DESIGNING CYBERSECURE SCHOOL VIDEO SURVEILLANCE SYSTEMS

A SECURITY-FIRST APPROACH TO PROTECTING MODERN EDUCATIONAL ENVIRONMENTS

WHITE PAPER

NOVEMBER 2026

i3 INTERNATIONAL™

Table of Contents

Why Are School Video Surveillance Systems Now Cybersecurity Assets?	2
Why Are School Security and IT Teams Being Forced to Collaborate More Closely?	3
What Does Cybersecure Surveillance Architecture Look Like?	4
How Can Network Segmentation Reduce Surveillance Cyber Risk?	5
Why Should Schools Adopt Zero Trust Security Principles?	6
What Security Features Should Schools Demand from Surveillance Vendors?	7
How Should Access to Surveillance Systems Be Controlled?	8
How Can Schools Protect Surveillance Data Throughout Its Lifecycle?	9
How Can Schools Maintain Control of Encryption Keys in Cloud-Based Surveillance Environments?	10
How Can Schools Prepare for a Security Incident Before One Happens?	16
How Can Modern Security Platforms Simplify Cybersecurity Management?	17
How Can Artificial Intelligence Improve Security Without Increasing Risk?	18
How Can Schools Improve Situational Awareness Beyond Traditional Cameras?	19
Why Is Ongoing Cybersecurity Management Essential?	20
What Does the Future of Secure School Surveillance Look Like?	21

School security has become increasingly complex: creating safe learning environments while protecting the technology systems that support them.

Today's video surveillance systems do far more than record events. They integrate with access control platforms, support remote administration, leverage artificial intelligence, connect to cloud services, and operate across school networks that support thousands of users and devices. While these capabilities provide significant operational and safety benefits, they also introduce new cybersecurity risks that cannot be ignored.

As physical security technologies become more connected, the line between physical security and cybersecurity continues to blur. A surveillance system can only be considered effective if it remains secure, available, and resilient when it is needed most.

> *For educational institutions, cybersecurity is no longer solely an IT concern. It has become an essential component of school safety strategy.*

This whitepaper explores how schools can design, deploy, and maintain cybersecure video surveillance environments that strengthen security posture, reduce operational risk, and support safer learning environments.

CONTACT US
support@i3international.com | 1.877.877.7241
Monday-Friday, 8:30AM - 8:00PM (EST)

CANADA
i3 International Inc. 251 Bartley Drive,
Unit 3 Toronto, ON M4A 2N7

USA
i3 America (Nevada) Inc.
4001 Cobb International Blvd NW, Kennesaw, GA 30152

Why Are School Video Surveillance Systems Now Cybersecurity Assets?

The transition from analog surveillance to IP-based video systems has fundamentally changed how schools must think about security.

Historically, cameras operated largely as isolated devices. Today, surveillance platforms are integrated ecosystems comprised of cameras, recording servers, management software, cloud services, analytics engines, mobile applications, and connected sensors. These systems often interact directly with school networks and other critical technologies.

This evolution has created tremendous opportunities for improving campus safety, but it has also expanded the attack surface available to cybercriminals.

A compromised surveillance system can result in:

- **Unauthorized access to live and recorded video.**
- **Disruption of security operations.**
- **Exposure of sensitive student, staff, or facility information.**
- **Loss of visibility during emergencies.**
- **Potential access pathways into other school systems.**

As a result, video surveillance must be viewed not simply as a physical security tool, but as a cybersecurity asset that requires the same level of protection as any critical technology system.

CONTACT US
support@i3international.com | 1.877.877.7241
Monday-Friday, 8:30AM - 8:00PM (EST)

CANADA
i3 International Inc. 251 Bartley Drive,
Unit 3 Toronto, ON M4A 2N7

USA
i3 America (Nevada) Inc.
4001 Cobb International Blvd NW, Kennesaw, GA 30152

Why Are School Security and IT Teams Being Forced to Collaborate More Closely?

For decades, physical security and information technology operated as separate disciplines.

Security teams focused on protecting people and facilities, while IT departments managed networks, endpoints, and digital infrastructure. Modern surveillance systems have effectively merged those responsibilities.

Today's cameras are network-connected devices. Video management platforms rely on servers, storage systems, cloud services, and authentication frameworks. Security decisions increasingly have cybersecurity implications, while cybersecurity decisions can directly affect physical security operations.

For example, a camera deployed without proper network controls can introduce unnecessary risk. On the other hand, restrictive IT policies that do not account for operational requirements can hinder investigations or emergency response.

> *The most successful educational institutions recognize that campus safety is now a shared responsibility between security and IT stakeholders. Planning, procurement, deployment, and lifecycle management should occur collaboratively to ensure security objectives align with both operational and cybersecurity requirements.*

CONTACT US
support@i3international.com | 1.877.877.7241
Monday-Friday, 8:30AM - 8:00PM (EST)

CANADA
i3 International Inc. 251 Bartley Drive,
Unit 3 Toronto, ON M4A 2N7

USA
i3 America (Nevada) Inc.
4001 Cobb International Blvd NW, Kennesaw, GA 30152

What Does Cybersecure Surveillance Architecture Look Like?

