GeoVision GV-Cloud Technical White Paper

1. Executive Summary

GV-Cloud is a browser-based platform that unifies video surveillance and access control within a single operating environment. By reducing dependence on on-site infrastructure, the platform simplifies remote management and provides scalable visibility across cameras, controllers, doors, and users across multiple regions.

For video operations, **GV-Cloud VMS** supports direct-to-cloud camera deployments and ONVIF-based integration via the **GV-Cloud Bridge Series** (including Bridge and Bridge Pro). For access control, **GV-Cloud Access Control** offers a serverless solution to manage controllers, credentials, and alarms remotely. Operational awareness is further extended by the **GV-Cloud app**, which enables remote viewing, playback, and door control from mobile devices.

This unified architecture provides maximum flexibility: businesses can adopt direct-to-cloud setups for new sites, bridge existing ONVIF cameras, and centrally manage distributed facilities. Furthermore, **GV-VPN** and the **GV-Mobile VPN app** establish secure site-to-site and mobile connectivity without the need for standalone VPN infrastructure or complex router configurations.

Strategic theme	Source-supported platform claim	Implication for decision-makers
Unified operations	Single browser-based experience spanning cloud VMS and cloud access control	Fewer disconnected workflows across monitoring, alarms, events, and response
Deployment flexibility	Direct-to-cloud cameras plus ONVIF integration through the GV-Cloud Bridge Series	Supports both greenfield deployments and modernization of existing camera estates
Operational scalability	Unlimited hosts, users, and regions across cloud services	Better fit for multi-site organizations that need centralized oversight without local server sprawl

2. Why Cloud-Based Physical Security Is Gaining Strategic Relevance

Organizations managing multiple sites increasingly require security systems that can be monitored remotely, scaled efficiently, and updated without constant dependence on local servers or complex network reconfiguration. In many legacy environments, video surveillance, door access, alarms, and event response remain fragmented across separate systems and interfaces. This slows investigations, complicates administration, and raises the effort required to maintain consistent policy across locations.

GV-Cloud directly addresses these pressures. Rather than treating video surveillance and access control as isolated systems, GV-Cloud combines them into a cloud-enabled operating model with browser-based administration and mobile access. The resulting value proposition centers on centralized visibility, faster remote management, and infrastructure flexibility for organizations of different sizes.

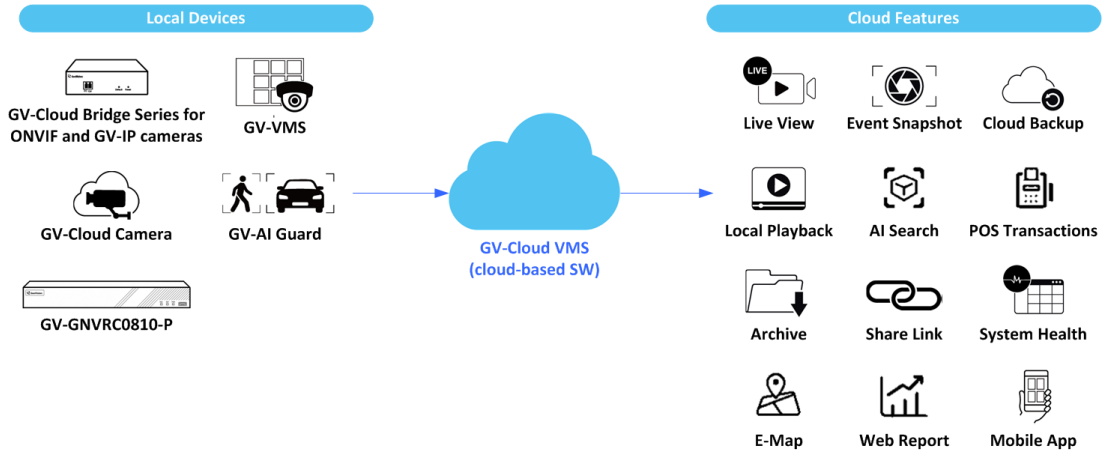
3. GV-Cloud Platform Overview

GV-Cloud is a VSaaS platform that combines video surveillance and access control into a single, browser-based management experience. The solution allows users to view and manage video and access operations remotely without relying on traditional, on-premises security management stacks for every use case.

