REDLEIF Verkada

The Public Sector Guide to Software-Defined Security

How **State Agencies** Are Building Unified Response Capabilities

Executive Resource Guide | 2026

The Challenge:

When Every Second Counts, Your Security System Shouldn't Make You Wait

State agencies face a fundamental challenge: how do you secure dozens of buildings, monitor environmental conditions, coordinate emergency responses across campuses, and manage visitor access, all while working with limited staff and budget?

Legacy security means juggling separate systems. Cameras on one platform. Door locks on another. Air quality sensors somewhere else. Visitor badges in a different system entirely. Need to lock down a building? You're calling facilities, logging into multiple dashboards, checking alarms, and hoping everything syncs up in time.

Unified physical security platforms flip that model. Instead of coordinating separate systems during a crisis, you press one button. Cameras, access control, alarms, and environmental sensors work together automatically.

10 seconds or 10 minutes

How fast can you respond to an emergency across your entire facility?

The answer depends on whether your security systems work together or require manual coordination across multiple platforms.

The difference matters. When an active threat is reported at your state capitol during a legislative session, you can't afford to spend 10 minutes making phone calls and toggling between systems. When a fire alarm triggers in a health services building with vulnerable populations, doors need to unlock immediately and cameras need to capture the evacuation without someone manually coordinating three different vendors.

This isn't theoretical. The technology exists today. The question is whether your agency is still operating with the old model or moving toward unified response.

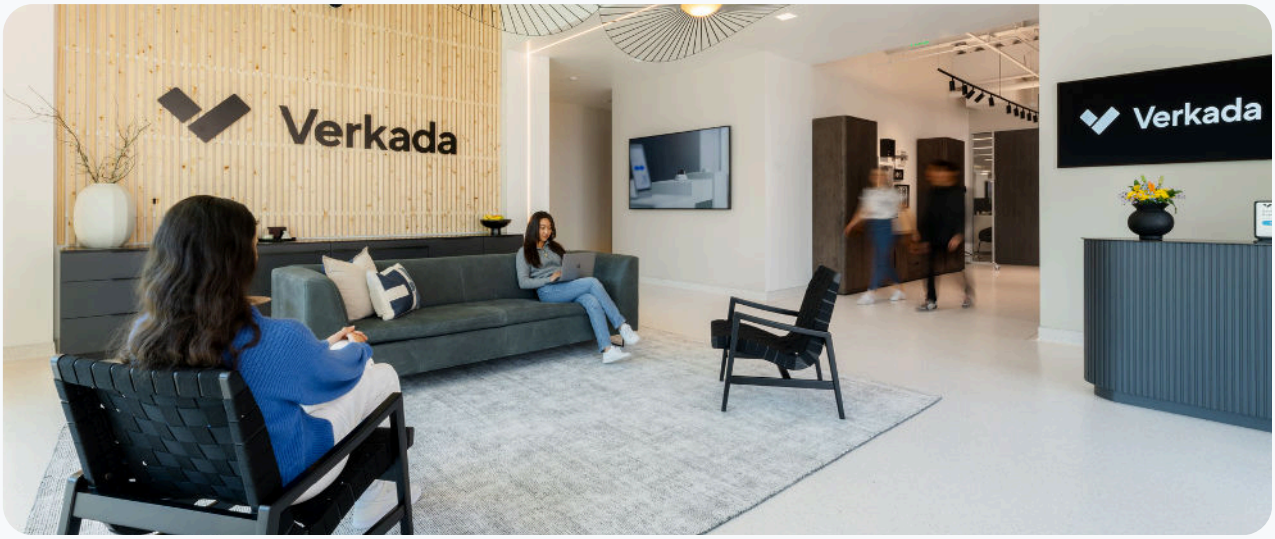
How We Got Here. And Why It Matters Now

The Legacy Model

Physical security used to mean buying individual systems. Cameras from one vendor. Door locks from another. Alarm panels from a third. Environmental sensors from a fourth. Each worked independently. Each had its own login, its own dashboard, its own way of doing things. Coordination happened through phone calls and spreadsheets.

This made sense 20 years ago. Security cameras were expensive, specialized equipment. Access control meant physical keys and maybe some card readers at main entrances. Environmental monitoring was something the facilities team handled separately. Integration wasn't really possible, so nobody expected it.

But that model creates real problems when something goes wrong. An emergency happens. Your security team needs to lock doors, pull up cameras, check who's in the building, trigger alarms, and share information with first responders. With separate systems, each step requires a different login, a different interface, a different process. What should take seconds takes minutes.



