, November 1, 2006

integration, the installer is responsible for ensuring that the latest VMS software is still fully compatible with the access control software. Before taking the end-user's system down and upgrading, many integrators will prefer building a test system in their lab to validate the integration.

Seeking support for an integrated solution can also become a complicated affair. Since there are two separate systems involved, each likely from two different vendors, when a problem occurs, it takes more time to resolve. Both manufacturers, and often the integrator, have to investigate and figure out which system is not behaving properly. The time it takes to resolve the issue in question is also dependent on the relationship between the two software manufacturers.

So, although there are many advantages derived from an integrated system in comparison to traditional interfacing, there are still many issues with this level of integration that emerge.

Open Platform Systems

Open-platform products, as referred to in the security industry, integrate with different hardware manufacturers without necessarily using industry standards like open-architecture systems.

Open-platform manufacturers develop, test and maintain the integration with every single devices supported by the product. Open-platform products tend to support a wide variety of manufacturers that offer similar functionalities and products that are commoditized. Manufacturers of such systems do so by building a generic integration layer that provides the most common functionalities and then by developing a driver for each specific product the system integrates with. This strategy works well for specialized appliances because they have fixed and well-defined functionalities.

The open platform VMS concept, for example, is well established in the market because IP cameras or IP encoders all offer common features.

These types of systems offer huge benefits to end users because they now have the freedom to change software or hardware vendors without having to discard all invested equipment.

The access control industry however, has been built on proprietary solutions, including single manufacturers for the door controllers and the management software. Today, it is easier for vendors to build closed access control systems. The reasons being that offering a closed system reduces complexity, simplifies testing efforts, and increases the revenue per customer by selling both the hardware and software. But this closed architecture removes a lot of flexibility for the end user.

Because of the success in video surveillance, and because end users are demanding more freedom, similar open-platform products are beginning to emerge in the access control industry. Today, IP-based door controllers are offered by manufacturers that do not even offer access control software. These hardware manufacturers publish their wired protocol or provide an SDK to communicate with their controllers. Other hardware companies are also offering more and more wireless IP locks bundled with readers that reduce the installation costs.

A Trend That Is Making Open Systems More Appealing

The emerging standards in the video surveillance industry like ONVIF and PSIA will eventually simplify the integration between software manufacturers and different security appliances such IP cameras, DVRs, door controllers, alarm panels, and fire panels because the communication protocol and functionalities will be standardized and consistent across hardware manufacturers.

The idea of creating a unified standard for security appliances is gaining in popularity due to its advantages. Standards will allow end users the freedom to choose from different manufacturers with minimal interoperability problems.

Manufacturers, on the other hand, will not need to conduct internal development tests or test for product compatibility with every single product; they will only focus on functionality and quality instead of interoperability. The interoperability is derived by the use of standards.

A Cut above The Rest: The Open-Unified Platform

With the open-platform concept already established in the video surveillance industry, the new trend toward non-proprietary door controllers in the access control industry and the emerging security standards, the dream of a unified security platform is achievable now within sight. A unified platform is a comprehensive software solution that manages access control, intrusion and video functionalities through non-proprietary security appliances.

A unified platform goes above and beyond tagging or bookmarking video when an access control event occurs or unlocking an access controlled door from the video surveillance user interface. It is a unified user interface that offers seamless integration between video, access and intrusion systems with built-in reporting and alarm management functionalities.

With this type of solution, it is possible to configure and manage video cameras, access controlled doors, print badges, monitor intrusion panels, and have everything at the security personnel's disposal to ensure the level of security of a facility within a single consistent software suite.

An open-unified solution protects the end user's investment through interoperability, meets the user's security needs and is affordable to buy and maintain.

An open-unified platform is a product that targets the mass market by providing built-in support for commoditized security products such IP cameras, DVRs, door controllers, alarm panels, badge printers, active directory for authentication and card management without requiring customization for every installation.

This type of solution that targets the mass market and does not require customization also tends to be less expensive than a custom-integrated solution.

Since a unified platform supports commoditized products, hardware investments are protected. Therefore, if the end user is not satisfied with the unified software solution, he can change software components without having to reinvest in specialized appliances.