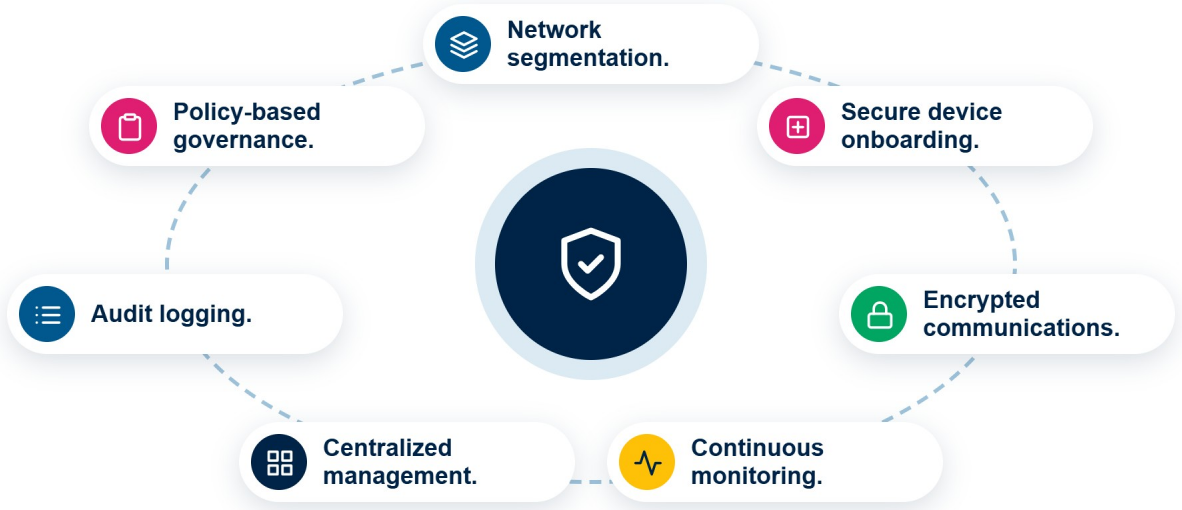
Strong cybersecurity begins long before cameras are installed.

Many schools focus their surveillance planning efforts on coverage areas, image quality, and storage requirements. While those factors matter, architecture ultimately determines whether a surveillance system can withstand modern cyber threats.

Cybersecure architecture is designed to limit exposure, contain risk, and maintain operational continuity. The objective is simple: if one component becomes compromised, the rest of the environment should remain protected.

Modern surveillance architecture can be strengthened through centralized video management platforms that provide secure device administration, system-wide monitoring, encrypted communications, and detailed audit logs. These platforms allow security and IT teams to manage multiple facilities from a centralized interface while maintaining visibility into device health and potential vulnerabilities.

Cybersecure architecture should include:



Building cybersecurity into system design from the beginning is significantly more effective than attempting to retrofit protections later.

CONTACT US
support@i3international.com | 1.877.877.7241
Monday-Friday, 8:30AM - 8:00PM (EST)

CANADA
i3 International Inc. 251 Bartley Drive,
Unit 3 Toronto, ON M4A 2N7

USA
i3 America (Nevada) Inc.
4001 Cobb International Blvd NW, Kennesaw, GA 30152

How Can Network Segmentation Reduce Surveillance Cyber Risk?

Network segmentation remains one of the most effective cybersecurity controls available to school districts.

Surveillance infrastructure should operate on dedicated security networks that are logically separated from administrative systems, classroom technologies, and student devices.

If a surveillance device is compromised, segmentation helps prevent attackers from moving throughout the broader network.

The benefits include:

- Reduced attack surface.
- Improved incident containment.
- Stronger network visibility.
- Simplified monitoring.
- Enhanced system resilience.

Rather than viewing surveillance infrastructure as a collection of cameras, schools should view it as a critical technology environment that requires dedicated protection.

CONTACT US
support@i3international.com | 1.877.877.7241
Monday-Friday, 8:30AM - 8:00PM (EST)

CANADA
i3 International Inc. 251 Bartley Drive,
Unit 3 Toronto, ON M4A 2N7

USA
i3 America (Nevada) Inc.
4001 Cobb International Blvd NW, Kennesaw, GA 30152

Why Should Schools Adopt Zero Trust Security Principles?

Traditional security models assumed that users and devices inside the network could generally be trusted Modern cybersecurity frameworks reject that assumption. Zero Trust operates on the principle of "never trust, always verify." Every user, device, application, and connection request must be continuously validated before granting access.

Within surveillance environments, Zero Trust helps ensure that:

- Only authorized personnel access security systems.
- Devices are continuously authenticated.
- Permissions remain tightly controlled.
- Suspicious behavior is identified more quickly.
- Security controls remain effective even when perimeter defenses are bypassed.

For schools operating increasingly interconnected environments, Zero Trust provides a strong foundation for protecting critical security infrastructure.