What Changed

Cloud-based platforms unified everything. Now cameras, access control, environmental sensors, visitor management, alarms, and intercoms operate as one system. Badge swipe at a door? Video automatically pulls up. Fire alarm triggers? Doors unlock and cameras capture the evacuation. Air quality drops? Alerts go out and the system logs who was in the building.

The technology shift happened quietly. While everyone was focused on upgrading individual components (better cameras, smarter door readers), a more fundamental change was taking place. The same cloud infrastructure that powers your email and file storage made it possible to run all your security systems from one platform.

This isn't about adding features to existing systems. It's a different architecture entirely. Instead of cameras that record to local servers, you have cameras that stream to the cloud. Instead of access control panels that require on-site programming, you have cloud-managed systems you can configure from anywhere. Instead of environmental sensors that trigger local alarms, you have sensors that integrate with your entire security response.

Why It Matters for State Agencies

You manage more facilities with fewer people. Your security team can't be everywhere. A unified platform means one person can oversee dozens of facilities because everything operates from one dashboard.

Emergency response can't wait for manual coordination. When something happens, your team needs to act immediately. Not call IT. Not dig through manuals. Not log into five different systems.

Every action needs a complete record. Audit trails aren't optional in government. Modern platforms log everything: who accessed what, when, and why. Video is automatically linked to badge activity and environmental sensor data. Incident reports generate themselves.

You can't rip and replace everything at once. Budget constraints are real. Modern platforms work with your existing infrastructure. Start with the platform. Upgrade cameras, sensors, and access hardware strategically over time. The unified software stays constant.

You need to justify every dollar. Show decision-makers exactly what you're gaining: response times drop from minutes to seconds, staff time saved monitoring multiple systems, facilities secured without adding headcount, environmental compliance automated.

The shift from isolated systems to unified platforms isn't just a technology upgrade. It changes what your security team can actually do when it matters most.

7 Use Cases Across State Operations

The following scenarios are drawn from real implementations. Similar principles apply across many state agencies with comparable operational needs.

Scenario 1:

Emergency Response at State Capitol Complex

The Situation:

An active threat is reported at the state capitol during a legislative session. Legislators, staff, and visitors are throughout the complex. Every second counts.

What You Can Do With a Unified Platform:

Security pulls out their phone and taps "Emergency Lockdown." Every door locks across the entire complex. Cameras automatically focus on threat areas. Live video streams to law enforcement via text message. Intercoms broadcast instructions to remain in place. Access logs show exactly who's in the building. A complete audit trail generates automatically.

First responders arrive with live video already on their phones. They can see the situation before entering. Security can unlock specific doors remotely to let law enforcement in while keeping other areas secured. No keys. No calling building to building. No hoping that everyone got the message.

What This Solves:

Response drops from 10+ minutes of coordination to under 10 seconds. Instead of security staff making phone calls to lock down different buildings, calling IT to pull camera footage, and trying to account for who's where, one person initiates a coordinated response from anywhere.

The platform handles the coordination automatically. Doors lock. Cameras record. Access logs freeze. Intercoms broadcast. Law enforcement gets live feeds. After the incident, the complete record (video, access logs, timestamps, actions taken) is already compiled for review and reporting.

Response Time:

Based on emergency response use cases from Las Vegas, Los Angeles

Scenario 2:

State Parks & Wildlife Management Across Remote Locations

The Situation:

Your state manages dozens of parks across thousands of acres. Ranger stations, trailheads, campgrounds, wildlife areas. Many locations have limited or no internet infrastructure. Vandalism, illegal dumping, and after-hours activity are ongoing problems. Rangers can't be everywhere at once.

What You Can Do With a Unified Platform:

Solar-powered cameras with LTE connectivity provide visibility across remote locations. Rangers monitor from mobile devices while on patrol. Motion-triggered alerts for after-hours activity mean rangers respond to actual incidents, not routine patrols of empty facilities. Wildlife tracking and visitor safety monitoring happen automatically. No trenching. No fiber runs. No local servers to maintain at each site.

When something happens (vandalism, illegal dumping, visitor injury), rangers have video evidence immediately. Cameras captured the incident. Timestamps are logged. Evidence is preserved in the cloud, not on a local recorder someone could steal or damage.

What This Solves:

Protection for remote assets without massive infrastructure investment. Rangers respond to incidents faster because they know what's happening before they arrive. Deterrence works because vandals realize they're being recorded even at remote sites. Evidence for wildlife management and visitor incidents is automatically preserved.

