Verkada

Upgrading Security for an Unpredictable World

A leadership guide to modernizing enterprise physical security infrastructure

Table of Contents

Introduction

Imagine investing in cutting-edge cameras or access control systems, only to have their potential stifled by outdated infrastructure.

This is the reality for many organizations still relying on legacy physical security systems. These antiquated solutions are more than a frustration—they create vulnerabilities. Unreliable hardware, limited investigative tools, and clunky management interfaces force physical security teams to work harder to achieve less. Meanwhile, other industries have embraced the power of the cloud to deliver scalability, efficiency, and innovation, leaving physical security struggling to catch up.

The hesitation to adopt cloud-based solutions has long been rooted in understandable concerns. Questions about bandwidth usage, network reliability, and the critical nature of security systems created barriers to change. However, advances in technology have removed these obstacles. Innovations like bandwidth optimization, hybrid-cloud architectures, and advanced cybersecurity measures have redefined what's possible, offering organizations the ability to modernize without compromise. The result? Physical security systems that are not only scalable and resilient but also simpler to manage.

Yet the problem goes deeper than outdated hardware. It's about an outdated change management approach as well. Too often, organizations focus solely on improving individual devices, neglecting the larger system architecture that ties them together. A state-of-the-art camera is only as effective as the infrastructure that supports it. If systems can't scale seamlessly, update effortlessly, or provide real-time visibility, even the most sophisticated devices will fall short.

The beauty of modern security infrastructure lies in its ability to break down the walls that have traditionally separated physical security from IT systems. Gone are the days of security operating in its own silo, with separate tools, separate teams, and separate headaches. Today's modernized systems speak the same language as your IT stack, integrating with everything from employee directories to point-of-sale systems. This isn't just about making things easier—it's about creating a unified security ecosystem that's greater than the sum of its parts.

The stakes have never been higher. Security threats are growing more sophisticated and unpredictable, and organizations are increasingly reliant on interconnected systems to safeguard their people and assets. Modernizing physical security infrastructure isn't just an opportunity—it's a necessity. By embracing cloud-based solutions, organizations can unlock a new era of resilience, efficiency, and control, positioning themselves to thrive in an unpredictable world. For those ready to lead, the time to make the transition is now.

If systems can't scale seamlessly, update effortlessly, or provide real-time visibility, even the most sophisticated devices will fall short.

The Core Components of Modern Enterprise Physical Security

The signs are impossible to miss: security threats now emerge from every direction, often morphing faster than traditional systems can track. A modern enterprise security system incorporates advanced technologies, scalable infrastructure, and comprehensive management tools to mitigate physical and digital threats—and operational challenges. They address the cumbersome nature of traditional systems through the reduction of on-premise hardware like NVRs and DVRs. These components of legacy systems are often difficult to use, prone to failures, and costly to maintain.

In contrast, cloud-based solutions can improve scalability and capability; integrate seamlessly with an organization's IT stack; work alongside SaaS platforms; and offer predictable, SaaS-like costs. This approach streamlines operations and management of the system, and often leads to greater collaboration between IT and security teams—creating a more unified overall security posture.

While these objectives are clear, turning them into tangible outcomes requires thoughtful planning, innovative approaches, and strategic implementation. The following pillars are critical to delivering an effective and scalable modern physical security system.

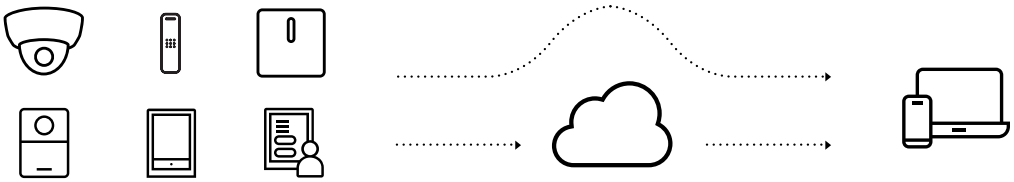
A hybrid-cloud approach combines the best of both worlds: the speed and reliability of on-premise systems with the flexibility and scalability of the cloud.

Hybrid-Cloud Architecture

In a survey by Verkada in partnership with The Harris Poll, 92% of physical security and IT leaders identified the cloud as the future of the industry.[1] While purely cloud-based solutions offer operational flexibility and centralized management, they also present challenges like increased reliance on networks and high bandwidth usage.

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

With this architecture, systems retain data both on-device and in the cloud, allowing for minimized reliance on network connectivity and reducing bandwidth usage to help ensure optimal performance even during network interruptions. Automatic, over-the-air software and firmware updates keep devices up to date and secure, while real-time device health monitoring alerts security teams of potential issues. Remote management capabilities further empower teams to access systems, share information, and manage devices from anywhere.



Centralized User Provisioning and Management

As systems become larger and more complex, simple user provisioning and management becomes critical. Cloud-based solutions simplify this process, making the setup and management of roles and permissions easier.

Remote provisioning capabilities allow administrators to onboard or remove users in real time, maintaining up-to-date access controls. Additionally, auditing and logging features provide visibility into user activity, supporting compliance and investigative workflows. By centralizing these functions, organizations can reduce complexity and enhance operational efficiency.

All of this is achieved by supporting and integrating with tools that help secure and streamline identity management, including:

Single Sign-On (SSO): Enables secure, authenticated one-click access across systems.

SCIM (System for Cross-domain Identity Management): Automates provisioning and deprovisioning of users from a central database.