CONTACT US
support@i3international.com | 1.877.877.7241
Monday-Friday, 8:30AM - 8:00PM (EST)

CANADA
i3 International Inc. 251 Bartley Drive,
Unit 3 Toronto, ON M4A 2N7

USA
i3 America (Nevada) Inc.
4001 Cobb International Blvd NW, Kennesaw, GA 30152

What Security Features Should Schools Demand from Surveillance Vendors?

Cybersecurity should be evaluated with the same scrutiny as video quality or analytics performance.

Schools should prioritize technologies that incorporate security throughout the entire product lifecycle.

Secure Firmware and Device Integrity	Devices should support secure boot processes and digitally signed firmware updates to help ensure systems operate only with verified software.
Encryption and Secure Communications	All communication between cameras, servers, management systems, and users should be protected using modern encryption standards.
Ongoing Security Support	Schools should seek technology partners that provide: • Regular firmware updates. • Long-term support commitments. • Vulnerability disclosure programs. • Security-focused product development practices.
Advanced Cybersecurity Capabilities	Additional security capabilities can further reduce risk, including encrypted cloud connectivity, centralized user management, secure evidence sharing, real-time health monitoring, and automated alerts that identify device failures, communication issues, or potential tampering attempts.

Cybersecurity maturity should be viewed as a core purchasing criterion rather than an optional feature.

CONTACT US
support@i3international.com | 1.877.877.7241
Monday-Friday, 8:30AM - 8:00PM (EST)

CANADA
i3 International Inc. 251 Bartley Drive,
Unit 3 Toronto, ON M4A 2N7

USA
i3 America (Nevada) Inc.
4001 Cobb International Blvd NW, Kennesaw, GA 30152

How Should Access to Surveillance Systems Be Controlled?

Access management remains one of the most important supports of surveillance cybersecurity.

Default credentials should be eliminated immediately following installation, and multi-factor authentication should be implemented wherever possible.

Role-based access controls help ensure users receive only the permissions necessary to perform their duties.

Classic examples include:



Security personnel monitoring live videos.



Administrators managing system configurations.



IT staff overseeing infrastructure health and cybersecurity.

Applying least privileged principles reduces risk while improving accountability and oversight.

CONTACT US
support@i3international.com | 1.877.877.7241
Monday-Friday, 8:30AM - 8:00PM (EST)

CANADA
i3 International Inc. 251 Bartley Drive,
Unit 3 Toronto, ON M4A 2N7

USA
i3 America (Nevada) Inc.
4001 Cobb International Blvd NW, Kennesaw, GA 30152

How Can Schools Protect Surveillance Data Throughout Its Lifecycle?

Video surveillance systems generate significant amounts of sensitive information.

Protecting that data requires security controls that extend across its entire lifecycle, from capture and storage to sharing and retention.

Video data should remain protected while:

01 **Being transmitted across networks.**

02 **Stored on local recording platforms.**

03 **Archived in cloud environments.**

04 **Shared during investigations.**

Strong encryption, secure storage mechanisms, effective key management, and clearly defined sharing procedures all play critical roles in maintaining data security. Schools should also consider secure cloud-based management capabilities that support encrypted video transfer, centralized access controls, secure backup processes, and controlled incident sharing. These capabilities help maintain requirements while minimizing unauthorized access risks.

Protecting surveillance data is both a cybersecurity obligation and a privacy responsibility.

CONTACT US
support@i3international.com | 1.877.877.7241
Monday-Friday, 8:30AM - 8:00PM (EST)