You're not running power and fiber to every trailhead. You're not maintaining local recording equipment at dozens of remote sites. You're not sending rangers to check if anything happened overnight. The platform tells them when and where attention is needed.

Remote site coverage with significant infrastructure savings | Similar principles apply to natural resources, conservation, and recreation agencies

Scenario 3:

Department of Transportation Work Zone Safety & Incident Response

The Situation:

Your state DOT manages highway construction zones, bridge inspection sites, and traffic incidents across the state. Work zone intrusions put crews at risk. Accidents need immediate response. Projects move from site to site, and permanent camera installations don't make sense.

What You Can Do With a Unified Platform:

Deploy mobile cameras at work zones and accident sites. Monitor traffic flow in real-time from the traffic management center. Detect accidents and hazards automatically. Share live feeds with highway patrol and emergency services. When the project wraps up, cameras relocate to the next site.

Work zone safety improves because supervisors can monitor from the office. Set up virtual line crossing to get alerts when vehicles enter restricted areas. If an incident occurs, search footage by vehicle description or set up motion detection zones for specific areas. Incident response is faster because emergency services can see the situation before units arrive. Investigations have video evidence from multiple angles without anyone having to scrub through hours of recordings.

What This Solves:

Faster incident response when minutes matter. Work zone safety monitoring without dedicating staff to watch cameras all day. Evidence for accident investigations and insurance claims that would otherwise be he-said-she-said. A portable system that moves with projects instead of permanent infrastructure that sits idle after construction ends.

Your traffic operations center can monitor construction zones across the state from one dashboard. Highway patrol gets live video links when incidents occur. Contractors can review footage to improve safety procedures. Insurance claims get resolved faster with clear evidence.

Real-time traffic monitoring | Similar use cases in transportation, public works, and infrastructure agencies

Scenario 4:

Fuel Theft Prevention at State Vehicle Fleet Yards

The Situation:

Your state operates maintenance yards for DOT trucks, law enforcement vehicles, and agency fleets. Fuel theft is an ongoing problem. Thousands of dollars disappear every year. Investigation is difficult because thefts happen overnight when nobody's there.

What You Can Do With a Unified Platform:

Cameras with license plate recognition monitor vehicle entries 24/7. Motion-triggered alerts when activity is detected after hours. Video evidence links vehicles to fuel pump activity. Integration with fleet management systems shows which vehicles should be there and which shouldn't. When someone pulls in after hours, security gets an alert with the license plate and live video. If it's an authorized maintenance vehicle, no problem. If it's not, law enforcement can respond while the theft is in progress, not three days later when someone notices the fuel is gone.

Instead of watching hours of footage to investigate an incident, search by license plate number or vehicle description ("white pickup truck"). Set up line crossing alerts so you know immediately when a vehicle approaches the fuel pumps after hours. AI-powered search turns a multi-hour investigation into a quick query.

What This Solves:

Fuel theft drops dramatically when thieves realize they're being recorded and license plates are captured. Investigations that used to take days (review logs, pull footage, try to identify vehicles) now take minutes. Type in a license plate or search "red sedan" and the platform finds every instance across all cameras instantly.

Intelligent search means your team isn't watching hours of video. They're finding exactly what they need in seconds. Insurance claims and internal investigations are backed by video evidence with timestamps and license plate data.

The real deterrent is that would-be thieves know the risk. Word gets around. When the first few people get caught with clear video evidence and plate numbers, the problem largely stops.

Stopped recurring fuel theft | Based on Tumwater School District fuel theft case

Scenario 5:

Multi-County Health & Human Services Offices

The Situation:

Your state health department operates multiple public-facing offices. Medicaid enrollment. WIC clinics. Child support services. Unemployment offices. High foot traffic. Interactions can become tense. Limited security staff. Budget doesn't allow for security guards at every location.

What You Can Do With a Unified Platform:

Unified platform covers all locations. Visitor management logs everyone who enters. Cameras in lobbies and service areas. Panic buttons at reception desks that instantly alert security and local law enforcement. Environmental sensors monitor air quality (important for health clinics). Central security team oversees all sites remotely.

When a situation escalates, the receptionist presses the panic button. Security instantly sees live video of what's happening. Law enforcement gets a text message with the address and live video link. The system logs exactly who was in the building at that time. If needed, security can lock doors remotely to prevent the situation from spreading to other areas.

