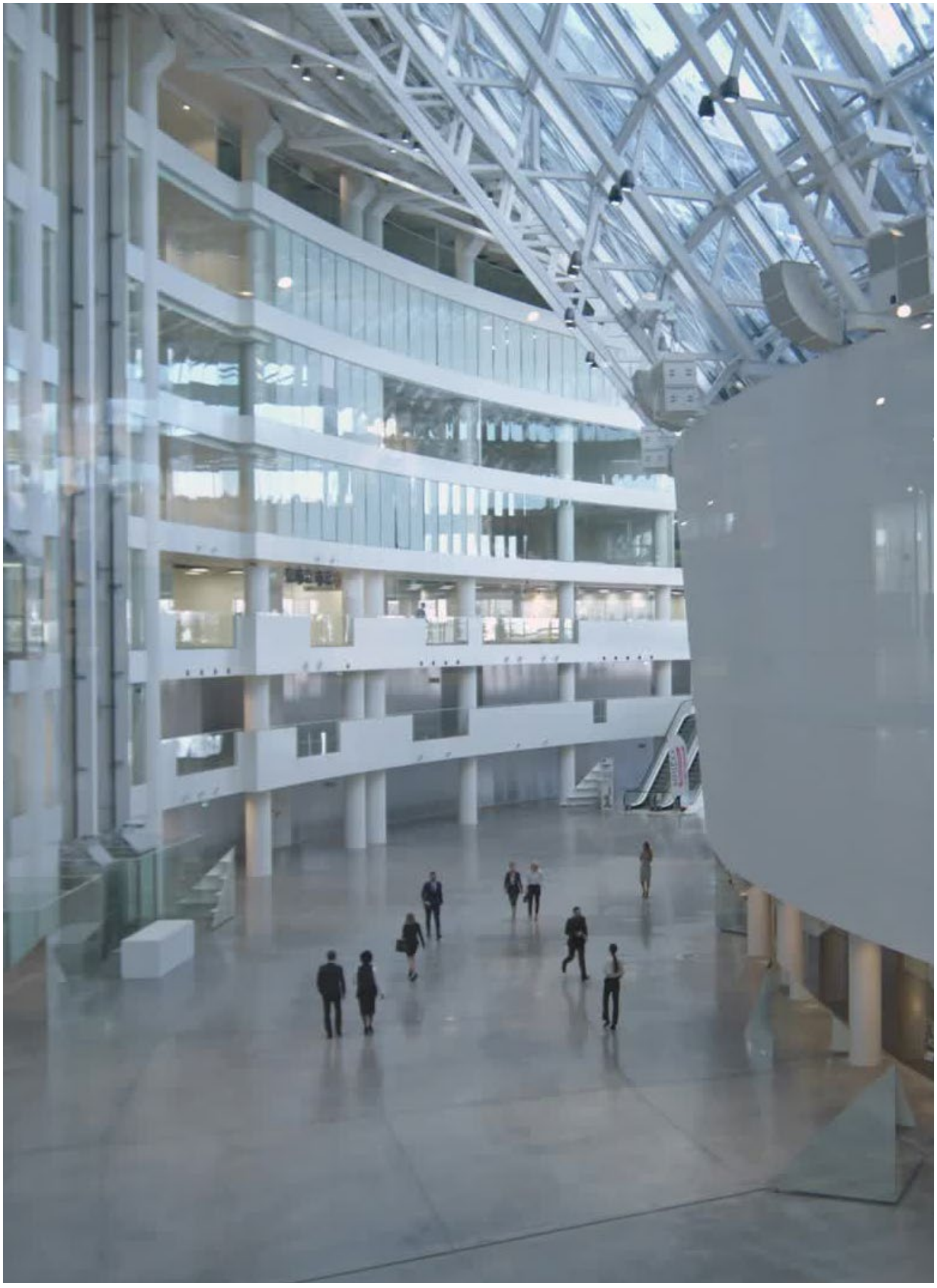