Nevertheless, something to keep in mind is that even if customization is not mandatory to deploy a unified platform, it must still allow for third-party integration and customizations through an SDK or API. The SDK or API must be available so the end user can contract external firms to design and maintain the custom integrations beyond their video and access control applications, and not rely solely on the unified platform manufacturer for these initiatives down the road.

The Unified Server Infrastructure

"A seamlessly integrated system offers centralized management, administration, monitoring and reporting. Its single, centralized database contains all the information that, in a non-integrated environment, would be distributed among multiple databases." [5]

A truly unified platform optimizes resources by sharing common servers and databases for:

- Authentication and permissions
- Licensing
- Configuration settings
- Alarms and events
- Audit and activity log
- Video recording
- Access logs

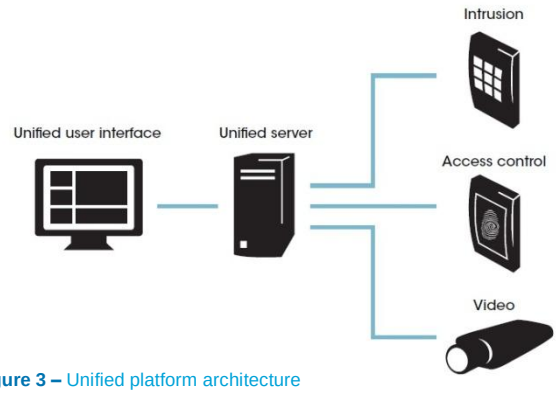

Figure 3 – Unified platform architecture

This type of architecture is easier to install and manage because it consists of a single software suite to learn, configure, upgrade, backup unlike the integrated system where these tasks must be done for all implicated systems.

[5] Finding Seamless Integration of Digital Video, Security Magazine, Rudy D. Prokupets May 7, 2003

A centralized server infrastructure also simplifies the end user's life because the user only needs to connect to a single server by using a single login. From that connection, they have access to all services offered by the unified platform. They no longer have to connect to different servers while conducting both video and access control investigations.

Unification from the server all the way up to the interface offers advantages beyond the end users' initial needs such as:

- Efficiency through a single interface
- Automation from event correlation
- Cost-effectiveness from single-source configuration and maintenance

The User Experience

A single user interface for multiple security applications allows operators to easily and efficiently move from one security task to another within the same interface, thus avoiding complicated workflows and interface manipulations to reach the required window.

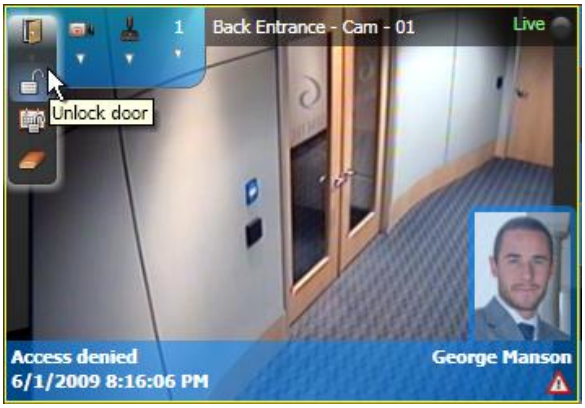

Figure 4 – Real-time monitoring

The user's workflows are consistent between the video and access so the user becomes more familiar with the system, experiences self-learning, and gains more confidence in his ability to use the system.

More so, the total number of workflows to understand is reduced by having common core functions. For example, alarm management, event to action, reporting, investigation, and incident-related workflows are all the same regardless of whether it is for video or access.

Figure 5 – Door activity report

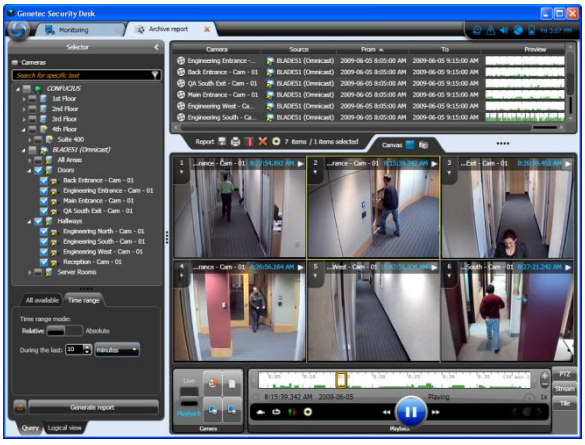

Figure 6 – Video archive report

Users are also only required to be trained on a single system; therefore they don't waste time switching to different applications or workstations as everything can be done in a single and coherent user interface.