What This Solves:

Staff safety in high-traffic public offices where tensions can run high. Incident documentation for workplace violence prevention and HR investigations. Visitor tracking for compliance requirements. One person can monitor security across dozens of offices instead of needing dedicated security at each location.

After an incident, you have the complete record. Who was there. What happened. What time. Video from multiple angles. Who responded. How long it took. This matters for staff safety, liability protection, and process improvement.

Multi-site oversight from one platform | Similar applications across social services, workforce development, and public assistance agencies

Scenario 6:

Disaster Response Coordination During Hurricane Or Wildfire Season

The Situation:

Your state emergency management agency needs to monitor critical infrastructure during natural disasters. Evacuation routes. Emergency shelters. State facilities. Coastal areas. Traditional on-premise systems go offline when power fails or networks go down.

What You Can Do With a Unified Platform:

Cloud platform remains accessible even if local infrastructure fails. Remote monitoring of flood conditions, facility damage, and evacuation progress. Share live feeds with FEMA and emergency services without worrying about server capacity. Mobile command center access for incident commanders in the field.

As the hurricane approaches, you're monitoring shelters filling up, watching coastal flooding in real-time, tracking facility damage, confirming evacuation routes are clear. All from one dashboard. When cell towers go down in some areas, LTE cameras with backup connectivity keep streaming. When local power fails, cameras with battery backup keep recording.

What This Solves:

Situational awareness during disasters when traditional systems fail. Coordination across state, county, and federal responders who all need access to the same information. Damage assessment without sending teams into dangerous areas before it's safe. A cloud platform that works when local servers would be underwater or without power.

After the disaster, you have comprehensive documentation for FEMA reimbursement. Timestamped video of flood levels, damage progression, evacuation completion. This matters for disaster aid applications and improving future response.

Operational during infrastructure failure | Relevant for emergency management, homeland security, and disaster preparedness operations

Scenario 7:

License Plate Recognition for Public Safety & Parking Enforcement

The Situation:

Your state law enforcement needs to locate stolen vehicles, track amber alert suspects, and manage parking at state facilities. Traditional methods mean officers manually checking plates or hoping they happen to spot a wanted vehicle.

What You Can Do With a Unified Platform:

LPR cameras at state facility entrances, park-and-rides, and high-traffic areas automatically scan plates. Alerts when stolen vehicles or wanted persons are detected. Capability to manage "License Plates of Interest" watchlists and integrate with external databases. Parking enforcement without manual ticketing (cameras know which plates have permits).

When a stolen vehicle drives past an LPR camera, the system immediately alerts law enforcement with the location, timestamp, and direction of travel. Officers respond with current information instead of chasing vehicles that passed by hours ago. Amber alert vehicles get flagged automatically.

For parking, the system knows which vehicles have valid permits. After grace period expires, unpermitted vehicles get automatic citations with photo evidence. No need for staff to walk lots checking windshields.

What This Solves:

Stolen vehicle recovery using your existing camera infrastructure instead of hoping an officer happens to spot the right car. Amber alert response with automated scanning across multiple locations. Warrant service when wanted individuals arrive at state facilities. Automated parking enforcement that pays for itself through violation revenue.

The system runs 24/7 without fatigue. It scans every plate that passes, checks watchlists instantly, and only alerts humans when action is needed. One LPR camera can process thousands of plates per day with accuracy human enforcement could never match.

Automated plate scanning with database integration | Applicable across law enforcement, public safety, and facility management operations

Why State Agencies Are Moving to Platform-Based Security

Built for the Way Government Actually Works

You manage more buildings with fewer people.

Your security team can't be everywhere. Budget constraints mean you're not adding headcount. A unified platform means one person can oversee dozens of facilities: watching cameras, managing access, monitoring environmental conditions, tracking visitors. They can do this because everything operates from one dashboard, not five different systems with separate logins and interfaces.

Think about what that means practically. Instead of your security lead spending the first 30 minutes of a shift logging into separate camera systems, access control platforms, visitor management tools, and environmental monitoring dashboards, they open one interface and see everything. A door is propped open at Building 7? They see the alert, pull up the camera for that door (automatically), and can address it immediately.

Every action needs a complete record.

Audit trails aren't optional in government. Someone will ask questions. Legislators. Auditors. Internal affairs. The media. You need answers backed by facts.

Modern platforms log everything: who accessed what, when, and why. Video is automatically linked to badge activity and environmental sensor data. When someone badges into a secure area, the system doesn't just log the badge swipe. It captures video of the person at the door, records environmental conditions (was the air quality alarm active?), notes who else was in the building, and timestamps everything.