SAML (Security Assertion Markup Language): Simplifies authentication across integrated systems and applications.

Multi-Factor Authentication (MFA): Adds an additional layer of security to user logins by requiring multiple forms of authentication.

1. Verkada. (2024, June 4). *The State of Cloud Physical Security.* Verkada. https://www.verkada.com/report-state-of-cloud-physical-security/

Integration with Existing IT Systems

The shift to cloud-based physical security systems introduces a critical need for seamless integration with existing IT infrastructure, to help maintain operational efficiency and cohesive workflows.

APIs

APIs are essential for integrating physical security data with other IT systems, enabling centralized analytics and streamlined operations. With such a broad range of use cases, APIs are the backbone of integrations. They ensure that physical security systems function as part of a larger unified, customized IT ecosystem rather than as isolated components, and support capabilities such as:

- 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.

Pre-Configured (Native) Integrations

Alongside APIs, industry-specific integrations can be offered to meet a diverse range of operational needs. Native integrations like the above make security systems adaptable and functional out-of-the-box. Examples include:

Point of Sale (POS): Synchronize video footage with transaction data to aid in fraud and theft investigations, reducing shrink in retail organizations.

Enterprise Resource Planning (ERP) systems: Monitor and track asset movement within facilities, providing a comprehensive view of inventory and logistics.

Student Information Systems (SIS): Link student and staff databases with the security system, improving safety in educational institutions.

Security Information and Event Management (SIEM) platforms: Centralize security information, alerts and logs for fast threat detection and response.

Electronic Medical Record (EMR) systems: Integrate with hospital or medical provider databases to improve patient safety and security.

Inventory Management systems: Enhance visibility and oversight of physical assets in warehouses.

Supply Chain Management (SCM) systems: Get deeper insights into critical areas that can cause disruptions in the supply chain.

Workflow Management tools: Streamline operational processes by linking security events with task and project management platforms.

Data Privacy and Security

Data privacy and cybersecurity are paramount for any network-connected system due to the amount of sensitive, private data security systems contain. Traditional IP cameras systems often lack automated updates, leaving them potentially vulnerable to exploitation unless manually (and actively) maintained. These measures allow modern physical security systems maintain robust defenses against evolving threats while supporting organizational compliance and privacy standards:

Zero Trust: Zero Trust principles[2] center on the concept that, by default, no user, device, or network is trusted without proper authentication and authorization. Network segmentation helps enforce this by isolating different parts of the network and limiting access unless explicitly authorized. This approach reduces the risks of cyberattacks by protecting against vulnerabilities in interconnected IoT devices.

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

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

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

2. CrowdStrike. (2025, January 5). Zero trust security: Principles, benefits, and implementation. CrowdStrike. https://www.crowdstrike.com/en-us/cybersecurity-101/zero-trust-security/

Key Benefits of Cloud-Based Physical Security Systems for IT Teams

Scalability for Enterprises

Cloud-based systems scale seamlessly, allowing enterprises to expand their security infrastructure as needed. These systems reduce the need for complex and costly server upgrades, providing flexibility and reducing deployment time. Additionally, cloud systems can adapt to fluctuating security demands, such as temporary construction sites or high-traffic areas, without the need for extensive infrastructure investments like NVRs and new ethernet wiring.

Operational Efficiency

Centralized management allows IT teams to monitor and maintain systems efficiently. These platforms enable streamlined oversight of multiple sites, reducing the complexity of managing disparate systems. Automated updates help devices remain up to date with the latest security patches and features, minimizing manual interventions and reducing downtime. Real-time alerts provide immediate visibility into critical issues, enabling teams to address potential threats or technical problems swiftly.

Ability to Delegate to Distributed Teams

A critical benefit for enterprises is the simplified delegation of security system ownership to remote locations, while still maintaining global visibility into the system. Central IT teams can reduce the burden of managing dispersed individual systems by enabling local teams to handle routine tasks like granting access or responding to incidents. Meanwhile, the central team can retain oversight for complex issues and facilitate compliance across all sites.

Ease of Use

Many modern cloud-based systems are designed with the user-experience in mind, focusing on intuitive interfaces that streamline day-to-day operations for IT professionals and security administrators. This focus on usability enables IT teams to spend significantly less time configuring the system, troubleshooting, and training end-users. With clear, user-friendly interfaces, security personnel require less time for onboarding and can quickly adapt to the system. Additionally, the usability alongside the remote access capabilities of a cloud-based system allows teams to access critical video footage and investigate and respond to incidents quicker and from anywhere.

> Cloud systems can adapt to fluctuating security demands, such as temporary construction sites or high-traffic areas, without the need for extensive infrastructure investments like NVRs and new ethernet wiring.

Enhanced Security Posture

By combining robust physical security with advanced cybersecurity measures, cloud-based systems deliver comprehensive protection against both external and internal threats, ensuring an organization's resilience in the face of evolving risks. Features such as end-to-end encryption, role-based access control (RBAC), and automated software updates help ensure that vulnerabilities are proactively addressed. The integration of multi-factor authentication (MFA) further secures access to critical systems, reducing the risk of unauthorized entry and enhancing organizational resilience.

Cost-Effectiveness Over Time

Reduced hardware dependencies, lower maintenance costs, and eliminating expenses associated with traditional on-premise solutions contribute to significant long-term savings. A total cost of ownership (TCO) analysis by SecurityInformed.com found that a cloud-based security system could offer a 35% savings over an on-site NVR enterprise system for an expected 5-year life of the system.[3] Cloud-based systems can also minimize downtime through the use of alerting (e.g., getting notified anytime a device goes offline), promoting 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. These savings allow organizations to allocate resources to other strategic priorities.