CANADA
i3 International Inc. 251 Bartley Drive,
Unit 3 Toronto, ON M4A 2N7

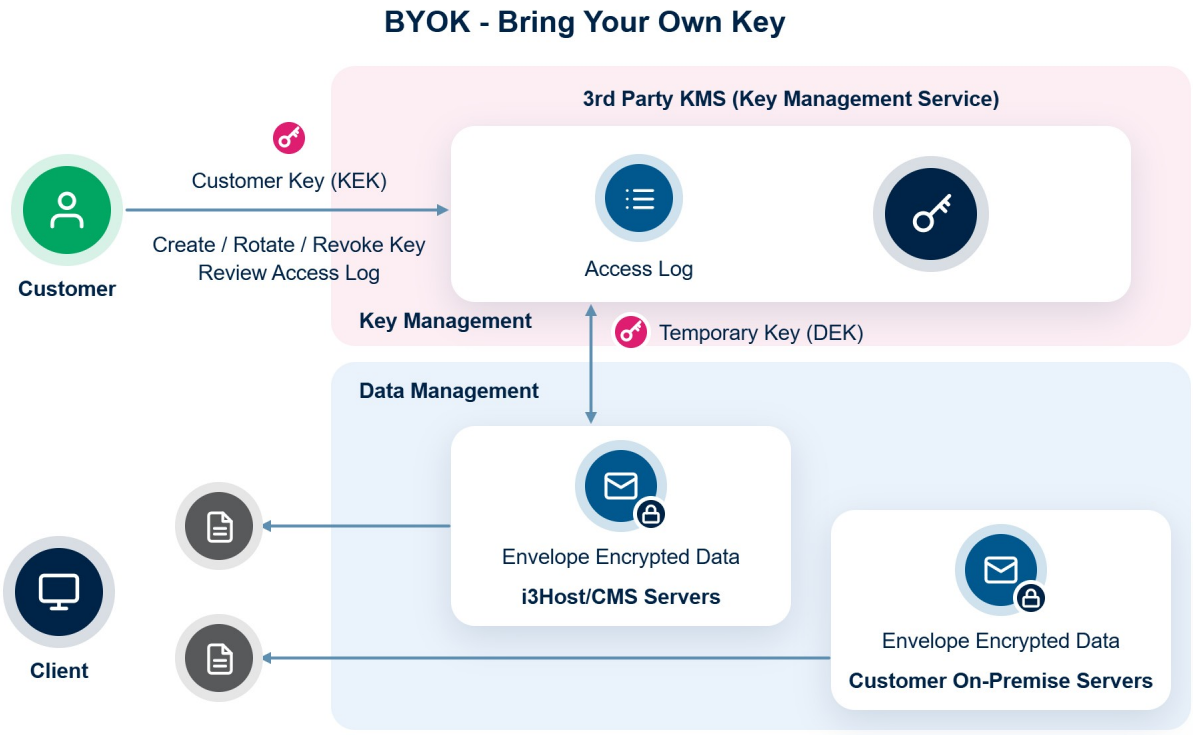
USA
i3 America (Nevada) Inc.
4001 Cobb International Blvd NW, Kennesaw, GA 30152

How Can Schools Maintain Control of Encryption Keys in Cloud-Based Surveillance Environments?

As educational institutions increasingly adopt cloud-connected security technologies, protecting data extends beyond encryption alone. Equally important is controlling the encryption keys that protect that data.

Modern surveillance platforms are increasingly leveraging cloud storage and cloud-based services to simplify management, improve scalability, and strengthen resilience. While these capabilities offer significant operational benefits, many schools and public-sector organizations require greater control over how sensitive security data is protected.

To address these concerns, advanced cloud security architectures support Bring Your Own Key (BYOK) encryption models that allow organizations to maintain ownership and control of their encryption keys. In a BYOK environment, surveillance data always remains encrypted, but the organization retains authority over the keys used to protect that information.



- Customer data is always encrypted with the customer owned key.
- KMS never access the data
- Envelope Encryption with wrapped data encryption key.
- Customer can create and revoke key any time, as only owner of the key.
- i3Service never access the customer key

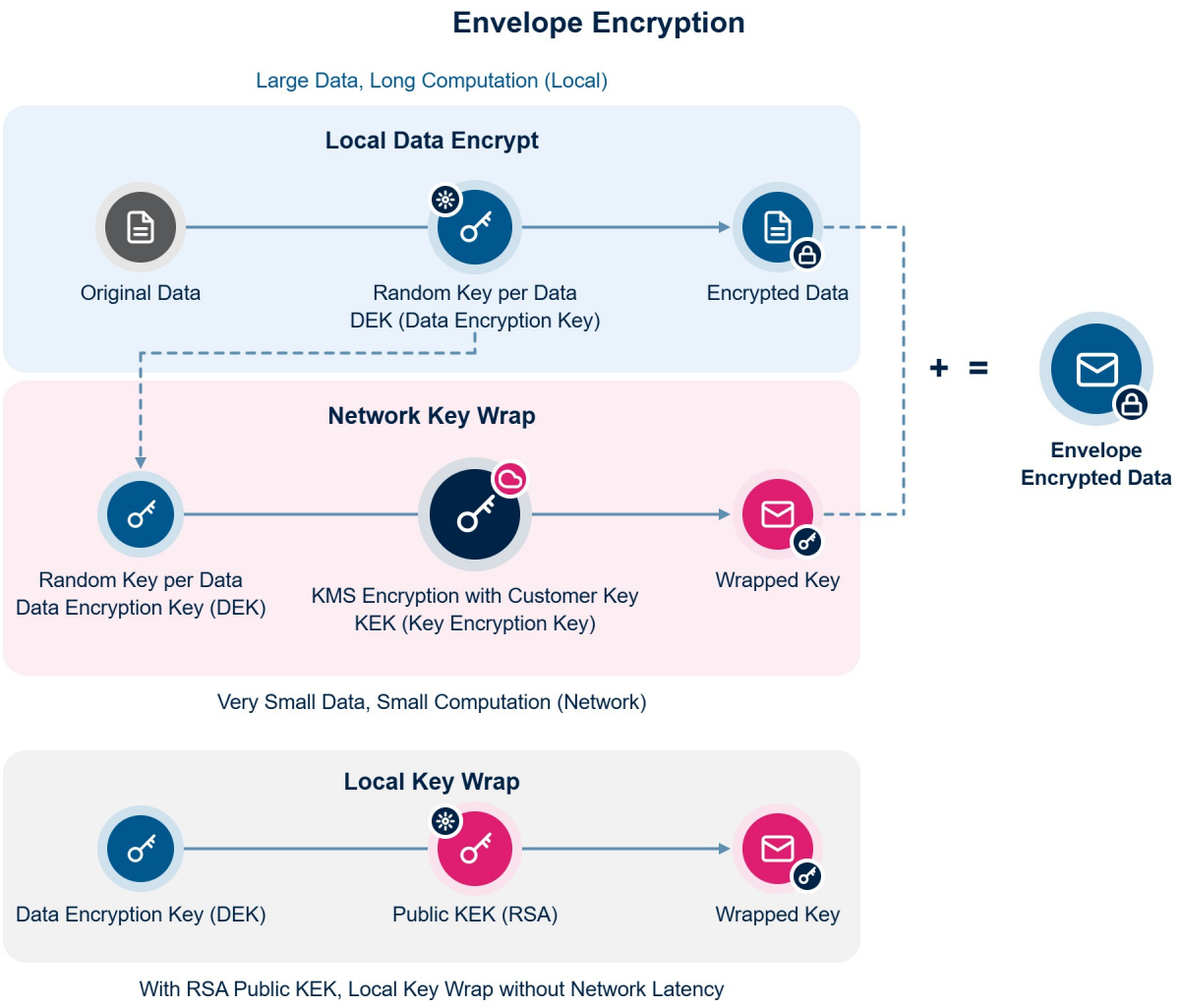
CONTACT US
support@i3international.com | 1.877.877.7241
Monday-Friday, 8:30AM - 8:00PM (EST)