- A browser-based management experience that unifies cloud video surveillance and cloud access control.
- Remote monitoring and administration of cameras, controllers, doors, users, logs, and events.
- Mobile extension through the GV-Cloud app for live view, playback, snapshots, push notifications, log queries, and door actions.
- Support for both direct-to-cloud architectures and integration of ONVIF-compliant cameras through the GV-Cloud Bridge Series.
- Region-based grouping and permissions that align administration with the structure of distributed organizations.

4. GV-Cloud VMS

GV-Cloud VMS is a cloud-based video surveillance and data center solution suitable for businesses of all sizes, capable of monitoring thousands of on-site cameras, alarm devices, motion triggers, and AI events through a single cloud-powered platform.



GV-Cloud VMS System Architecture

Deployment and integration model

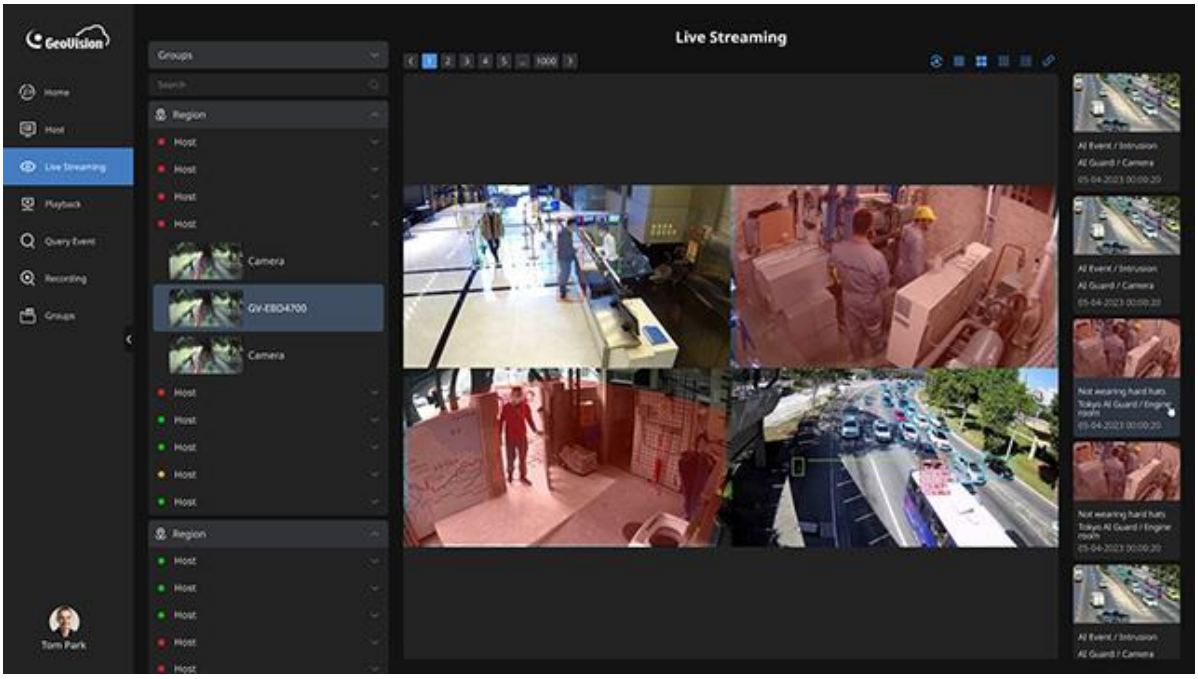
- Direct-to-cloud integration for supported AI analytics cameras with onboard storage, reducing the need for on-site NVR or VMS infrastructure in those deployments.
- Support for ONVIF-compliant cameras through the GV-Cloud Bridge Series.
- Integration pathways with local GeoVision software environments such as GV-VMS, GV-AI Guard, and GV-Recording Server.
- Cross-browser access through major modern browsers including Chrome, Firefox, Safari, and Edge.