Minimized downtime

Streamlined management

Reduced infrastructure

Faster deployment

3. SecurityInformed. (2022, June 16). The total cost of ownership of true cloud video surveillance. SecurityInformed. https://www.securityinformed.com/insights/total-cost-of-ownership-true-cloud-video-surveillance-co-12058-ga-co-1616048003-ga.1655380280.html

Total Cost of Ownership (TCO) of cloud-based physical security systems

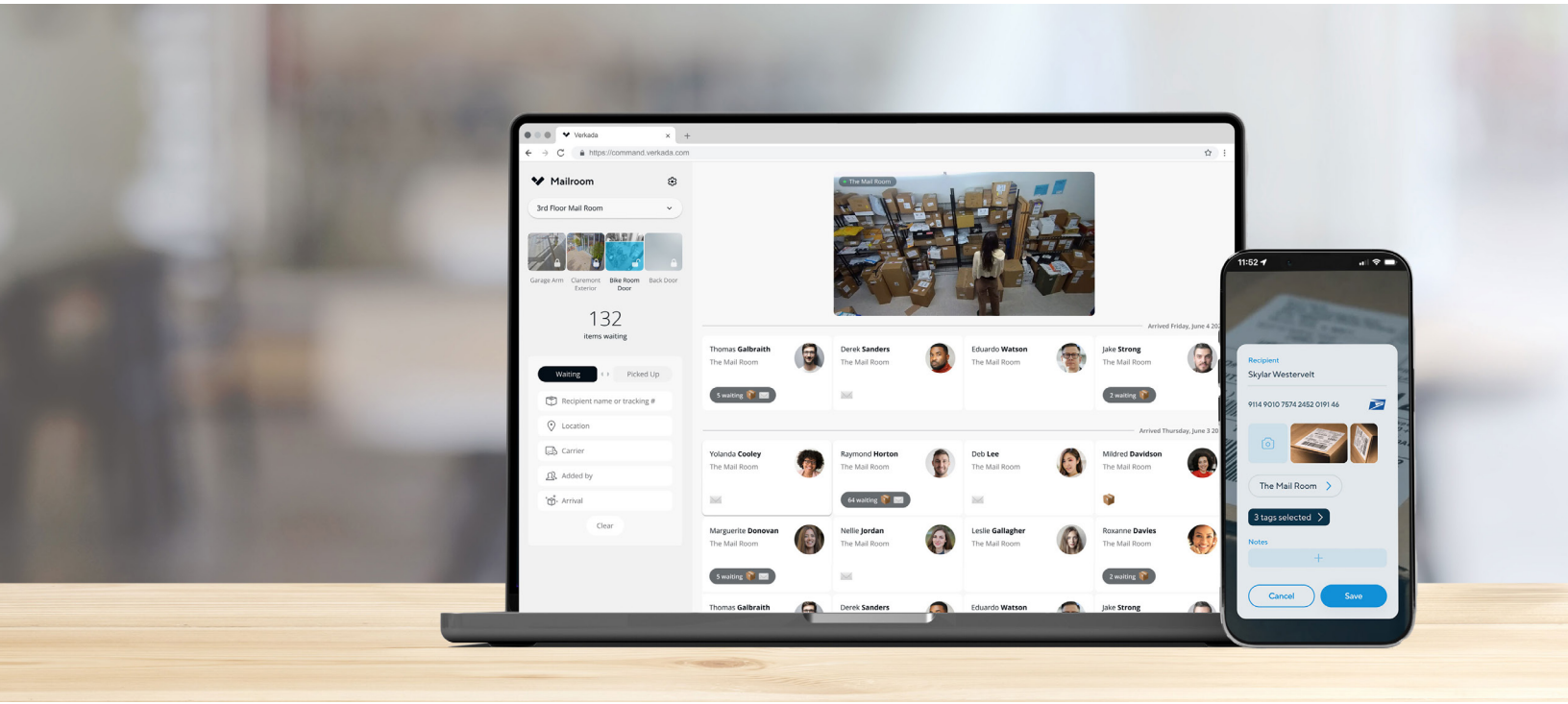
Compared to traditional systems

Source: SecurityInformed.com

Lower for small businesses

Lower for large commercial businesses

Lower for multi-site retail operations



Improved Collaboration Between IT and Security

Integrated systems align security and IT workflows through joint ownership of the system, 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.

AI Capabilities

Cloud-based systems leverage AI-powered tools to revolutionize how organizations approach security management and investigations. These advanced analytics are made possible through the huge computational power of the cloud. Without the resources of the cloud, implementing these features would be impractical and limited.

How cloud-enabled AI has become a part of critical security workflows

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.

