Plugin-based integration vs. true unification

Find out how integrated and unified security systems are different and why unification enables smoother growth and collaboration across your organization.

Integration refers to establishing some form of connectivity between two or more standalone systems. These can include video, access control, intrusion, intercom, automatic license plate recognition (ALPR), and various business and Industrial IIoT systems and sensors.

Unification, on the other hand, refers to having one platform that has all systems and capabilities embedded at its core. A unified platform is engineered from the start for different system components to work together. This offers a streamlined approach to how systems are managed, how data is shared, and how processes across your organization evolve.

How open architecture broadens all possibilities

A unified platform that is built on an open architecture is the pathway to unlimited possibilities. You'll get a unified user experience, with the flexibility to add integrations with various other technologies or systems. This allows you to really adapt and customize your deployment to suit your needs and preferences. Ultimately, strong integrations within a rich, unified platform helps you extract the most value from your investments.

Understanding how basic integrations and unification compares

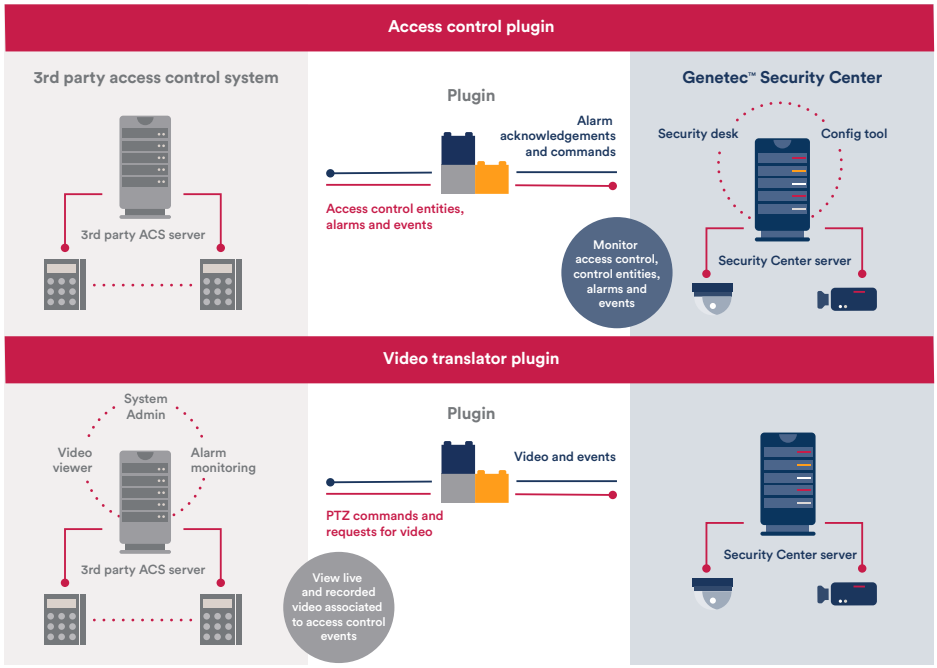
Plugin-based integration 	Unification 
Several disparate systems	ONE platform for video, access control, ALPR, intrusion, intercom, etc
Several user interface (UI) apps for configuring each	ONE UI for configuring all embedded systems
Several UI apps for monitoring each system with some exchange of information	ONE UI for monitoring video, access control ALPR, intrusion, intercom and all other capabilities
Possible inability to acknowledge another system's alarms within each system UI	ONE UI for managing all system events and alarms
Limited ability to link video and data within reporting tasks	ONE platform for consolidated reporting and business insights
Separate architectures, little to no consolidation	ONE unified platform and interface to train personnel on
Personnel must be trained on several systems	ONE service agreement to purchase and renew
Several service agreements to purchase and renew	ONE vendor contact for all system support
Must coordinate between vendors for support	ONE seamless upgrade experience with assured compatibility
Plugin integrations may not be compatible with system version upgrades	ONE platform from which to uphold cybersecurity best practices

Integration with a unification approach

If you don't have the right foundation, then integrations are just connections. What matters most is investing in a seamless, unified, open-platform experience. This will deliver a centralized view and enable better flow of data across all operator activities.

	Integration	Unification
Centralized Servers	✗ Having multiple separate systems will require more server and processing power, increasing hardware demands.	✓ A unified platform allows you to consolidate hardware resources, so you can deploy and maintain fewer servers.
Seamless Upgrades	✗ When you upgrade one system, you can run into compatibility issues with other linked systems.	✓ When you upgrade one system, you can run into compatibility issues with other linked systems.
Unified threat management	✗ When serious threats happen, operators may need to jump from system to system to piece information together. This slows emergency response.	✓ A unified platform provides all video and data in one view, and guides operators through operating procedures to help them efficiently respond to any situation.
Efficient and Consolidated Reporting	✗ Multiple reports must be generated and then manually consolidated to correlate events and alarms from different standalone systems.	✓ A unified platform offers consolidated reporting capabilities. You can automate or generate reports that include video linked with other system data for quick review.

How plugin-based integrations work



A plugin integration aims to bring different security applications together in the same UI. The challenge is that users won't always have access to the full scope of information or capabilities available within the connected system. These integrations are also prone to failure following upgrades, creating bigger issues for users as systems evolve.

For example, in some cases, an access control plugin will only display third-party access control entities, events, and alarms. A video translator plugin may only push video and events to a third-party access solution. In many cases, users may still need to log in to different vendor systems to handle monitoring, reporting, and configuration tasks.

The Genetec unified security experience

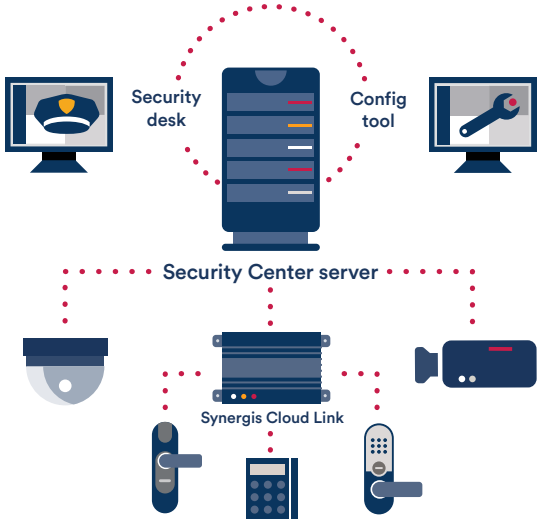
EVERYTHING IN ONE PLACE - Stop going back and forth between applications. Monitor video, access control, intercom, intrusion, and IoT within one unified experience.

EASY TO UPGRADE - When a new version of the unified platform is released, you'll get a hassle-free upgrade experience for all systems and capabilities embedded in the unified platform.

OPEN AND ADAPTABLE - Tap into an ecosystem of over 900 solutions and choose from a wide range of supported devices from leading technology vendors.

EFFICIENT DEPLOYMENT - Everything from entity configuration and user training to cybersecurity hardening happens in one unified platform. This minimizes the time and costs associated with getting your system up and running.

Genetec Security Center unified solution



The depth of integration with third-party plugins will vary. For more information on specific plugin integrations, including their capabilities and limitations, please speak to your Genetec representative.

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

UPDATED: 22-AUG-24