Verkada

Core Components of Software-First Physical Security

For IT leaders, managing physical security systems traditionally meant dealing with proprietary hardware like NVRs and DVRs that existed outside the modern IT stack. Today's cloud-based security solutions eliminate this legacy hardware, integrating seamlessly with existing IT infrastructure and SaaS platforms while delivering improved scalability and efficiency.

Hybrid-Cloud Architecture

A hybrid-cloud approach combines the best of both worlds: the reliability of on-premise systems with the flexibility and scalability of the cloud. This architecture reduces the need for outdated hardware like NVRs/DVRs, creating a solution that is easier to deploy and scale as needed. By using edge-based computing, systems can provide low-latency performance for critical operations while leveraging cloud-computing capabilities for centralized management, firmware updates, and AI-based analytics.

Centralized User Provisioning and Management

Centralized user management streamlines the setup and control of roles and permissions across interconnected security systems. Built-in support for identity management tools enables real-time user provisioning, while comprehensive audit logs maintain compliance and support investigations.

Enhanced Security Posture

Modern cloud-based security combines physical and cyber protection through robust features like end-to-end encryption, role-based access control (RBAC), and automated updates. This comprehensive approach proactively addresses vulnerabilities while multi-factor authentication (MFA) prevents unauthorized access, ensuring total organizational resilience against evolving threats.

MULTI-LAYER PROTECTION

- Physical Security
- Cyber Security
- Access Control Visualization
- Threat Prevention Indicators

Integration with Existing IT Systems

The shift to cloud-based physical security systems introduces a critical need for seamless integration with existing IT infrastructure, ensuring operational efficiency and cohesive workflows. Cloud-based systems can help teams make better use of APIs for integrating physical security data with other IT systems, enabling centralized analytics and streamlined operations.

APIs

APIs help ensure that physical security systems function as part of a unified IT ecosystem rather than as isolated components and can be used for:

- Accessing live and recorded video feeds for use with additional analytical tools or for redundant storage.
- Integrating door events and user access into broader organizational systems.
- Automating user provisioning and management, reducing administrative overhead.

Native Integrations

Native integrations make security systems adaptable and functional in the context of:

- Enterprise Resource Planning (ERP) systems that monitor and track asset movement within facilities.
- Student Information Systems (SIS) which link student/staff databases with the security system.
- Security Information and Event Management (SIEM) platforms that help centralize security information, alerts and logs for fast threat detection and response.

Data Privacy and Security

Data privacy and cybersecurity are paramount for any network-connected system. Traditional IP cameras systems often lack automated updates, making them cumbersome to maintain and leaving them potentially vulnerable to exploitation. Modern systems mitigate these risks with features that maintain robust defenses against evolving threats while supporting organizational compliance and privacy standards.

Encryption

All data, whether at rest, in transit, or stored in the cloud, is encrypted to prevent unauthorized access and provide data integrity.

Streamlined Access Management

Integration with SSO systems simplifies user authentication while maintaining rigorous security protocols, reducing the risk of credential-based breaches.

Zero Trust

By adhering to zero trust principles, cloud-connected security systems enforce continuous verification of users and devices, preventing lateral movement within the network and reducing the risk of insider threats.

Proactive Updates

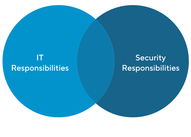
Automatic firmware updates address vulnerabilities as soon as they are identified, reducing exposure to potential exploits and ensuring system integrity.

Encryption Key Management

Gives the organization exclusive control over encryption keys, enhancing security and meeting stringent compliance requirements. This prevents even the cloud provider from accessing data.

Improved Collaboration Between IT and Security

Integrated systems align security and IT workflows, fostering collaboration and improving communication between departments. This alignment enables faster incident response times, more cohesive policy enforcement, and shared accountability for system performance. Collaborative platforms also simplify the deployment of new security policies and updates across an organization's entire infrastructure.



Minimized downtime

Faster deployment

Streamlined management

Reduced infrastructure

Cost-Effectiveness

Cloud-based systems can minimize downtime through the use of alerting, ensuring continuous security operations. Operational costs are further reduced through streamlined system management, faster deployment of new locations, decreased reliance on physical infrastructure, and less time spent on investigations and training.

AI Capabilities

Modern cloud platforms incorporate powerful AI features like video search and intelligent alerting. These tools make investigations faster and more accurate by automatically identifying relevant footage or notifying teams of unusual activity. For IT leaders, this reduces manual workloads and enhances situational awareness.

Regular Video Feed

AI-Enhanced Feed

Object detection

Face detection

Motion Analysis

Video Search: AI enables instant searches across video footage, allowing security teams to find specific events or individuals in seconds rather than manually scrubbing through hours of recordings.

Intelligent Alerts: AI-driven notifications identify unusual activity, such as unauthorized access or loitering, and alert teams in real time. This proactive approach minimizes response times and prevents incidents from escalating.

Pattern Recognition: Machine learning algorithms identify patterns and trends in security data, helping organizations detect recurring issues or potential vulnerabilities before they become critical problems.

Incident Management: Automated tools assist in compiling reports, archiving relevant footage, and analyzing incidents, streamlining investigations and improving outcomes.