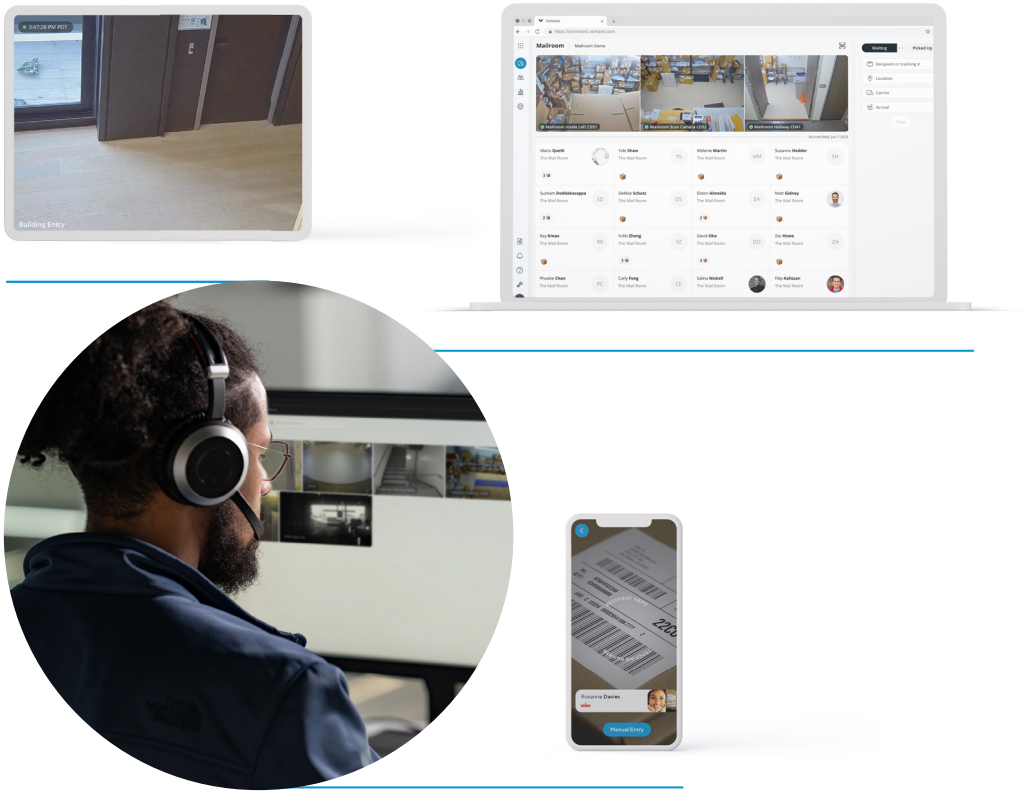
Incident Management: Automated tools assist in compiling reports, archiving relevant footage, and analyzing incidents, streamlining investigations and improving outcomes.

Key Benefits of Cloud-Based Physical Security Systems for Physical Security Teams

While cloud-based systems provide IT teams with enhanced security and streamlined infrastructure, they also confer significant advantages for physical security professionals. These benefits enhance day-to-day management and improve the effectiveness of security operations.

Manage from Anywhere

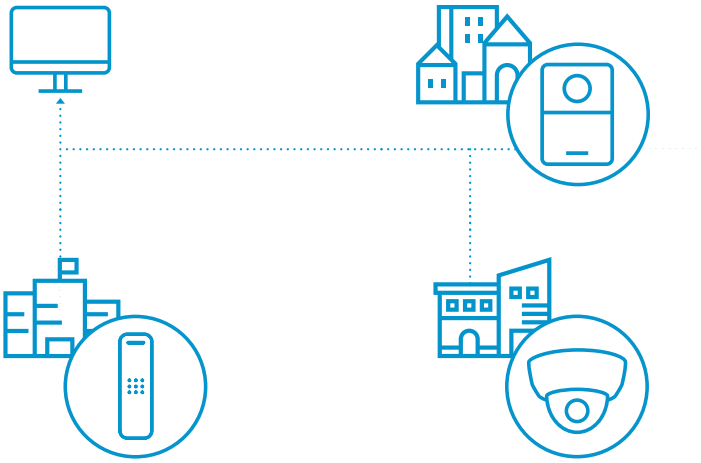
Cloud-based systems allow security professionals to monitor and manage systems remotely. Whether accessing live feeds, responding to incidents, or making adjustments to settings, the ability to operate from any internet-enabled device promotes quicker decision-making and enhanced responsiveness.



Centralized View Across All Sites

For organizations with multiple locations, cloud-based systems provide a unified platform to monitor all sites in one interface. This centralized view simplifies oversight and increases consistency in security practices across the entire organization.

Additionally, local teams are able to handle site-specific needs such as conducting investigations, managing alerting workflows and responding to incidents. By maintaining centralized oversight while delegating every day operations to local teams, organizations achieve a balance of control and efficiency at every level.

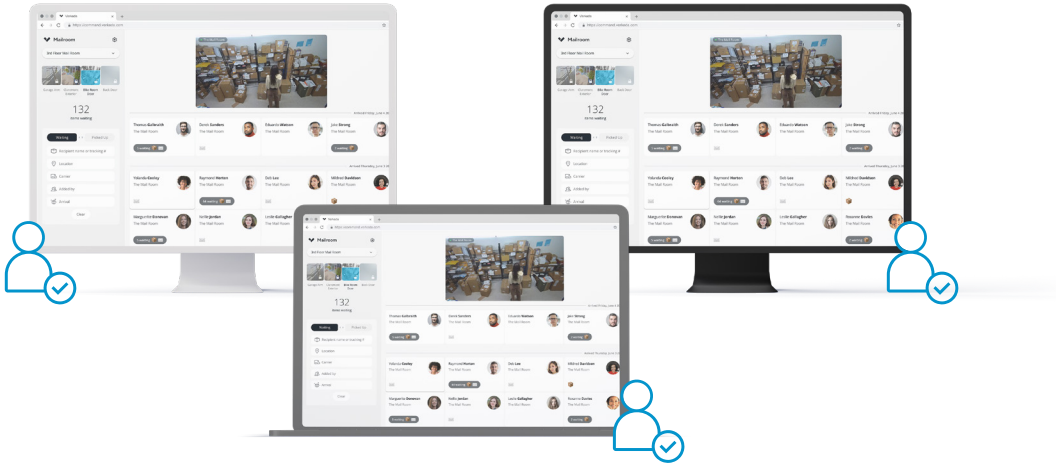


Leveraging AI Capabilities for Investigations

Modern hybrid-cloud platforms utilize computer vision (CV) to incorporate powerful AI features like natural language video search and intelligent alerting. These tools help make investigations faster and more accurate by automatically identifying relevant footage or notifying teams of unusual activity. All of this is designed to allow physical security leaders to reduce manual workloads and enhance situational awareness for better day-to-day operations.