Incident reports with camera footage, access logs, and sensor readings generate themselves. You're not manually compiling data from three different systems, hoping the timestamps match up, trying to figure out which camera angle covers which door. The platform knows. It creates the report. You review and submit.

This matters when the inspector general shows up asking about after-hours access to the evidence room. You don't need three weeks to compile records. You pull up the report: who entered, when, video footage, whether any alarms triggered, complete audit trail. Done.

Emergency response can't wait for IT help.

When something happens, your security staff needs to act immediately. Not call IT. Not dig through manuals. Not log into five different systems while an active situation unfolds.

Mobile apps and intuitive interfaces mean your team can respond from anywhere. Security lead is at lunch when a panic button triggers at the health services building? They pull out their phone, see live video, unlock doors for law enforcement, and coordinate response without rushing back to the office.

This is the difference between platforms built for daily operations and legacy systems built for IT administrators. Modern platforms assume your security team are professionals who need tools that work under pressure, not system administrators who need three-day training courses to perform basic functions.

You can't rip and replace everything at once.

Budget constraints are real. Your cameras work. Your door readers function. Maybe they're not cutting-edge, but they're in place and operational. Telling your CFO you need to replace all of it isn't realistic.

Modern platforms work with your existing infrastructure. Start with the platform. Connect your existing cameras through integration technology. Upgrade access hardware strategically over time as budget allows or equipment fails. The unified software stays constant. Your team learns one interface, and it keeps getting better.

This is the sustainable path forward. Year one, you deploy new platform cameras at priority facilities and connect existing cameras where possible. You prove ROI. Year two, you add access control at facilities where unified response matters most. Year three, you expand environmental sensors and visitor management. Throughout, your team is using one platform that keeps improving.

The alternative (waiting until you have budget to replace everything at once) means you're still operating with the old model in 2030. That's not realistic, and it's not necessary.

You need to justify every dollar.

Decision-makers need specifics. "Better security" doesn't get budget approval. Numbers do.

Show them response times: minutes to seconds. Show them staff time saved: one person monitoring 50 facilities instead of needing security at each location. Show them facilities secured without adding headcount. Show them environmental compliance automated (you're not manually checking sensor logs and hoping you catch problems before inspectors do).

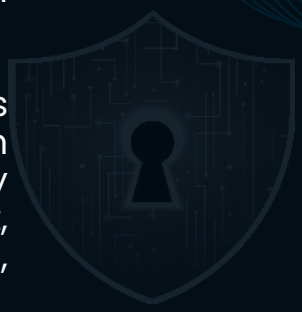
Modern platforms generate these metrics automatically. Average response time to alarms. Time saved on incident report compilation. Reduction in after-hours incidents after cameras were installed. Cost per facility for centralized monitoring versus the alternative (security guards, more staff, or accepting the risk).

Making the Platform Decision

The Questions That Actually Matter

The question used to be "Which access control system should we buy?" Now it's "Which platform will run our security operations?"

That reframing matters. This isn't just about cameras or door readers. It's about choosing the platform your team will use every day for emergency response, routine monitoring, visitor management, environmental compliance, incident investigation, and multi-site coordination.



Can it actually do what we need during an emergency?

The real test: Can your security team lock down an entire campus, pull up cameras, and share live video with first responders, all from a mobile phone in under 10 seconds?

If the answer is "yes, but someone would need to call IT first" or "yes, if they're at their desk," the platform fails the primary test. Emergencies don't wait. Your team needs to act immediately from wherever they are.

Related questions worth asking:

- Can you see what's happening across all your cameras and sensors during an incident without logging into multiple systems?
- Can you grant temporary access to law enforcement remotely without mailing keys or having someone drive to the facility?
- Will your staff actually be able to use this under pressure, or does it require IT support to coordinate cameras, access control, and alarms?

The answer should be obvious within five minutes of watching a demo. If the vendor is clicking through multiple screens, explaining complex workflows, and promising "it's easier once you learn it," that's your answer. Under pressure, complex systems fail.

Does it work with what we already have?

The real test: Can it connect to your existing cameras and access control hardware, or do you have to replace everything at once?

Budget reality means you need a platform that meets you where you are. You have cameras that work. You have door readers in place. Maybe they're not cutting-edge, but ripping them out and starting over isn't in this year's budget or next year's either.

Related questions:

- Can you add environmental sensors and visitor management without rebuilding infrastructure?
- Can you start with cameras in one building, add access control later, and scale over time, or do you have to commit to everything up front?
- Can you upgrade hardware gradually as budget allows, or is it all or nothing?