Core capabilities

- Remote live view, playback, and event query through a web browser.
- AI event support and AI-powered search by people and vehicle attributes.
- Support for cloud backup plans with retention options including 3, 7, 15, 30, 60, 90, 180, and 365 days.
- Region-specific user and camera permissions to align monitoring access with corporate structure.
- E-Map support to visualize device locations and improve situational response.

Operational and resilience considerations

GV-Cloud VMS supports regional data processing and storage across multiple data centers, including the United States and the European Union. When a device connects to GV-Cloud, the system automatically detects IP location and stores data in the nearest appropriate data center. For decision-makers, this is relevant because it links cloud operations with data residency and operational localization considerations.

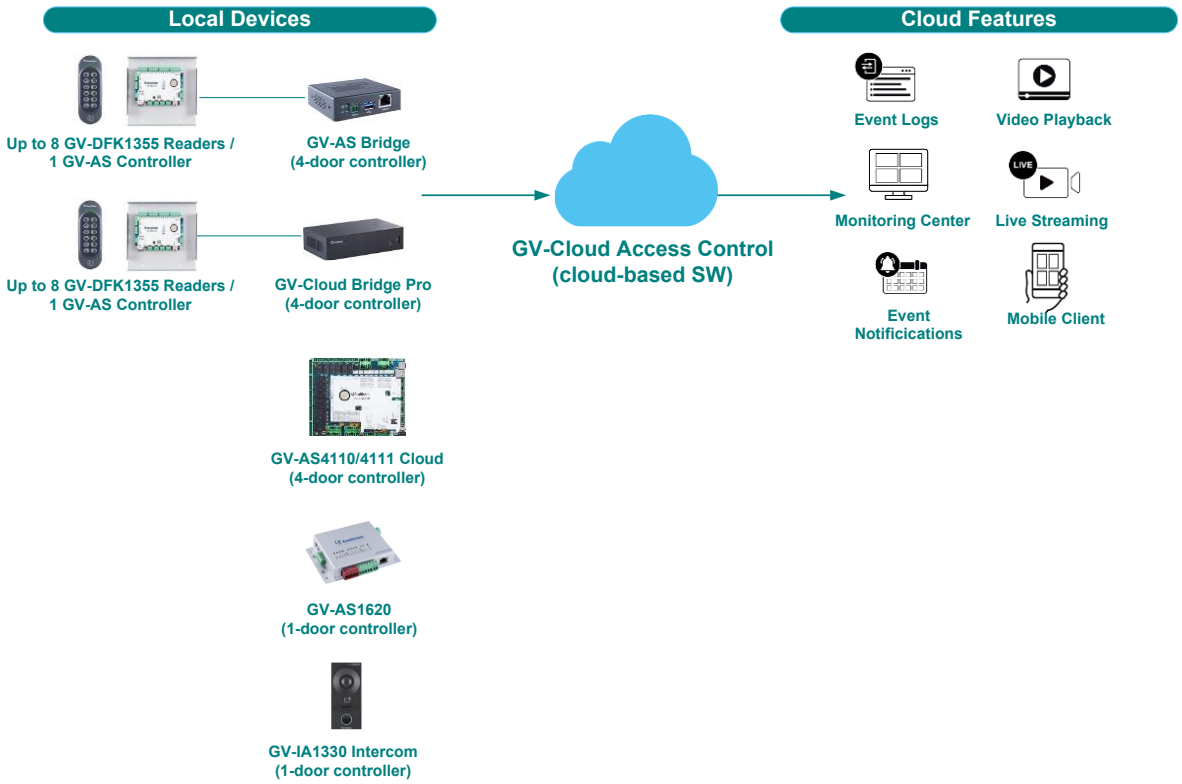


GV-Cloud VMS User Interface

VMS category	Source-supported details
Scale positioning	Suitable for businesses of all sizes; intended to monitor thousands of on-site cameras, alarm devices, motion triggers, and AI events.
Video access	Live streams, playback review, and event queries via web browser.
Cloud retention	Cloud recording plans cited at 3, 7, 15, 30, 60, 90, 180, and 365 days.
Resolution notes	Local playback supports up to 12 MP and cloud playback up to 8 MP.
Administrative structure	Unlimited hosts, groups, users, and regions supported.