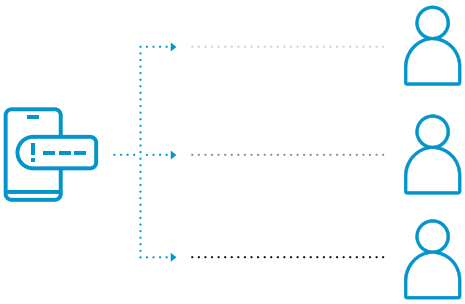
Standardized Systems for Simplified Training

A standardized, cloud-based security system allows all team members across distributed sites to work with the same tools and workflows. This consistency simplifies training and reduces the learning curve for new hires, improving overall team efficiency.



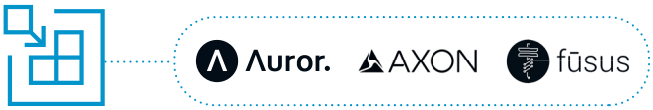
Sophisticated Alerting Workflows

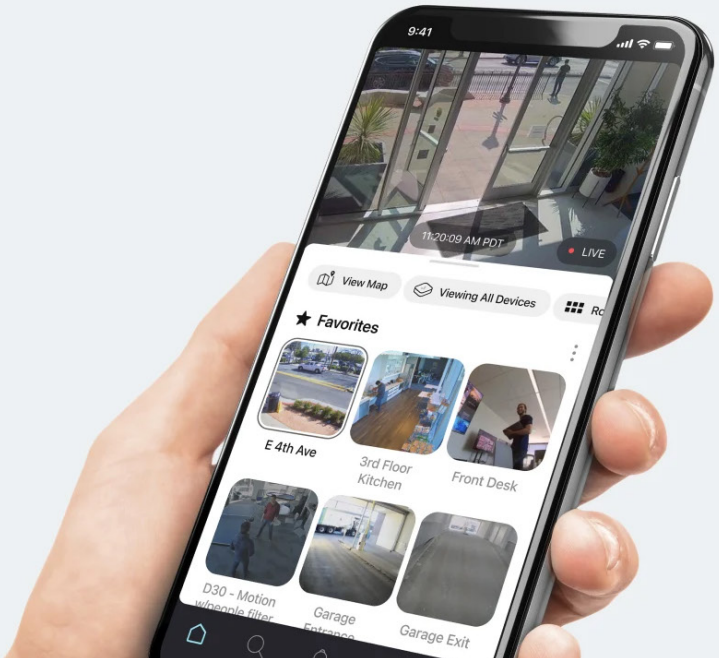
Cloud systems enable advanced alerting capabilities, including customizable workflows. Alerts can be routed to specific individuals, teams, or centralized operations centers (e.g., GSOCs) based on predefined criteria. This helps ensure that the right people are informed at the right time.



Seamless Integration with Other Systems

Integrations with other cloud-based physical security tools, such as incident management platforms (e.g., Auror, Fusus, Axon), enhance operational efficiency. These integrations allow physical security teams to consolidate workflows and create a more cohesive approach to managing security events.





Key Benefit of Cloud-Based Physical Security Systems for Operations Teams

Enhanced Observability with APIs

Modern cloud-based systems offer advantages for operational teams by enhancing observability and centralizing analytics through the use of APIs. By leveraging customizable API calls, organizations can extract data from distributed sites to gain operational insights, maintain detailed logs, and streamline workflows. This improved observability at scale empowers close monitoring of trends, identification of inefficiencies, and optimization of security operations through data-driven decisions.

By leveraging customizable API calls, organizations can extract data from distributed sites to gain operational insights, maintain detailed logs, and streamline workflows.

Cloud Transition Strategies

While the benefits of a cloud-based system make them an increasingly compelling choice, the prospect of transitioning an entire legacy system to this new architecture can be daunting. Making this transition requires careful planning and a strategic approach to change management tailored specifically to an organization's needs. Outlined below are key strategies and considerations for guiding this process.

Approaches to Deployment

Organizations transitioning to a cloud-based security system may choose one of the following deployment strategies:

New Deployments

For new locations without existing systems or infrastructure, the absence of a legacy system provides a unique opportunity to design a security system from the ground up with cloud-based solutions in mind. This type of deployment is fully optimized for future-forward technology, avoiding the limitations and challenges of retrofitting older equipment. However, if an organization has other sites and buildings that are still operating legacy systems, integration strategies (below) must be implemented to ensure consistency in operation across all locations.

Some organizations may choose to pilot cloud transition specifically with a new deployment and use it as a proof of concept before strategically deploying to the rest of their sites.