Event Correlation

A unified system is designed to offer event correlation because events and alarms are managed by a single server infrastructure. Access and video events are correlated to minimize false alarms. For example, when a tailgating event is detected by the video sub-system, the access control sub-system can automatically confirm if there was a single or

multiple access cards swiped at the door in question, in which case and alarm would or would not be automated.

A unified platform with good event correlation can significantly reduce investigation time by filtering out false alarms.

Ease of Maintenance and Support

With a unified system, only a single software platform needs to be upgraded and maintained instead of with an integrated solution that has multiple systems to address. The ease of upgrade results in time savings for integrators and simplifies the technical support aspect in case of issues since no time will be wasted trying to find which vendor needs to be called. Integrators have a single point of contact to work with. For the end user, this translates into a quicker response time to resolve problems and get clear answers.

Also, because a unified system is designed to address the mass market with commoditized appliances, the systems installation for most customers will have similarities, and often include the same combination of products. Therefore, if an integration problem between the software and specialized appliance occurs, chances are that the problem has occurred somewhere else before, and a solution has already been found. This ultimately means that the customer can improve their system by learning from the experiences and applications of other end users.

What about PSIM?

Physical security information management (PSIM) is a recent term used in the security industry for a software product able to supervise multiple distinct systems. The primary function of a PSIM is to manage information coming from different systems and present them inside a single user interface.

As opposed to a unified platform, a PSIM does not generally have a built-in access control, intrusion, or video surveillance solution. Instead, it integrates different systems through proprietary SDKs and APIs. Compatibility challenges could also arise when one of the sub-systems requires an upgrade or maintenance. Additionally, every system integrated within a PSIM has to be configured separately and there is a great degree of redundancy and duplicated efforts, e.g., configuring users within a PSIM and the underlying access, video, and intrusions systems.

On the other hand, a PSIM integrates with a wider range of products because they "hand-craft" the system on top of multiple security systems within a corporation. Nonetheless, opting for a PSIM can be difficult and expensive.

According to John Honovich, founder of IPvideomarket.info, "The main challenge with PSIM is that it is expensive and requires high-touch to optimize and deploy. Most deployments cost in excess of $300,000 USD, a modest sum for a Fortune 500 company but generally unjustifiable for mass market use."[6]

The disadvantages of expensive custom integrations within a PSIM and the associated long-term support costs of such a highly customized product, have to be objectively considered against benefits such as the bridging of many underlying systems and an integrated user interface.

[6] Physical Security Information Management (PSIM), John Honovich, http://ipvideomarket.info/companies/PSIM

Are You Being Efficient, Flexible and Cost-Effective in The Way You Approach Video and Access Control Integration?

As you've read in the previous pages, there are many ways to deploy a physical security system that includes both video surveillance and access control. Although interfacing and integration are the most commonly deployed methods, open-platform unification offers the most efficient, flexible and cost-effective video and access control applications.

That is why it is important to take a moment to see if you are employing the most optimal method of unifying your video and access control systems. The answer could help you save time and reduce costs.

YES	NO	Does your integrated solution allow you to…
☐	☐	Connect to a single server using a single client application to access all your video and access control functions?
☐	☐	Use the same software to create badges, monitor access control events and create video recording reports?
☐	☐	Buy doors controllers and IP cameras from more than one manufacturer?
☐	☐	Maintain consistent user workflows for all security functions across all systems including acknowledging alarms, locking down a facility, or generating reports?
☐	☐	Configure the entire system using a single interface, instead of several user applications?
☐	☐	Consolidate the logging and configurations of events and alarms for both access control and video?
☐	☐	Conduct only one software upgrade when you need to upgrade your access and video security system?
☐	☐	Rely on a single manufacturer when you experience problem with the video and access control systems?
☐	☐	Offer your operators one training and have a single reference manual for the entire security system?