CANADA
i3 International Inc. 251 Bartley Drive,
Unit 3 Toronto, ON M4A 2N7

USA
i3 America (Nevada) Inc.
4001 Cobb International Blvd NW, Kennesaw, GA 30152

Understanding Encryption Keys

Encryption converts readable information into protected data that cannot be accessed without the appropriate cryptographic key. Whether video evidence is being transmitted, stored, archived, or shared, encryption helps ensure data remains protected from unauthorized access.

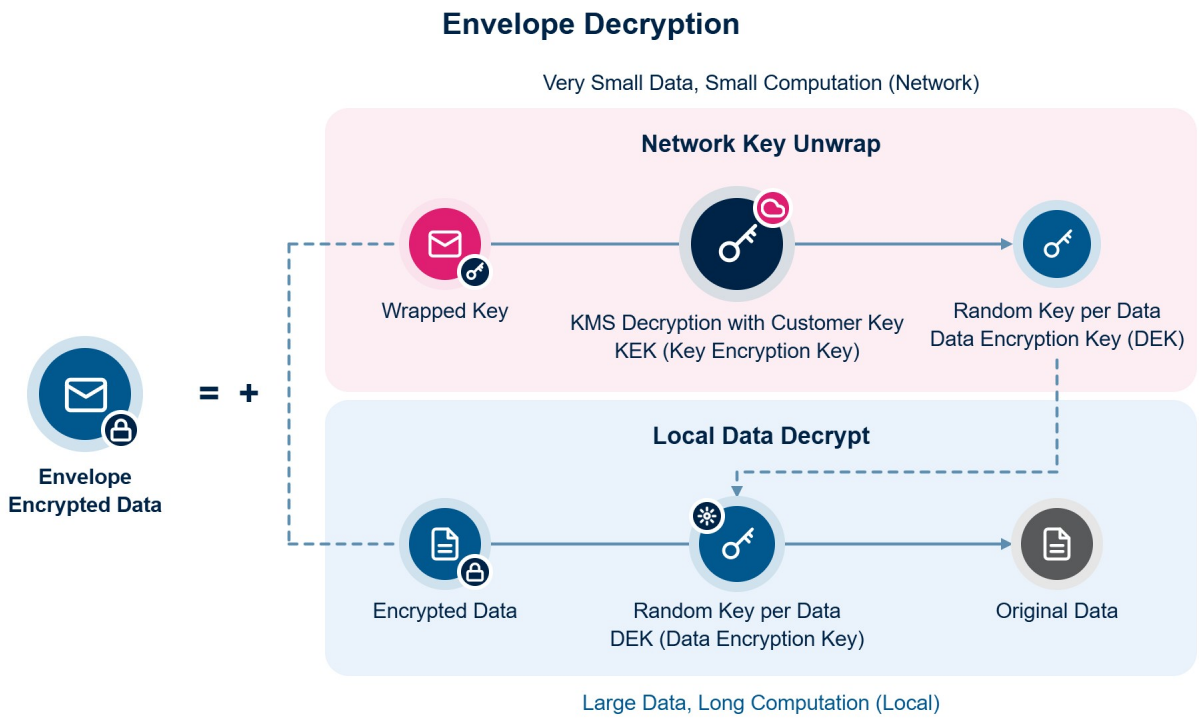


- DEK, Data Encryption Key, used to encrypt data, randomly generetaed short text per data.
- KEK, Key Encryption Key,used to wrap (encrypt) DEK, customer created key unknown to any other.
- RSA KEK, faster encryption, public RSA Key of KEK can be used repeatedly in a session.