Complete Rip and Replace

A comprehensive rip and replace approach involves replacing all components of the physical security system at the same time. This method is often chosen by organizations aiming to standardize technology across all sites for consistency, resolve issues with outdated infrastructure that no longer meets operational or compliance requirements, and shorten the overall transition timeline to achieve rapid modernization. While this approach is the fastest way to achieve full system modernization, it requires significant upfront investment and careful planning to minimize operational disruption.

Phased/Hybrid Transition

While a complete replacement of the system may be the desired outcome for many IT and security teams, things like budget and operational downtime may prevent a full rip and replace from being a viable strategy. Instead, organizations may choose a phased approach that replaces legacy systems incrementally.

It is critical to note that during the phased transition there will be a combination of both modern and legacy systems for an extended period of time. This will require additional collaboration and effort among teams to manage and integrate disparate systems throughout the transition process (see the **Integration Approaches for Phased Transition** section for strategies used to manage this challenge).

Below are some of the common variations of the phased approach:

Time-Based Replacement

With this strategy, upgrades are made systematically across departments, sites or regions within a set timeframe regardless of whether devices or infrastructure have failed. This promotes a steady pace of modernization while controlling costs and minimizing operational disruptions. By adopting this method, organizations can schedule upgrades during low-traffic periods for specific buildings, and prioritize the higher risk sites or regions first. This approach allows for easier allocation of resources, and can minimize concerns with having disparate systems because departments and sites are getting converted in unison, thus the local teams are able to collaborate with the new system.

Some downsides of this approach include the length of time required to reach full system compliance; operating disparate systems for a predetermined set of time; and the replacement of devices and infrastructure that may have been recently installed/not at end of life.

Failure-Based Replacement

A failure-based replacement strategy only replaces legacy hardware as it fails. This can be the most cost-effective solution in the short term, as existing hardware investments are being utilized until end of life and there is likely less new hardware investment early on. On the other hand, this strategy can extend the transition timeline and require ongoing integration between the two systems that may make daily use of the overall system more difficult.

This strategy is often chosen by organizations looking to extend the lifecycle of their existing investment while gradually incorporating modern infrastructure. However, the piecemeal nature of this method can result in operational inefficiencies and challenges, temporary compatibility issues and a lack of system cohesion.

Product-Based Replacement

This approach focuses on replacing one product line, such as cameras, entirely before addressing other systems like access control or sensors. By prioritizing specific components, organizations can modernize incrementally and focus on the most outdated systems first, while distributing costs and resources over time. However, similarly to the other phased approaches this strategy will have longer intervals of discontinuity between systems.

Combining All of the Above

The reality for many organizations is that their existing system architecture is complex and no single template will work. For this reason, a combination of the above strategies are commonly employed to create a deployment strategy that makes sense for the organization and their most pressing needs.

Integration Approaches For Phased Transitions

If a phased approach is chosen, additional consideration is needed for integrating legacy and new systems during the transition process.

Parallel Systems

In a parallel system, both legacy and modern architectures are in place and being operated concurrently. This approach provides continuity during the upgrade process and allows for a gradual shift in operations—but it can also lead to operational inefficiencies as staff must manage and monitor two systems at once, which may result in data silos and fragmented workflows.

Some organizations may choose to implement upgrades based on sites or regions, allowing for localized training and adjustments based on the needs of that area. Other organizations choose a "swivel screen" approach where both cloud-based and on-premise systems are operated alongside one another.

Unified VMS Integration

With this integration, legacy video management systems (VMS) are maintained across all sites until the transition to the cloud is complete. This approach simplifies integration by continuing to use familiar workflows and infrastructure while phasing in new hardware. Video streams can be sent from the cloud system to the VMS using the Real-Time Streaming Protocol (RTSP) or using camera streaming APIs. While this strategy simplifies the transition process because teams can use familiar workflows, it delays the adoption of full cloud-based capabilities, which may limit access to advanced features and analytics in the interim.

Event-Based Integration

An event-based integration centralizes data from both legacy and modern systems in a Security Information and Event Management (SIEM) system through the use of APIs or streaming protocols. This enables organizations to consolidate event monitoring and streamline workflows across disparate systems. By bringing data together in one centralized platform, security teams gain improved situational awareness, enabling faster and more informed decision-making.

While event-based integrations offer significant benefits, they are not without challenges. Event-driven integration requires robust API management and technical expertise to set up and maintain. This added complexity may increase the burden on IT resources during the transition phase. Additionally, potential delays in event triggers and video streaming can occur during network outages impacting real-time responses.

Bridged Solution

A bridged solution uses cloud connectors or adapters to integrate legacy devices into a cloud-based solution. These tools translate data between old and new systems, and are network connected allowing for the cloud connection. This enables immediate centralization without having to replace outdated hardware, which can then be gradually replaced over time. This can reduce upfront costs and extend the utility of existing investments, and cloud-computing can be used to offer improved analytics.

However, this solution is not without its own set of limitations. It can add complexity and additional hardware, increasing maintenance demands and requiring additional technical expertise to ensure streamlined operations. Additionally, while bridges facilitate compatibility, they may not fully unlock the advanced features of the cloud-based platform potentially limiting the systems capabilities until a full upgrade is completed. Lastly, by continuing to use legacy devices, manual firmware updates may still be required and if not performed regularly can serve as a network vulnerability.

How to Navigate a Transition and Where to Start

Whether implementing a complete rip and replace approach or orchestrating a carefully phased deployment, the key is to maintain clear sight of the end goal: a unified, resilient, and future-ready security infrastructure.