For more information on finding the best method to unify your video and access control systems, contact a Genetec representative at 1 (514) 332-4000 or marketing@genetec.com today.

References

Tracking People, Packages and Vehicles. February 1, 2009. Retrieved August 12, 2010 from Securitymagazine.com: http://www.securitymagazine.com/articles/tracking-people-packages-and-vehicles-1

Anderson, Richard. *Video and Access Control Integration: Why Your Access and Surveillance Systems Are Not On Speaking Terms*. March 25, 2009. Retrieved August 12, 2010 from Securityinfowatch.com: http://www.securityinfowatch.com/Features/video-and-access-control-integration

Gager, Russ. *Trends in Video Integration: The Need for 'Open Book' Design*. April 3, 2006. Retrieved August 8, 2010 from SDMmag.com: http://www.sdmmag.com/CDA/Articles/Feature_Article/f68791d49f06a010VgnVCM100000f932a8c0____

Gager, Russ. *Integration: The Suppliers' Perspective.* May, 1, 2006. Retrieved August 8, 2010 from SDMmag.com: http://www.sdmmag.com/Articles/Feature_Article/5fe2a2b7615fa010VgnVCM100000f932a8c0____

Gager, Russ. *Integration: The Integrators' Perspective*. May, 1, 2006. Retrieved August 8, 2010 from SDMmag.com: http://www.sdmmag.com/Articles/Cover_Story/2c1208583b09b010VgnVCM100000f932a8c0____

Gager, Russ. *Integration: The End Users' Perspective*. May, 1, 2006. Retrieved August 8, 2010 from SDMmag.com: http://www.sdmmag.com/Articles/Feature_Article/2d03d0b9adf1c010VgnVCM100000f932a8c0____

Gager, Russ. How To Improve Your Integrated System Projects. November 1, 2006. Retrieved August 8, 2010 from SDMmag.com: http://www.sdmmag.com/Articles/Feature_Article/6c179fe0f62fe010VgnVCM100000f932a8c0____

Georgia State University. CIS 8020 Definition of Systems Integration. Retrieved August 8, 2010 from http://en.wikipedia.org/wiki/System_integration

Hodgson, Karyn. Access Control: Feature Sets That Sell. July 1, 2010. Retrieved August 12, 2010 from SDMmag.com: http://www.sdmmag.com/Articles/Feature_Article/BNP_GUID_9-5-2006_A_10000000000000863557

Prokupets, Rudy D. *Finding Seamless Integration of Digital Video*. May 7, 2003. Retrieved August 12, 2010 from Securitymagazine.com: http://www.securitymagazine.com/articles/finding-seamless-integration-of-digital-video-1

Thomas, Beth. Industry View: Checklist for Converged Access Control. June 3, 2008. Retrieved August 12, 2010 from CSO Online: http://www.csoonline.com/article/375063/industry-view-checklist-for-converged-access-control

Zalud, Bill. Convergence 2.0. February 1, 2009. Retrieved August 8, 2010 from Securitymagazine.com: http://www.securitymagazine.com/articles/convergence-2-0

About Genetec

Genetec is a pioneer in the physical security and public safety industry and a global provider of world-class IP license plate recognition (LPR), video surveillance and access control solutions to markets such as transportation, education, retail, gaming, government and more. With sales offices and partnerships around the world, Genetec has established itself as the leader in innovative networked solutions by employing a high level of flexibility and forward-thinking principles into the development of its core technology and business solutions. Genetec's corporate culture is an extension of these very same principles, encouraging a dynamic and innovative workforce that is dedicated to the development of cutting-edge solutions and to exceptional customer care. For more information, visit genetec.com.

Genetec

2280, Alfred-Nobel Blvd., Suite 400
Montreal, Quebec, Canada
H4S 2A4

Tel.: (514) 332-4000 / Fax: (514) 332-1692
genetec.com / info@genetec.com

UnifiedPlatform_WP1EN