CONTACT US
support@i3international.com | 1.877.877.7241
Monday-Friday, 8:30AM - 8:00PM (EST)

CANADA
i3 International Inc. 251 Bartley Drive,
Unit 3 Toronto, ON M4A 2N7

USA
i3 America (Nevada) Inc.
4001 Cobb International Blvd NW, Kennesaw, GA 30152



- Only KMS can unwrap DEK, without KMS, data reading is not possible.

To simplify key management while maintaining strong security, modern platforms typically offer two approaches:

Option 1: Bring Your Own Key (BYOK)

For organizations requiring maximum control over their data security, encryption keys can be managed through an external Key Management Service (KMS).

Under this model:

- Surveillance data is always encrypted.
- Encryption keys remain under customer control.
- The surveillance provider never has access to the customer's encryption key.
- Encryption and decryption operations are performed through the customer's KMS.
- Organizations can rotate, replace, or revoke keys without relying on the surveillance vendor.
- Detailed key usage logs can provide additional auditability and compliance support.

CONTACT US
support@i3international.com | 1.877.877.7241
Monday-Friday, 8:30AM - 8:00PM (EST)

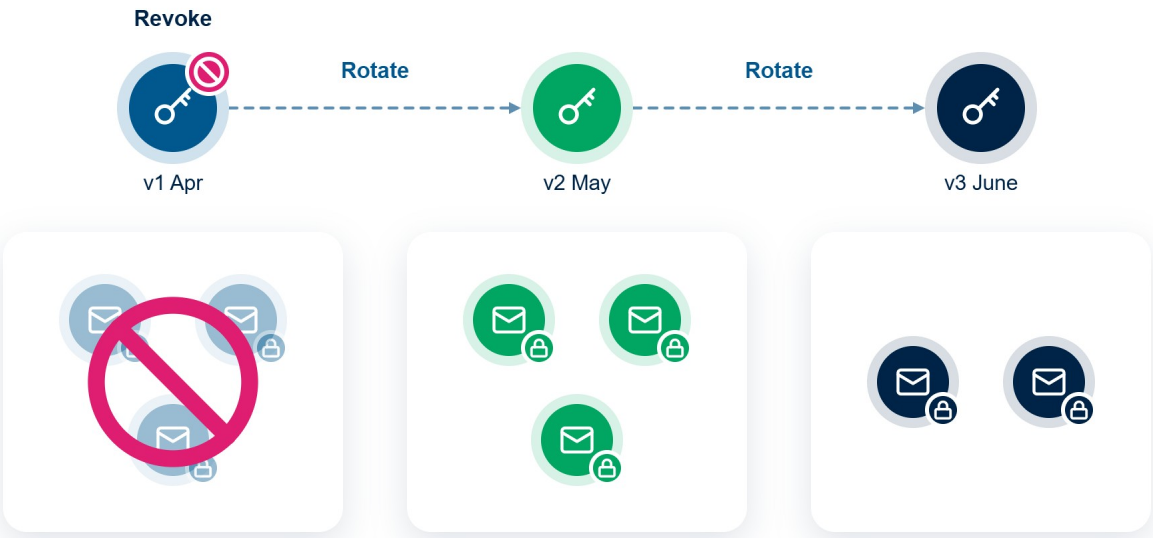
CANADA
i3 International Inc. 251 Bartley Drive,
Unit 3 Toronto, ON M4A 2N7

USA
i3 America (Nevada) Inc.
4001 Cobb International Blvd NW, Kennesaw, GA 30152

This approach significantly reduces risk because the cloud provider can store encrypted data but cannot independently decrypt it without authorization from the customer's key management system.

If an organization chooses to revoke a key, any data protected using that key can immediately become inaccessible, providing an additional layer of control over sensitive information.

Key Rotation and Revocation



- Rotate Key, KMS can periodically generate new key and keep all old keys.
- Revoke Key, Once a key is revoked, any data enveloped with a revoked key can't be read any longer.
- Customer can generate a new key any time and revoke any key any time.

CONTACT US
support@i3international.com | 1.877.877.7241
Monday-Friday, 8:30AM - 8:00PM (EST)

CANADA
i3 International Inc. 251 Bartley Drive,
Unit 3 Toronto, ON M4A 2N7

USA
i3 America (Nevada) Inc.
4001 Cobb International Blvd NW, Kennesaw, GA 30152

Option 2: Provider-Managed Encryption Keys

Not every school district has the resources or desire to manage its own encryption infrastructure. For these organizations, cloud platforms may offer provider-managed encryption keys.

Under this approach:

- **Surveillance data always remains encrypted.**
- **Encryption keys are managed by the service provider.**
- **Schools benefit from strong data protection without the complexity of operating a separate KMS environment.**
- **Data is never stored in plain text.**

While organizations may have less direct control over key management, provider-managed encryption can still deliver strong protection when combined with secure cloud architecture, role-based access controls, audit logging, and continuous monitoring.