The right answer is that the platform provides a path forward. New equipment works natively with full capabilities. Existing equipment connects where possible through integration technology. You upgrade strategically over time. The platform stays constant.

Will it save time or create more work?

The real test: Does badge activity automatically pull up video, or do you have to hunt for footage across separate camera systems?

The point of integration is that the platform does the work. Someone badges into a secure area, and video from that door automatically appears. An alarm triggers, and cameras near that location pop up. A panic button is pressed, and law enforcement gets a text message with live video already loaded.

If your team is still hunting through camera lists, scrubbing timelines to match badge swipes, manually compiling incident reports from three different systems, the "unified platform" isn't unified. It's just multiple systems with a single login.

Related questions:

- Are incident reports with video, access logs, and environmental data generated automatically, or does someone have to compile from multiple systems manually?
- Can you manage cameras, access control, environmental sensors, and visitor management across 50 facilities from one dashboard, or does each system require separate logins?

The time savings are real and measurable. Calculate how much time your team currently spends logging into separate systems, hunting for footage, compiling incident reports, checking sensor logs manually. A truly unified platform eliminates most of that work.

What does it actually cost to operate?

The real test: What are you spending today on staff time, maintenance, delayed response, and operational inefficiency?

Most agencies focus on upfront costs and miss the operational expenses that add up over time. Calculate what you're actually spending:

Staff time: How many hours per week does your team spend logging into separate systems, hunting for footage, manually compiling incident reports, and coordinating between platforms? If your security lead spends 30 minutes per shift just getting systems ready, that's 2.5 hours per week per person. Multiply that across your team. That time has a dollar cost.

Maintenance and IT overhead: Separate servers for cameras, access control, and sensors mean ongoing maintenance contracts, update management, hardware refresh cycles, and IT staff time. Cloud platforms eliminate most of that overhead. No servers to maintain. No manual updates across different systems. No wondering if everything will work together after the next patch.

Delayed response: What's the cost when your security team takes 10 minutes to coordinate a response instead of 10 seconds? In some scenarios (active threats, medical emergencies, facility evacuations), delayed response has real consequences. How do you quantify the risk of not being able to lock down a building immediately?

Investigation time: When an incident happens, how long does it take to compile footage, access logs, and reports from multiple systems? If investigations that used to take hours now take minutes, that efficiency has measurable value. When insurance claims or legal reviews need documentation, how quickly can you provide complete records?

Hardware flexibility: Can you work with existing infrastructure and upgrade strategically, or do you need to replace everything at once? Integration capability means you can prove ROI on a small scale before committing to full deployment.

The platforms that look more expensive on a spec sheet comparison often cost less to operate over time because they eliminate the hidden costs: staff time, maintenance overhead, delayed response, investigation hours, and the operational friction of coordinating separate systems during critical incidents.

Does it meet government accountability requirements?

The real test: Complete audit trails: who accessed what, when, and why, with video automatically linked?

You will be asked to explain what happened. Maybe not today. Maybe not this year. But eventually someone will ask, and you'll need documentation.

Related questions:

- Incident reports: camera footage, access logs, environmental sensor data (air quality, temperature), all timestamped and linked in one report?
- Visitor tracking: badge printing, movement across facilities, auto-expiring credentials, all logged?
- Environmental compliance: air quality, temperature, humidity monitoring with automated alerts and records?

The platform should assume you need complete documentation and provide it automatically. You shouldn't have to build custom reports or manually compile data from multiple systems every time an auditor shows up.

Can it scale across our operations?