5. GV-Cloud Access Control

GV-Cloud Access Control is a cloud-based access control solution that facilitates remote management and enhances security at all access levels. Easy to deploy with no need for on-site servers, GV-Cloud Access Control supports centralized monitoring of controllers and doors across distributed environments.



GV-Cloud Access Control System Architecture

Administrative and operational capabilities

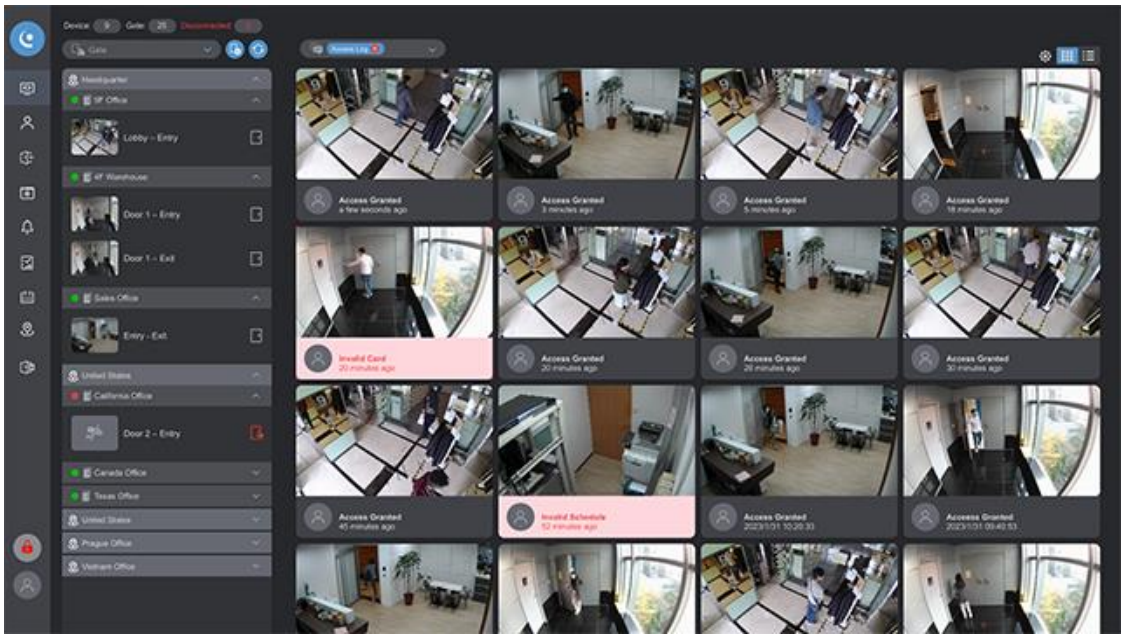
- Cloud configuration for controllers, doors, access rules, users, and cards.
- Unified remote management and monitoring of controllers and doors.
- Region-specific controller and door permission settings to match corporate structure.
- Batch enrollment of cards and users, including Excel-based import workflows.
- Log search across access and event activity, plus system and audit records.

Access modes, alarms, and response

- Supported access modes include card only, card plus PIN code, and passcode.
- Door alarm support includes Held Open, Force Open, Tamper, and Fire Alarm.
- Emergency lockdown enables rapid facility-wide door control in response to critical security events.
- Notification methods include e-mail plus mobile, web, and desktop push notifications.
- Video integration supports snapshots, live view, and playback for faster incident assessment.