CONTACT US
support@i3international.com | 1.877.877.7241
Monday-Friday, 8:30AM - 8:00PM (EST)

CANADA
i3 International Inc. 251 Bartley Drive,
Unit 3 Toronto, ON M4A 2N7

USA
i3 America (Nevada) Inc.
4001 Cobb International Blvd NW, Kennesaw, GA 30152

Why Key Management Matters for School Security

Encryption is only as effective as the controls governing the keys themselves. For educational institutions managing sensitive video evidence, student privacy concerns, and regulatory obligations, strong key management helps ensure:

- **Video data remains protected even if storage systems are compromised.**
- **Access to surveillance evidence can be tightly controlled.**
- **Security administrators maintain visibility into encryption activity.**
- **Data ownership remains with the organization.**
- **Cloud services can be utilized without sacrificing security requirements.**

As surveillance systems continue to expand into cloud-connected environments, organizations should evaluate not only whether data is encrypted, but also who controls the keys used to protect it. Advanced key management capabilities such as BYOK provide schools with greater transparency, stronger governance, and enhanced confidence that sensitive security data remains under their control

CONTACT US
support@i3international.com | 1.877.877.7241
Monday-Friday, 8:30AM - 8:00PM (EST)

CANADA
i3 International Inc. 251 Bartley Drive,
Unit 3 Toronto, ON M4A 2N7

USA
i3 America (Nevada) Inc.
4001 Cobb International Blvd NW, Kennesaw, GA 30152

How Can Schools Prepare for a Security Incident Before One Happens?

One of the most overlooked aspects of surveillance cybersecurity is incident preparedness.

Many organizations invest heavily in prevention while spending far less time developing response strategies.

The reality is that no security environment is immune to failure. Devices go offline. Networks experience outages. Vulnerabilities emerge. Cyberattacks occur.

Schools should establish clear procedures that answer critical questions:

- **Who should be notified if cameras become unavailable?**
- **How will investigations continue during a system outage?**
- **What happens if recording infrastructure is compromised?**
- **How quickly can critical systems be restored?**
- **What backup procedures exist for evidence preservation?**

Just as schools conduct lockdown drills, fire alarm drills and other emergency response exercises, they should regularly evaluate the resilience of their surveillance infrastructure and incident response plans.

> *Cybersecurity is not measured solely by the absence of incidents. It is measured by an organization's ability to respond effectively when incidents occur.*

CONTACT US
support@i3international.com | 1.877.877.7241
Monday-Friday, 8:30AM - 8:00PM (EST)

CANADA
i3 International Inc. 251 Bartley Drive,
Unit 3 Toronto, ON M4A 2N7

USA
i3 America (Nevada) Inc.
4001 Cobb International Blvd NW, Kennesaw, GA 30152

How Can Modern Security Platforms Simplify Cybersecurity Management?

Managing hundreds or even thousands of security devices can create significant operational challenges.

Modern surveillance platforms help reduce this complexity by centralizing administration while incorporating cybersecurity controls directly into daily operations.

Common capabilities include:

- Centralized device management.
- Automated notifications and alerts.
- Encrypted evidence sharing.
- Role-based access controls.
- Real-time system health monitoring.
- Secure cloud connectivity.
- Audit trails and or activity tracking.

These capabilities not only strengthen cybersecurity but also reduce administrative burdens for both security and IT teams.

CONTACT US
support@i3international.com | 1.877.877.7241
Monday-Friday, 8:30AM - 8:00PM (EST)

CANADA
i3 International Inc. 251 Bartley Drive,
Unit 3 Toronto, ON M4A 2N7

USA
i3 America (Nevada) Inc.
4001 Cobb International Blvd NW, Kennesaw, GA 30152

How Can Artificial Intelligence Improve Security Without Increasing Risk?

Artificial intelligence is rapidly transforming modern surveillance programs.

When implemented responsibly, AI can help security teams identify unusual activity, prioritize alerts, automate routine monitoring tasks, and speed up investigations.

Advanced analytics can assist with:

- Intelligent video search.
- Camera tampering identification.
- Automated incident notifications.
- Loitering detection.
- Obstruction detection.
- Operational health monitoring.

However, AI should enhance human decision-making rather than replace it.

Schools must establish policies that define how analytics are configured, monitored, reviewed, and validated. Transparency, accountability, and privacy considerations should remain central to every deployment.

> *The future of surveillance is not about collecting more videos. It is about transforming data into actionable intelligence while maintaining trust and security.*

CONTACT US
support@i3international.com | 1.877.877.7241
Monday-Friday, 8:30AM - 8:00PM (EST)

CANADA
i3 International Inc. 251 Bartley Drive,
Unit 3 Toronto, ON M4A 2N7

USA
i3 America (Nevada) Inc.
4001 Cobb International Blvd NW, Kennesaw, GA 30152

How Can Schools Improve Situational Awareness Beyond Traditional Cameras?

While cameras remain the foundation of most surveillance deployments, they are no longer the only source of meaningful security intelligence.

Many schools are now leveraging intelligent sensors and integrated analytics platforms to gain visibility into incidents that may not be captured through video alone.