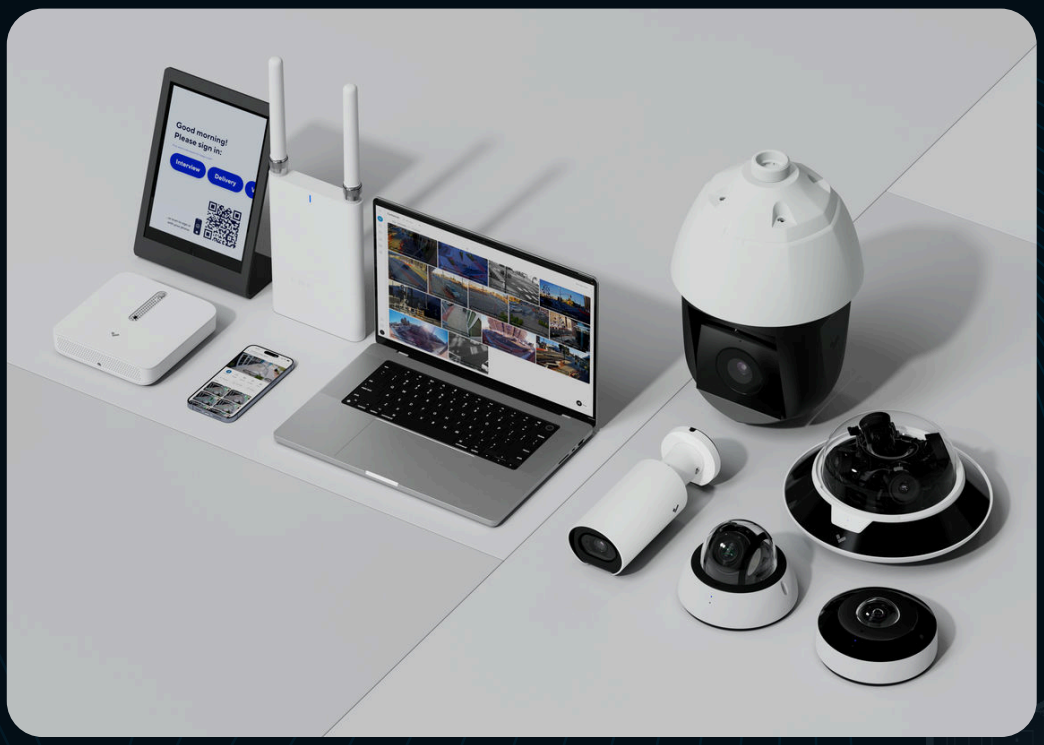
The real test: Start with cameras at one facility, add access control later, expand environmental monitoring over time, without rebuilding infrastructure?

Your security needs will change. Buildings get added. New compliance requirements emerge. Budget becomes available for expansions. The platform should scale gracefully without requiring architectural overhauls.

Related questions:

- Manage regional offices, state parks, and critical facilities from the same platform (all cameras, all doors, all sensors)?
- Add new sites by connecting devices, not deploying separate servers for cameras, access, and sensors?

Cloud platforms scale naturally. Adding a new facility means connecting devices to the platform, not installing local servers, running new network infrastructure, or rebuilding system architecture. Your team manages 10 facilities or 100 from the same dashboard.



How Verkada Solves This for State Agencies

Platform First, Hardware When It Makes Sense

Verkada built a unified cloud platform for physical security specifically designed for distributed operations like state government. Cameras, access control, environmental sensors, visitor management, alarms, and intercoms, all operating from one platform your team can manage from anywhere.

Start with what matters most. Add capabilities over time.

You don't have to replace everything at once. Start with cameras where visibility matters most. Add access control when budget allows. Integrate environmental sensors later. Connect existing cameras through Command Connector (Verkada's technology for bringing third-party cameras into the unified platform). Everything operates from one dashboard, one mobile app, one interface your team learns once.

What you get right away:

- Cloud-based platform for cameras, access control, environmental sensors, visitor management, alarms, and intercoms (no servers to maintain)
- Unified dashboard for all facilities and all security systems
- Mobile access for security staff (full functionality from phones, not watered-down views)
- Automatic updates and new features across the entire platform
- Integration with existing infrastructure where it makes sense

What this means operationally:

A typical phased implementation might look like this:

Phase 1

Deploy Verkada cameras at priority facilities. Connect existing cameras through Command Connector where possible. Prove value. Get your team comfortable with the platform. Start generating metrics on response times and operational efficiency.

Phase 2

Add access control at facilities where unified response matters most (state capitol, public safety buildings, facilities with high-value assets or sensitive populations). Now badge activity automatically pulls up video. Emergency lockdowns coordinate doors and cameras simultaneously.

Phase 3

Add environmental sensors and visitor management. Complete coverage across security, access, environmental compliance, and visitor tracking. All on one platform.

Phase 4

Expand across all facilities. Upgrade hardware strategically as budget allows or equipment reaches end of life. The platform stays constant. Your team keeps using the same interface. Capabilities keep improving through automatic updates.

The platform stays constant. Your capabilities keep improving.

Because Verkada is cloud-native, new features roll out automatically across cameras, access control, sensors, and everything else. Your security team in 2028 will have capabilities that don't exist yet, without ripping and replacing infrastructure.