Scalability and mobility

GV-Cloud Access Control supports unlimited hosts, user accounts, regions, and devices per region, together with up to 100,000 cards. Each user can be assigned up to 5 cards and 1 passcode, or up to 6 cards in total. Mobile access is supported through the GV-QR1352 reader and GV-Mobile Access app, with QR-code creation for temporary access. These capabilities are particularly relevant for organizations that must manage large user populations across multiple facilities while maintaining centralized visibility.



GV-Cloud Access Control User Interface

Area	Source-supported specification	Decision-maker relevance
Scalability	Unlimited hosts, user accounts, and regions; up to 100,000 cards	Supports large or growing estates without redesigning the management model
Credential model	Up to 6 cards per user and temporary access via QR code	Improves flexibility for visitors, contractors, and hybrid work scenarios
Alarming	Held Open, Force Open, Tamper, and Fire Alarm	Supports faster exception handling and incident visibility
Video linkage	Snapshots, live view, and playback integration	Helps operators investigate access events without switching systems

6. The Role of GV-Cloud Bridge Series in Hybrid Modernization

For organizations with existing camera deployments, the GV-Cloud Bridge Series devices provide a path to connect ONVIF-compliant and GeoVision IP cameras to the cloud environment.

- Connects ONVIF and GV/UA-IP cameras to GV-Cloud VMS.
- Supports motion-triggered snapshots and video attachments to GV-Cloud VMS from GeoVision IP cameras or third-party ONVIF cameras.
- Provides built-in VPN functionality that establishes a secure virtual network connection for the GV-Cloud Bridge Series, reducing the need for port forwarding.
- Enables cloud migration and remote administration without requiring immediate camera replacement across every site.
- Uses local USB storage for sending playback recordings to GV-Cloud VMS in supported scenarios.

In business terms, the GV-Cloud Bridge Series reduces modernization friction. It helps organizations extend cloud management principles to installed camera environments while preserving existing investment in compatible cameras. This hybrid deployment model can be valuable when budgets, site conditions, or refresh cycles do not support full greenfield replacement.

7. Mobile Experience and Operational Reach

The GV-Cloud mobile app allows operators to access GV-Cloud VMS hosts and GV-Cloud Access Control devices from mobile devices. Supported capabilities include push notifications, live view, playback, snapshots, door unlock, event log queries, and visitor call support in selected access scenarios.

- Remote awareness through event-triggered push notifications.
- Live and recorded video access for faster review outside the control room.
- Remote door actions and event queries for mobile operators or supervisors.
- Support for iOS and Android, with English, Japanese, and Traditional Chinese language support.

For distributed operations, this mobile layer extends the practical reach of centralized security administration. It allows designated personnel to stay connected to events and workflows without being physically present at a workstation or facility.

8. Security, Data Handling, and Administrative Control

GV-Cloud employs encrypted transmission, centralized cloud management, and regional data-center infrastructure. The following security and administrative capabilities are built into the platform.