Environmental monitoring solutions can help identify vaping activity, air quality concerns, aggression indicators, and other safety-related events occurring throughout school facilities. When integrated with video surveillance systems, these technologies provide additional context and improve response effectiveness.

Equally important, integrated platforms can provide real-time health monitoring for cameras, servers, and connected devices, enabling administrators to identify failures before they affect the overall safety.

By combining video surveillance, analytics, sensor technologies, and centralized management, schools can create a more comprehensive and resilient security ecosystem.

CONTACT US
support@i3international.com | 1.877.877.7241
Monday-Friday, 8:30AM - 8:00PM (EST)

CANADA
i3 International Inc. 251 Bartley Drive,
Unit 3 Toronto, ON M4A 2N7

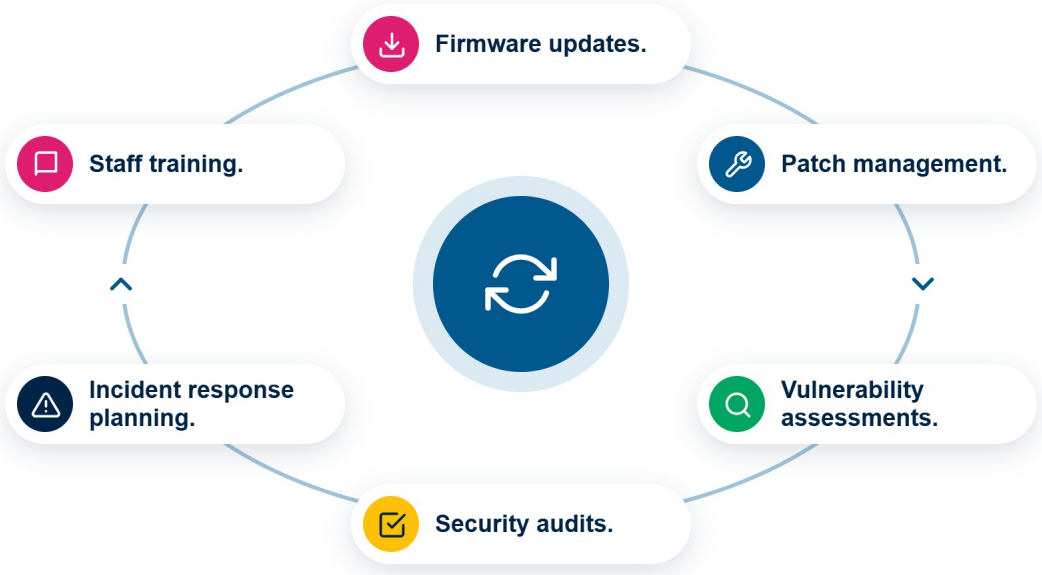
USA
i3 America (Nevada) Inc.
4001 Cobb International Blvd NW, Kennesaw, GA 30152

Why Is Ongoing Cybersecurity Management Essential?

Cybersecurity is not a one-time project.

Threats evolve. Technologies change. New vulnerabilities emerge. Security programs must continuously adapt.

Schools should establish formal processes for:



Regular assessments help identify weaknesses before they become operational risks and ensure systems continue to align with evolving security requirements.

> *Long-term resilience depends on treating cybersecurity as a continuous operational practice rather than a deployment milestone.*

CONTACT US
support@i3international.com | 1.877.877.7241
Monday-Friday, 8:30AM - 8:00PM (EST)

CANADA
i3 International Inc. 251 Bartley Drive,
Unit 3 Toronto, ON M4A 2N7

USA
i3 America (Nevada) Inc.
4001 Cobb International Blvd NW, Kennesaw, GA 30152

What Does the Future of Secure School Surveillance Look Like?

The conversation around school surveillance has changed dramatically.

The question is no longer whether schools should deploy video surveillance technologies. The question is whether those technologies can be trusted to operate securely, reliably, and effectively in an increasingly connected world.

Building a cybersecure surveillance environment requires more than selecting cameras and deploying recording servers. It demands thoughtful architecture, secure data practices, continuous monitoring, strong control, and collaboration between security and IT departments.

Schools that embrace this approach gain more than protection from cyber threats. They create resilient security ecosystems capable of supporting investigations, emergency response, compliance requirements, and day-to-day operations.

As surveillance technologies continue to evolve, the institutions that succeed will be those that view cybersecurity not as an added feature, but as a fundamental design principle.

By embedding security into every stage of the surveillance lifecycle, schools can better protect their students, staff, facilities, and the technologies that help keep them safe. In the modern educational environment, an effective surveillance system does more than record incidents. It provides the foundation for a safer, more resilient, and more secure school.

CONTACT US
support@i3international.com | 1.877.877.7241
Monday-Friday, 8:30AM - 8:00PM (EST)

CANADA
i3 International Inc. 251 Bartley Drive,
Unit 3 Toronto, ON M4A 2N7

USA
i3 America (Nevada) Inc.
4001 Cobb International Blvd NW, Kennesaw, GA 30152