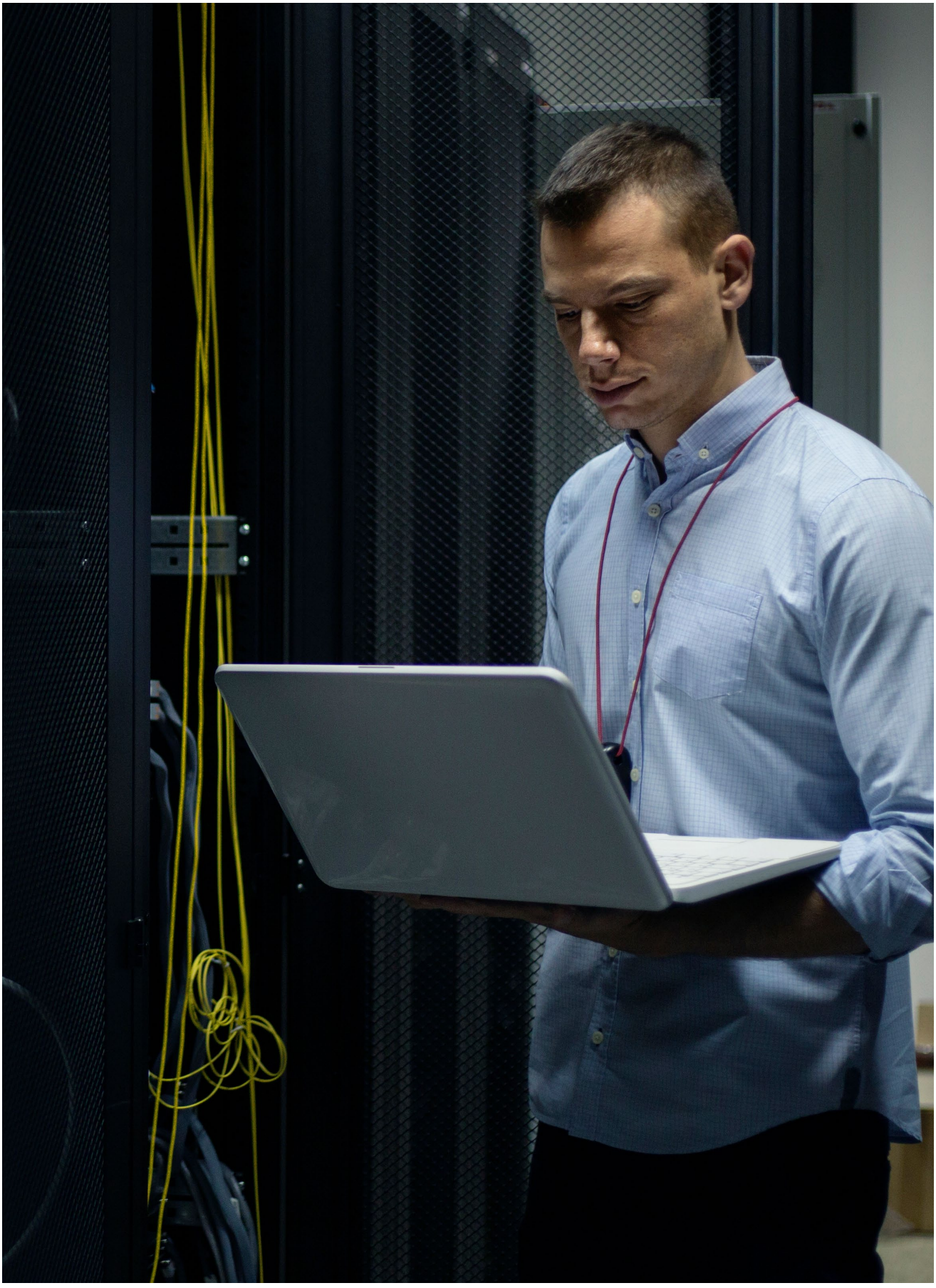
Whitepaper