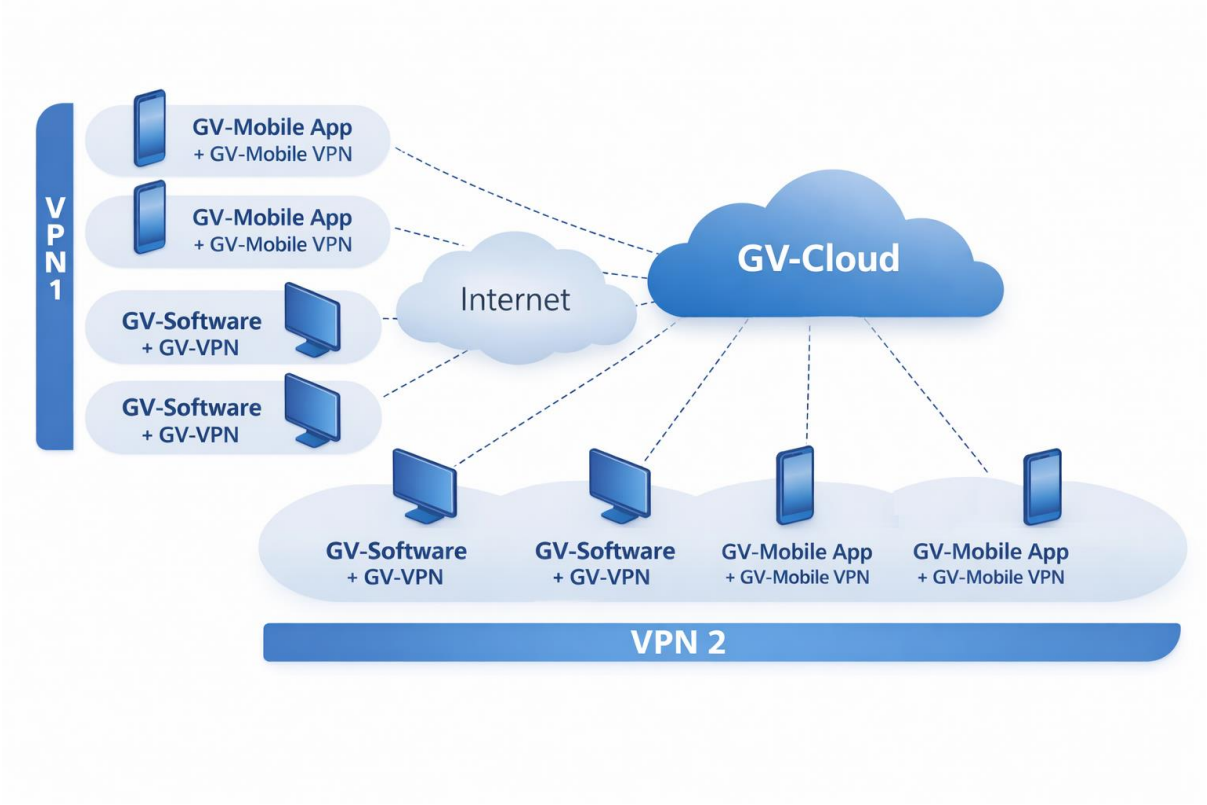
- HTTPS-encrypted transmission secures all data in transit.
- Database and transmission encryption protect access control data at rest and in transit.
- Regional data processing and storage span data centers in the United States and the European Union, supporting data residency requirements for GV-Cloud VMS deployments.
- Region-based permissions for users, cameras, controllers, and doors help align access privileges with organizational structure.
- Emergency lockdown, alarm monitoring, and video-linked event review improve response readiness in operational settings.

For executive stakeholders, the significance lies in combining remote accessibility with administrative control. Centralized permissions and cloud visibility can improve consistency across sites, while regional data-center handling may help organizations frame internal discussions about deployment locality, resilience, and governance.

9. GV-VPN: Secure Network Infrastructure for Cloud-Connected Sites

GV-VPN is the third core module of the GV-Cloud ecosystem, providing simplified secure network infrastructure that automatically bypasses NAT restrictions to achieve secure interconnections across network nodes. Together with the GV-Cloud platform, the **GV-VPN desktop utility** allows GeoVision desktop software running on separate PCs to connect to a virtual private network.

Multiple VPNs can be created on the GV-Cloud platform, enabling flexible and logically separated deployment across different teams or locations without requiring complex firewall configuration or manual port forwarding. Mobile devices can also join the same VPN through the **GV-Mobile VPN mobile app**, enabling GeoVision mobile apps to securely connect within the same network environment.