01 Evaluate Current Infrastructure

Identify gaps and pain points with the current system, and where opportunities exist to improve. This step is critical for understanding what aspects of the system need to be replaced now, in the mid term, or in the long term.

	Issue	Questions to Ask
☐	System Reliability	• Which components of the current system fail most frequently? • What is causing these failures? • Which systems are oldest or most outdated?
☐	Scalability and Infrastructure	• Can the current infrastructure support future growth? • Does the existing infrastructure need to be updated (e.g., still using co-axial cable infrastructure)? • How many new sites will be added in the near future? • Does the new system enable easy and seamless scaling?
☐	Compatibility	• Are there integration challenges with current systems? • Are there integration challenges with planned/future systems?

02
New System Assessment

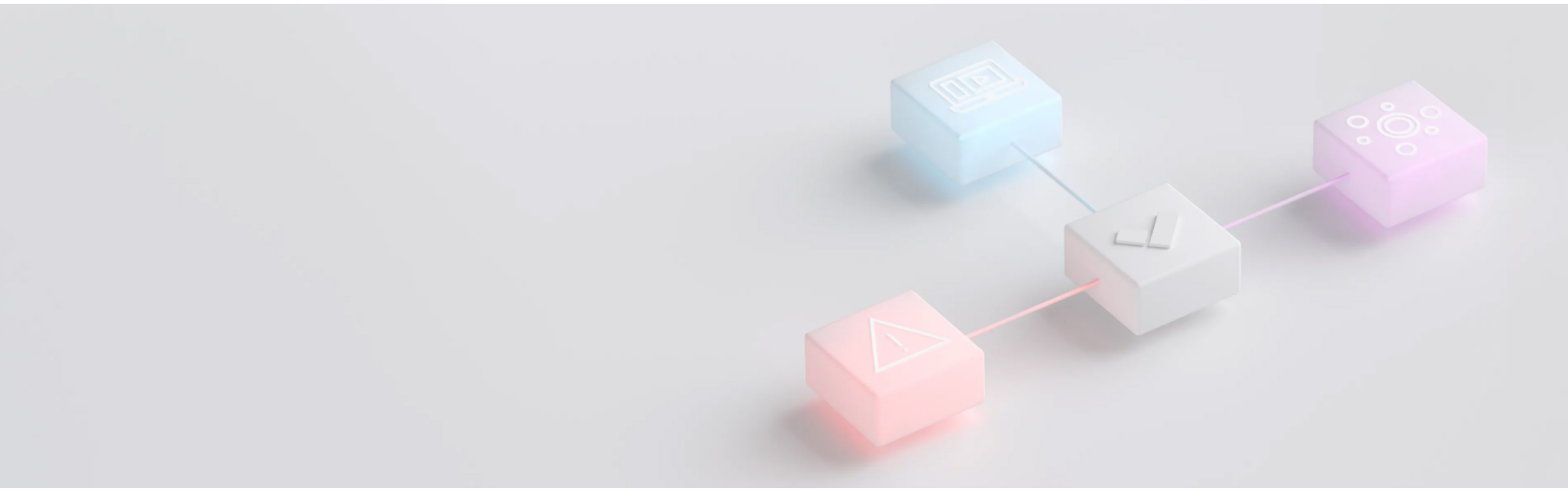
Define measurable goals for the new system and each stage of the transition, such as improved scalability or enhanced threat detection.

	Issue	Questions to Ask
☐	Functionality Improvements	• What specific threats should the upgraded system address more effectively? • Which analytical tools are most important to the organization? • Which features/tools are least effective in the current system? • Which systems currently offer over-the-air updates? • Which sites or systems would most benefit from cutting-edge features?
☐	Scalability Goals	• What is the desired capacity of the system after modernization? • What are the future plans for expansion after the change?
☐	Operational Efficiency	• How will this transition reduce time and resource allocation for both IT and security teams? • What process currently takes the most time for operational teams, and what would reduce that time spent?
☐	Cybersecurity Posture	• Are there any known cybersecurity issues or gaps in the current system? • Which of the current systems offer automated software and firmware updates? • What level of risk and responsibility does the IT team currently take ownership over? • Does the new system adhere to industry standard security best practices like Zero Trust, encryption in transit and at rest, and performing regular penetration tests?
☐	System Reliability	• Does the new system offer a hardware warranty? • Has the organization assessed the new system's service level agreement?

03
Plan For Integrations

Evaluate APIs and integration capabilities to ensure compatibility with existing systems and workflows. If a complex integration using APIs, scripting or other engineering resources is needed, plan for this in the timeline.

	Issue	Questions to Ask
☐	API Compatibility	• Do the new systems offer robust APIs for integration with existing workflows? • Can existing workflows be retained with a shift to newer, more advanced systems?
☐	Integration Assessment	• Which current systems (e.g., user management tools, single sign on platforms, etc.) does the new security system need to integrate with? • Do any of these systems require a native integration? • Is the organization capable of building custom integrations where native integrations might not exist?
☐	Resource Allocation	• What technical expertise is required to handle the integration process? • Does the organization have IT staff that can handle this technical process? • Will they have the bandwidth to integrate systems within the proposed timeline?
☐	Timeline Impacts	• How will integrations affect the overall deployment schedule? • Which integrations are most important, and which can be dealt with post-launch?



04
Engage Stakeholders

Collaborate with all key stakeholders, including IT, security, leadership and finance, to align priorities and gain consensus on the transition plan. Higher engagement from critical stakeholders can drastically increase budget allocation, deployment speed, and the overall effectiveness of the final solution.