Extending the lifespan of physical security through unification

Genetec™



Contents



Executive summary

Many organizations find themselves with proprietary solutions that are not meeting their evolving security needs. These solutions can be a serious liability as they try to respond to new, emerging security threats, a growing footprint, and increasing pressure from decentralization.

When looking to modernize their existing physical security system, organizations have to decide which is the best foundation for their new security infrastructure. There are two options available:

- Systems integration
- Unification

1

The journey towards modernization

The decision to modernize a physical security system is the first step in a multi-stage journey that can dramatically improve security and business operations for an organization. The journey towards modernization can be divided into four stages: expansion, connection, automation, and understanding.

Stage 1: Expansion

The first stage is increasing sensor coverage through a standalone security application. After deciding to modernize, an organization begins updating its infrastructure and increasing security by extending the range of its current system by adding in new hardware, including high-resolution cameras and biometric readers.

Stage 2: Connection

Then, once an organization realizes its goals for increased sensor coverage, they look for ways to augment security with data from other systems. At this stage, organizations work to connect different systems together, for example, connecting video surveillance and access control systems to increase the speed of access verification and investigation or bringing together video surveillance and communications to improve emergency response in public spaces.

Stage 3: Automation

The increase in the number and variety of sensors and the subsequent streaming of all that data through a single pane of glass leads to one application in the security system being bombarded, often in a non-prioritized manner, with massive amounts of information. As a result, security personnel become overwhelmed because they are not able to easily discern what data is important and actionable. At this stage, the organization needs to automate repetitive day-to-day tasks to help operators focus on what really matters.

93% of organizations that moved to a unified platform saw a decrease in compatibility issues across their security system.

Stage 4: Understanding

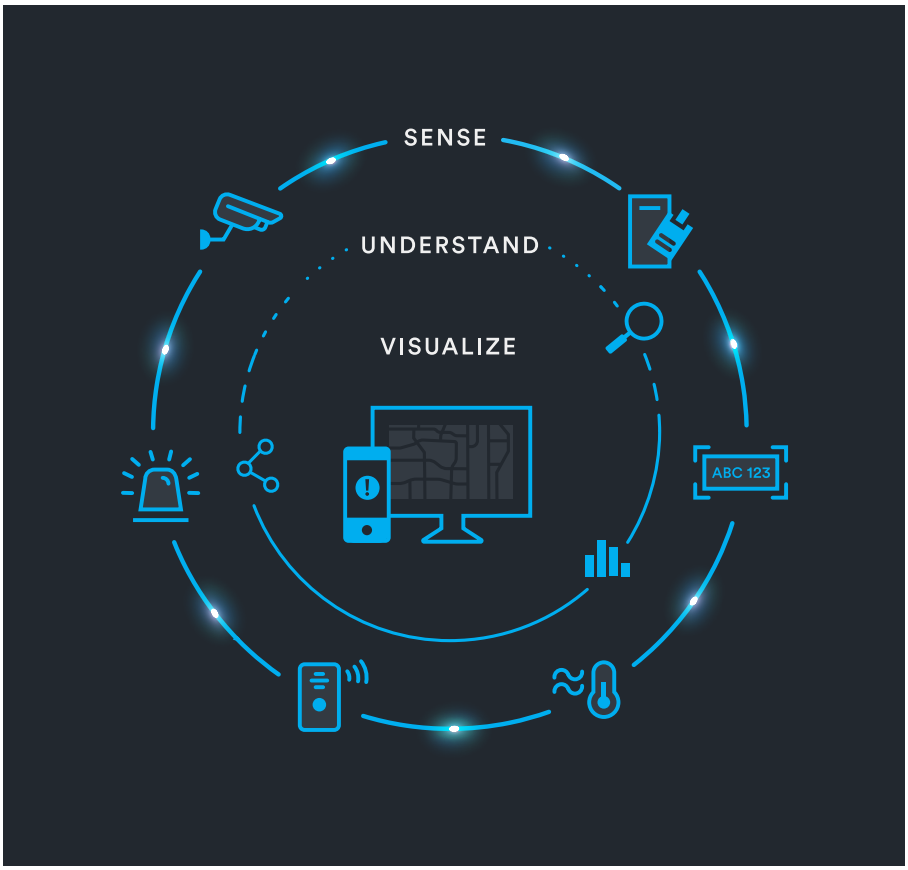
With all of this data being collected in its physical security system, an organization can now consider how to use this data to gather insights about its operations and processes. This stage of modernization is no longer just about security but is also about improving intelligence and business operations. The goal is to use the data collected in security systems as a potential competitive differentiator.

For most organizations, the journey towards modernization ends between stages 2 and 3. After increasing their sensor coverage with their new system and partially integrating some of their legacy sensors, maintaining this complex and precarious technology stack overwhelms their systems administrators. But, by adopting a long-term vision and using this opportunity for modernization to deploy a unified platform and solve larger issues related to scalability and lack of operational efficiency, organizations can reach the final stage and begin using data to drive business operations.