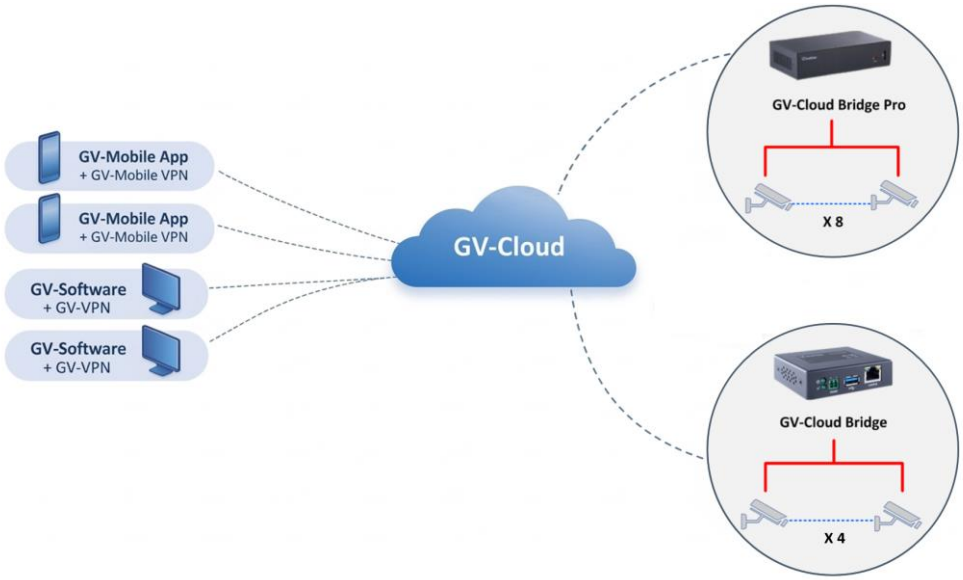
GV-VPN System Architecture

How GV-VPN works

GV-VPN utilizes the GV-Cloud platform to coordinate VPN provisioning and peer discovery. Once the GV-VPN desktop utility is installed, it registers with the cloud to automate connection establishment. This managed approach removes the requirement for static IPs, inbound firewall rules, or dedicated server infrastructure. It delivers secure, scalable site-to-site and node-to-node encryption while eliminating manual configuration overhead.

Integration with GV-Cloud Bridge Series

GV-Cloud Bridge Series provides **built-in VPN functionality** that extends network-level security to bridge-connected devices. When enabled, the bridge establishes a secure virtual network connection without requiring individual VPN configuration. This integration is particularly relevant in hybrid deployments where legacy cameras and access hardware are connected through GV-Cloud Bridge Series, allowing them to be remotely accessed without replacing or reconfiguring each endpoint.



GV-VPN Integration with GV-Cloud Bridge Series

IP Mapping allows individual devices on the same local area network as the bridge to be accessed through the VPN by mapping their IP addresses to VPN IP addresses. This provides individual VPN access to legacy devices that do not support VPN functionality.

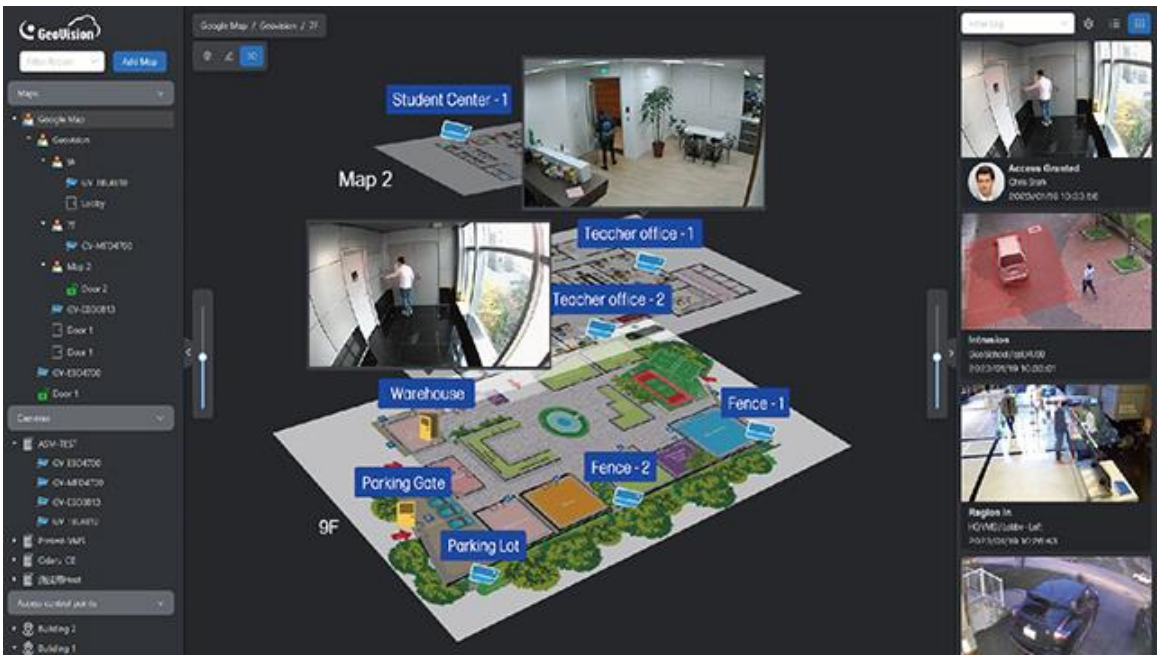
Key capabilities and decision-maker relevance