This has already happened multiple times. License plate recognition improved through software updates to existing cameras. Person of interest alerts got smarter. Search capabilities expanded. Existing customers got these improvements automatically because the platform architecture supports continuous enhancement.

Compare this to legacy systems where "upgrades" mean replacing hardware, reinstalling software, hoping everything still works together, and retraining your team on new interfaces. With cloud-native platforms, updates happen automatically and your team shows up Monday morning with new capabilities.

What Makes Verkada Different for Government

Verkada fits exceptionally well in the public sector: multiple distributed facilities, limited staff, tight budgets, accountability requirements, and operational needs where minutes versus seconds actually matters.

Designed for distributed operations: One person can manage security across 50 facilities from one dashboard. Mobile apps provide full functionality (not watered-down read-only views). New facilities get added by connecting devices, not deploying servers and network infrastructure.

Accountability built in: Every action is logged. Every badge swipe has linked video. Every incident generates a report with footage, access logs, sensor data, timestamps. Audit trails are automatic, not something you manually compile when questions get asked.

Integration with existing infrastructure: Command Connector brings third-party cameras into the unified platform. They won't have every feature that native Verkada cameras provide, but they'll appear in the same dashboard, with the same search capabilities, linked to the same access control and sensor data. This gives you a path forward that doesn't require forklift replacement of working equipment.

Scalable without complexity: Adding cameras doesn't mean adding servers. Adding facilities doesn't mean adding IT staff. Cloud infrastructure scales transparently. Your team manages more with the same headcount.

The platform works the way government operations actually work: distributed facilities, constrained resources, accountability requirements, and situations where response time isn't a nice-to-have, it's the difference between containing an incident and escalating crisis.

5 Takeaways for Decision-Makers

The Platform Matters More Than the Hardware

1. The platform decision is more strategic than the hardware decision.

This isn't a camera project or an access control upgrade. It's the unified platform your team will use every day for cameras, access control, environmental monitoring, visitor management, emergency response, and multi-site coordination.

The platform decision matters more than individual hardware specs. Cameras and door readers can be upgraded over time. The platform architecture (cloud versus on-premise, unified versus separate systems, scalable versus fixed) defines what your team can actually do, both now and as your needs evolve.

Choose the platform that matches where you're headed, not just where you are today.

2. Response time matters, especially when it's measured in seconds versus minutes.

Unified platforms let you lock down entire campuses, share live video, and coordinate response in under 10 seconds from a mobile phone. Legacy systems require logging into separate platforms for cameras, access, and alarms, taking 10 or more minutes of coordination. In emergency scenarios (active threats at state capitols, urgent facility lockdowns, coordinated response to critical incidents), that difference matters.

This isn't theoretical. Multiple state agencies, local governments, and educational institutions have proven the 10-second unified response model works in real emergencies. The technology exists and functions as described.

3. Start with what matters most. Add capabilities over time. Everything on one platform.

You don't need to replace everything at once. Start with cameras where visibility is most critical. Add access control when budget allows. Integrate environmental sensors and visitor management as needs and resources align. The platform stays constant as you add capabilities.

This is the sustainable path forward. Waiting until you have budget to replace everything means you're still operating with the old model years from now. Strategic phased deployment means you're gaining capabilities, proving ROI, and building toward complete coverage on a timeline that matches budget reality.

4. Cloud-based platforms eliminate server maintenance and scale across everything.

No local servers for cameras, access, sensors, or visitor management. No manual updates. No wondering if systems will still work together after the next patch. Manage 1 facility or 100 from the same dashboard. Regional offices don't need IT staff on-site to manage security infrastructure.

Cloud infrastructure means your platform keeps improving. Software updates roll out automatically. New features become available without hardware replacement. Security patches apply across your entire deployment without IT teams visiting each facility.

5. Verkada built this specifically for distributed government operations.

State agencies managing dozens of facilities with constrained budgets, limited staff, and accountability requirements: that's the core use case Verkada designed for. Cameras, access control, environmental sensors, visitor management, alarms, intercoms, all on one cloud platform built for the way government actually works.

This isn't security technology adapted for government use. It's technology designed from the ground up for distributed operations where unified response matters, where staff are managing multiple facilities remotely, where audit trails and documentation are mandatory, and where platforms need to scale without proportionally scaling complexity or cost.

Want to learn more about what Verkada is doing for state agencies?

Visit **Verkada's page on The Trading Post** for more public sector content on modern physical security solutions.

Visit **Verkada's website** for case studies, implementation guides, and resources specific to state and local government operations.

REDLEIF Verkada 2026