The main reason why the journey ends between the second and third stages for so many goes back to the foundation of their physical security system. When organizations begin modernizing, they often adopt a systems integration approach instead of choosing unification. While systems integration allows organizations to address immediate concerns as well as some short-term security challenges, it is not a long-term vision. As a result of the overhead involved with maintaining a solution built using this approach, organizations find themselves caught in a continual cycle of release, break, validate, and upgrade. They are not able to achieve greater business intelligence because they are having to spend time and money on maintenance as their core components constantly need to be upgraded on different release cycles.

According to a recent Genetec unification impact survey, 93% of organizations that moved to a unified platform saw a decrease in compatibility issues across their security system. By enabling the flow of data across all security and operational activities, unification empowers organizations to address the unique challenges in each stage of their journey. Implementing a single software platform that offers a single interface to manage core security systems, such as access control, intercom, intrusion, and video devices, is crucial. But, with the pace of innovation in the industry accelerating, the ability to bring in external sensors and data while maintaining a coherent, intuitive user experience is needed for true long-term sustainability.

In addition to protecting organizations from potential roadblocks in the short term, unification also helps them to expand their business by supporting long-term growth and evolution. Because an open, unified platform facilitates the flow and management of data across activities, organizations can move beyond traditional reactive physical security activities and towards improving their business operations.



Most integrated solutions will require operators to use multiple systems because none offer the required functionalities in one user interface.

2

Systems integration

Systems integration has become a popular substitute for traditional interfacing as a result of advancements in technology and increased collaboration between manufacturers. In the security industry, standard protocols and software development kits (SDK) are most often used to physically or functionally connect different computing systems and software applications.

Standard protocols are powerful and generally considered to be more effective than an SDK. They support a mix of operating systems and allow users to manage their applications in real-time. Standard protocols are popular for edge-device integrations, like IP cameras or door controllers, but are most commonly used between two software applications. However, as opposed to using an SDK, integrating two systems through a standard protocol is time-consuming and may require a shared database between the systems.

An SDK, also referred to as an application programming interface (API), consists of a DLL package created and distributed by software manufacturers that allows other manufacturers to integrate with their systems. SDKs simplify the integration by hiding complex mechanisms from other software developers, including authentication, video decoding, and complex standard protocols.

2.1 Benefits of systems integration

Regardless of the method of integration, integrated systems give users the tools they need to become more efficient. For example, an integrated access control and video management solution may display live or playback video associated with an access control event from the access control user interface.

Another advantage of systems integration is that organizations no longer have to rely on a single manufacturer for their entire security system. Working with integrated solutions allows them to deal with multiple independent vendors, each with its own ecosystem of technology partners. This reduces costs because, for example, if an organization is not satisfied with its current video management system (VMS), it can switch to another manufacturer without starting from scratch, as long as the new VMS is compatible with the other components in its security system.

2.2 Problems with systems integration

While systems integration can achieve a deeper level of product integration, there are some drawbacks to this approach.

Most integration solutions still require operators to use multiple systems because none of them independently offer the required functionalities in one user interface. Even when advanced functionalities are supported at the moment of installation, new features introduced by different vendors will not be usable in the primary system, preventing organizations from modernizing their processes gradually and overcoming new threats.

This means that there are instances in which an operator has to move back and forth between systems. For example, an operator might be required to perform pan-tilt-zoom (PTZ) in the VMS because that functionality is limited inside the organization's access control system (ACS). Other ACS limitations that could force operators to move between systems include not supporting camera sequences, difficulty searching through video recordings, and a lack of motion search capabilities.

Future maintenance and configuration are additional drawbacks to consider with an integrated system. Since the administrator has two or three independent systems to configure and keep synchronized, maintenance requires more time. The inefficiency of an integrated system is further increased because many of the necessary configurations are redundant, meaning that administrators have to perform the same tasks across multiple systems. Examples of this include security managers having to create accounts and specify privileges for users in multiple systems and security operators having to configure each new camera across multiple systems.