- Automatic NAT traversal eliminates per-site firewall configuration, reducing IT effort in distributed deployments.
- Multiple VPN environments can be provisioned from GV-Cloud, supporting logical network separation across teams, departments, or physical locations.
- The GV-VPN desktop utility connects GeoVision desktop software into the virtual network, extending the secure environment to existing workstation-based workflows without requiring a separate VPN client stack.
- VPN functionality on GV-Cloud Bridge Series provides a secure virtual network connection for bridge-connected devices without per-device VPN setup, making it well-suited for hybrid environments with legacy hardware.

For organizations where IT and security teams must maintain strict network boundaries between sites or user groups, GV-VPN provides a cloud-managed mechanism for enforcing those boundaries without deploying standalone VPN server infrastructure. This is particularly relevant in distributed environments where maintaining consistent network security policy across many locations would otherwise require significant per-site configuration effort.

10. Representative Use Cases

Use case	Why GV-Cloud may fit
Multi-site retail and branch operations	Centralized monitoring of stores, back offices, and entrances; remote incident review; simplified user and door management across locations.
Commercial offices and mixed-use facilities	Region-based permissions, mobile access, and video-linked access events for front desk, after-hours, and distributed tenant operations.
Education and campus environments	Unified management of cameras, alarms, doors, and lockdown-related workflows across buildings and zones.
Light industrial and logistics sites	Support for broad camera estates, event visibility, and remote administration over geographically distributed facilities.



3D E-Map Visualization Example

11. Evaluation Criteria for Decision-Makers

Organizations evaluating GV-Cloud should consider both business and technical fit. The following criteria provide a structured framework for the review process.

1. Assess whether the organization favors direct-to-cloud camera deployment, bridge-based modernization of ONVIF cameras, or a mixed model across sites.
2. Review data handling expectations, including desired cloud retention periods, geographic deployment considerations, and operational recovery requirements.
3. Map the intended administrative structure by site, region, user group, and security role to determine how region-based permissions should be configured.
4. Identify required integrations such as mobile access, video-linked access events, AI search, snapshots, or existing GeoVision software environments.
5. Confirm facility-level requirements for controller counts, card volume, temporary access workflows, alarm conditions, and door management scenarios.
6. Validate networking and storage prerequisites in bridge-assisted deployments, including supported camera models and local USB storage behavior where relevant.

12. Conclusion

GV-Cloud is best understood as a unified cloud operating model for physical security rather than a single isolated product. Its value lies in bringing together cloud video surveillance, cloud access control, mobile operations, and hybrid camera connectivity under a browser-based management experience.

For organizations seeking to modernize from fragmented or server-dependent environments, the combination of GV-Cloud VMS, GV-Cloud Access Control, GV-Cloud Bridge Series, and GV-VPN creates a credible modernization pathway. New sites can take advantage of direct-to-cloud options, while existing ONVIF estates can be integrated through bridge devices. Secure network connectivity between sites can be established through GV-VPN without deploying independent VPN server infrastructure. This flexibility, together with region-based administration and mobile reach, makes GV-Cloud a relevant platform for evaluating scalable, remotely managed physical security operations.