	Issue	Questions to Ask
☐	Cross-Departmental Alignment	• Have all stakeholder concerns been addressed in the transition plan? • Do you have buy-in from executives and decision makers?
☐	Budget Considerations	• How will the cost of deployment impact current financial goals and priorities? • Have you performed a total cost of ownership analysis of the new system, and compared it to the TCO of the old system?
☐	Timeline Coordination	• Are there any organizational timelines or constraints that impact the deployment process? • Are local sites prepared to begin the upgrade process?

05
Deployment Strategy

Based on the infographic above, use the deployment strategy that works best for the organization at large. Some organizations prefer a full rip and replace, guaranteeing a unified and cohesive system. More commonly, a rolling installation approach will be taken. If this is the case, make sure to plan the stages of the deployment carefully.

	Issue	Questions to Ask
☐	Deployment Approach	• Which deployment approach was selected based on the strategies highlighted in this document? • Does this strategy align with organizational needs?
☐	Site Prioritization	• Which locations or departments should be prioritized for upgrades based on risk, operational demands, or current gaps in functionality?
☐	Downtime Mitigation	• What can be done to minimize disruption during deployment phases? • Is it possible to keep older systems online while the new system is installed?

06
Consider Operational Impact

Analyze how each deployment and integration will affect daily operations for key stakeholders, including potential downtime or disruptions. Consider if these periods of downtime will introduce risk or violate compliance requirements for local teams and adjust accordingly.

	Issue	Questions to Ask
☐	Downtime Risk	• Which areas are the highest risk? (entryways, cash drawers, parking lots, etc) • How can risks associated with system downtime be mitigated during deployment?
☐	Compliance	• Are there compliance requirements that could be impacted by downtime or integrations?
☐	Stakeholder Impact	• How will the transition process affect the team's daily operations? • What can be done to smooth the transition process for end users?

07
Budget Allocation

Ensure deployment strategy is in alignment with budgetary requirements and financial resources, balancing immediate costs with long-term benefits.

	Issue	Questions to Ask
☐	Cost breakdown	• What are the short-term and long-term costs associated with the transition? • Has a total cost of ownership (TCO) assessment been performed?
☐	Financial Alignment	• How does the deployment fit within the organization's financial goals and restrictions?
☐	ROI Projections	• What, if any, return on investment (ROI) is expected? • What is the timeline for this ROI?

08
Employee Training

There will be a period of time where security and IT personnel need to learn the new system. Equip teams with the knowledge and skills needed to manage new systems effectively ahead of time to facilitate minimal downtime as the new system is implemented.

	Issue	Questions to Ask
☐	Training Resources	• What kinds of resources (manuals, training sessions, knowledgebase articles, etc) are required for effective onboarding? • Does the new system provide these resources, or other training resources?
☐	Training Timeline	• How much time will the initial training process take?
☐	Training Effectiveness and Retention	• How frequently will training be offered or required? • What tools are needed to ensure proficiency over time?

The Future of Enterprise Security

The transition to modern, cloud-based physical security systems represents more than just a technological upgrade—it's a strategic imperative for enterprises looking to thrive in an increasingly complex world. As organizations navigate this transformation, success lies not in choosing between an immediate overhaul or a gradual transition, but in crafting a thoughtful modernization strategy that aligns with their unique operational needs, security requirements, and business objectives. Whether implementing a complete rip and replace approach or orchestrating a carefully phased deployment, the key is to maintain clear sight of the end goal: a unified, resilient, and future-ready security infrastructure.

The journey to modernization requires more than just technology. It demands a commitment to rethinking outdated processes, aligning cross-functional teams, and building a security infrastructure designed for the future.

The rewards of this transformation extend far beyond improved security capabilities. Organizations that successfully modernize their physical security infrastructure can realize unexpected benefits: IT teams find themselves spending less time managing hardware and more time driving innovation; security teams gain powerful new tools for investigation and incident prevention; and operations teams unlock new insights that drive better business decisions. The integration of AI capabilities, once a pipe dream for traditional systems, becomes a practical reality that continuously enhances security effectiveness while reducing manual workload.

However, the journey to modernization requires more than just technology. It demands a commitment to rethinking outdated processes, aligning cross-functional teams, and building a security infrastructure designed for the future. That may seem daunting, but organizations don't have to navigate it alone. With clear deployment strategies, proven integration approaches, and a growing ecosystem of solutions providers, enterprises have more resources than ever to guide their transformation journey. The key is to start with a clear assessment of current needs and future goals, engage stakeholders early in the process, and develop a comprehensive plan that addresses everything from technical requirements to employee training.

As we look to the future, one thing becomes clear: the organizations that thrive will be those that embrace this security infrastructure modernization not as a one-time upgrade, but as the beginning of a new approach to physical security; one that is more adaptable, more intelligent, and more closely aligned with their overall business objectives. The tools and technologies are ready, the benefits are proven, and the time for transformation is now.

The dividing line between security leaders and security liabilities will be drawn not by the size of their security budgets, but by their willingness to embrace this transformative moment and build security infrastructure that's ready for tomorrow's challenges, not yesterday's threats.

Verkada

Verkada is a pioneer in cloud-based physical security solutions by enabling over 30,000 organizations in 85+ countries to protect their people and property in a way that respects individuals' privacy. Designed with simplicity in mind, Verkada offers six product lines — video security cameras, door-based access control, environmental sensors, alarms, workplace, and intercoms — that provide exceptional visibility through a single cloud-based software platform.