Organizations might also find it challenging to conduct upgrades and get support for their integrated systems. As manufacturers constantly change their software to support new functionalities, these changes can affect the way existing integrations work and can even cause integrated systems to lose compatibility, especially when they change their SDK or API. This has the potential to delay upgrades or force an organization to invest in reintegrating the affected systems.

Seeking support for an integrated solution can also be complicated. Because an integrated solution is comprised of different systems from different vendors, it can take time to resolve problems. The manufacturers, and often the integrator, first have to investigate the problem and figure out which system is not behaving properly. Then, they have to fix the issue, which could result in more delays depending on the relationship between the manufacturers.

3

What about PSIM?

As stated earlier, most organizations that decide to modernize their physical security systems do not move past the second stage in their journey as a result of increasing complexity and rising maintenance costs.

Physical security information management (PSIM) solutions can help organizations move to the third stage of their modernization journey. A PSIM is a software product that can supervise multiple distinct systems. Its primary function is to manage information from different systems and present that data in a single user interface.

A PSIM does not generally have a built-in access control, intrusion, or video surveillance solution. Instead, it is usually custom-built for an organization on top of multiple preexisting security systems and integrates them through proprietary SDKs and APIs. While this type of software is expensive to install, it is flexible because it can integrate with a wide range of security products.

This solution also helps to ensure that operators can manage all the data coming into the system in a scalable way. By installing a PSIM, an organization can design workflows to guide operator responses and create automated processes that do not require human intervention.

3.1 Problems with PSIM solutions

Organizations thinking about installing a PSIM should be mindful of potential compatibility issues, as well as the long-term costs associated with maintaining support for a range of highly customized products.

Because a PSIM relies on the same approach as traditional integrations, an organization can face compatibility challenges when one of the sub-systems requires maintenance or an upgrade. Additionally, every system integrated within a PSIM has to be configured separately. This leads to a high degree of redundancy and duplicated effort. For instance, when using a PSIM, an organization would have to configure users in the PSIM as well as in each of the underlying access control, video, voice communications, and intrusion systems. PSIM solutions are also static, which makes it very difficult to improve processes and workflow once the solution has been deployed.

4

Unification: the open, unified platform

An open, unified platform is a comprehensive software solution that helps organizations meet their immediate and long-term security needs. By offering seamless interconnectivity between multiple systems, including video, access, intercom, and intrusion, it provides everything security personnel need within a single, unified software suite.

4.1 Get the facts

Unification is also cost-effective. According to the Genetec unification impact survey, 77% of respondents said that unification reduced their infrastructure footprint, 78% said it improved maintenance costs, and 89% said it reduced maintenance time.

An open, unified platform costs less to purchase and maintain than custom-integrated solutions and also protects an organization's security investment through interoperability. With out-of-the-box interoperability, this solution targets the mass market by providing built-in support for commoditized security products without requiring customization for every installation. These commoditized products include IP cameras, DVRs, door controllers, alarm panels, intercoms, badge printers, active directory for authentication, and card management.

Since an open, unified platform supports commoditized products, hardware investments are also protected. If an organization is not satisfied with the unified software solution, it can change software components without having to reinvest in specialized appliances.

Even though customization is not necessary when deploying an open, unified platform, the platform still allows for 3rd party integration and customizations through an SDK or API. Because a unified platform is built around activities like monitoring and reporting and is not designed for a single technology, its interface seamlessly supports new integrations. With these types of tools,

A unified solution means users only have to learn, configure, upgrade, and backup a single software suite.

organizations can tap into existing integrations and also design and maintain custom integrations on their own instead of having to rely on the unified platform manufacturer

4.2 The unified server infrastructure

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
- schedules

Deploying a unified server infrastructure means that users only have to learn, configure, upgrade, and backup a single software suite. This makes installing and managing an open, unified platform easier than an integrated system. Access is also easier as administrators can manage the system through a single application, regardless of the number of servers or technologies. Then, with this connection, they can access all the services offered by the system as the data is stored in one central location.

Unification from the server to the interface offers distinct benefits for organizations, including:

- greater efficiency through the use of a single interface
- greater situational intelligence through automated event correlation across systems
- reduced costs through shared configuration and maintenance

4.3 The user experience

An open, unified platform also offers a single user interface for multiple security applications. As a result, switching from one application to another is seamless. This means that operators can easily and efficiently move from one security task to another, saving time and energy and improving security. According to the Genetec survey of customers who deployed unified platforms,

- 63% said they saw a major improvement in event detection
- 59% said they saw major improvements in response times

- 70% saw major improvements in the time needed to gather evidence and other relevant information

The common user interface also reduces the time required to train new operators on individual systems within the security infrastructure. According to the Genetec unification impact survey, 86% of respondents saw a reduction in the time spent in training for new operators and 88% reported a reduction in the number of operator errors.

All systems built on an open, unified platform also share common core functions. This means that alarm management, event to action, reporting, investigation, and incident-related workflows are all the same regardless of whether they are for video, access control, or voice communications. This significantly reduces the total number of workflows that operators need to learn and use.

4.3.1 Event correlation

Since events and alarms are managed by a single server infrastructure, a unified system offers event correlation by design. By correlating access and video events, for example, a unified platform allows operators to quickly validate a cardholder's identity when an access event occurs, to ensure the authenticity of their credentials. Event correlation can also significantly reduce response time by filtering out false alarms.

4.3.2 Ease of maintenance and support

A unified system is easier to upgrade and maintain than an integrated solution because it has a single software platform. Instead of upgrading multiple systems, an integrator only has to upgrade the platform, saving time and simplifying maintenance if support is ever required from the manufacturer. It also minimizes system downtime during upgrades. According to the Genetec unification impact survey, 83% of respondents reported a decrease in the time spent on individual technical issues and 53% said that unification had a major impact on maintenance.

4.3.3 The importance of integration

In the security industry, open, unified platform systems, unlike open, architecture systems, do not use industry standards to integrate with hardware from different manufacturers. This method of integration is accomplished by first building a generic integration layer that provides the most common functionalities and then developing a driver for each specific product the system integrates with.

In these systems, open, unified platform manufacturers are responsible for developing, testing, and maintaining integration with every device supported by their product. Open, unified platform systems tend to support a wide variety of manufacturers that offer similar functionalities and products that are commoditized. This strategy works well for specialized appliances because they have fixed, well-defined functionalities. With these types of systems, organizations also have the freedom to change software or hardware vendors without having to replace all of their existing security equipment.

5

Choosing a solution

Before beginning the process of modernization, organizations have to decide on the ideal foundation for their new physical security system. Although most organizations invest in systems integration, unification is a better option. In addition to offering the most efficient, flexible, and cost-effective applications, unification also gives organizations the confidence they need to undertake the multi-stage journey towards improved business operations and sustained long-term growth.


25
56

Genetec Inc. is an innovative technology company with a broad solutions portfolio that encompasses security, intelligence, and operations. The company's flagship product, Genetec™ Security Center, is a physical security platform that unifies IP-based video surveillance, access control, automatic license plate recognition (ALPR), communications, and analytics. Genetec also develops cloud-based solutions and services designed to improve security and contribute new levels of operational intelligence for governments, enterprises, transport, and the communities in which we live. Founded in 1997, and headquartered in Montréal, Canada, Genetec serves its global customers via an extensive network of resellers, integrators, certified channel partners, and consultants in over 159 countries.

Video surveillance: Achieve greater situational awareness and enhance security within your city with the ability to share cameras across agencies and organizations, providing a common operational picture and improving incident response time.

Access control: Heighten your organization's security, effectively respond to threats, and make clearer and timelier decisions with a unified, IP-ready platform, whether deploying a new access control system or updating an existing installation.

Automatic license plate recognition: Automate the detection of vehicles of interest, increase parking enforcement efficiency and accelerate public safety investigations through the ability to share license plate data with selected agencies and partner organizations, without forfeiting ownership and privacy.

Operational decision support: Create efficiency for incident handling and decision making with advanced workflows that guide operators from situation alerts through policy-based procedures to detailed case compilation export.

Investigative case management: Simplify case management and speed up investigations with a platform that allows you to centralize digital evidence and securely collaborate with investigators, outside agencies and the public.

Cloud services: Extend the capabilities of your on-premises security system and reduce IT costs with highly scalable, on-demand cloud services that allow your city to easily cope with rapidly changing security requirements and operate with greater efficiency.

Genetec Inc.
genetec.com/locations
info@genetec.com
@genetec

UPDATED:25-MAR-21