

# Four Critical Imperatives for a Proactive Security Transformation

\$100B in retail shrinkage. \$130B lost to workplace violence. Why security must evolve from response to prevention.





The stakes have never been higher. Security leaders in loss prevention, asset protection, and risk management are operating in an environment defined by complexity, scale, and rising risk. Financial loss, workplace violence, and increasingly sophisticated criminal activity have elevated security from a back-office function to a strategic business priority.

These U.S. statistics over the last few years are not isolated incidents — they are early indicators of a global security crisis.:

- ✓ **Retail Shrink:** U.S. retailers lost \$100B
- ✓ **Employee Theft:** \$30B in annual losses
- ✓ **Workplace Violence:** Costs businesses over \$130B each year
- ✓ **Tool Theft:** Over \$1B in rental equipment stolen annually
- ✓ **ATM Losses:** \$6M per year, with 66% involving physical attacks

This escalating financial loss and continued exposure have transformed security from a compliance function into a critical strategic imperative. Today's security leaders are no longer focused solely on response and enforcement. Their roles now span enterprise-wide responsibilities that require deeper data analysis, real-time decision-making, and active oversight of technology-driven security systems.

At the same time, they are expected to deliver stronger outcomes with constrained resources, heightened accountability, and broader organizational impact. In this environment, speed matters — delays in detection and response directly increase organizational exposure, making speed as critical as the technology itself.

Given this landscape, it's clear: traditional security approaches are no longer sufficient. Organizations now need strategies and systems that proactively prevent incidents, protect people, and safeguard assets across all operations.



# Why Traditional Security Systems Fall Short

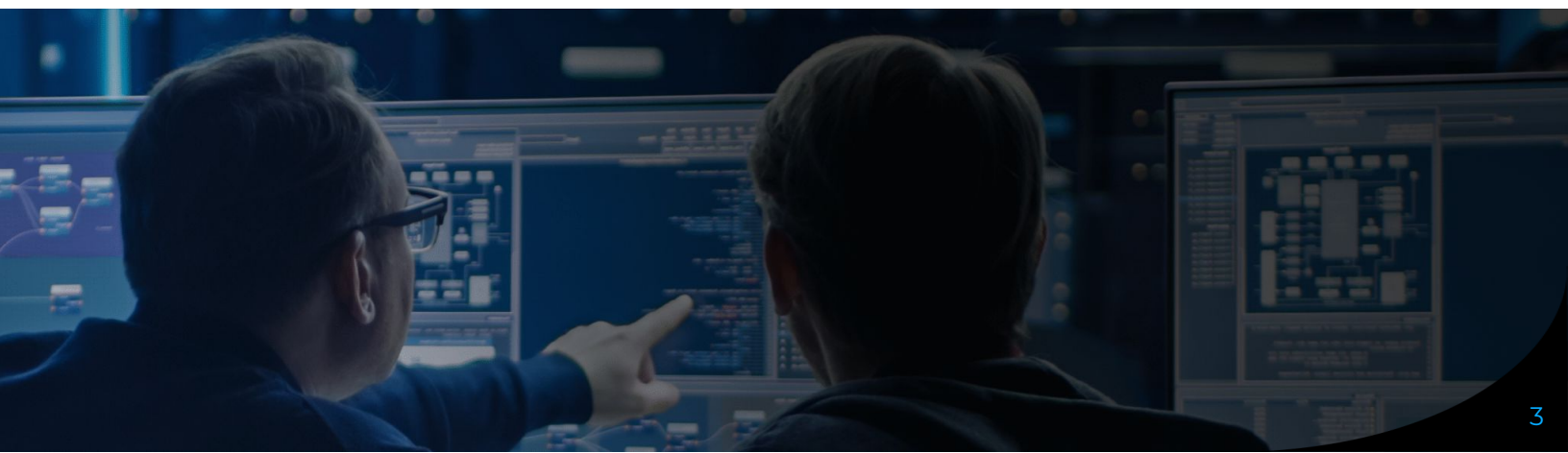
Many enterprise security environments still rely on legacy systems built for a very different risk landscape. Traditional video surveillance, alarms, and access control tools were designed to document incidents after they occur, not prevent them in real time. Recreating or replacing these systems is often costly, time-intensive, and still insufficient to meet modern security expectations.

## The Evolving Threat Landscape

Security leaders face increasingly sophisticated and varied threats, each demanding more than traditional approaches can provide:

- ✓ **Organized Retail Crime (ORC):** Coordinated theft rings cause significant losses far beyond what basic surveillance can detect.
- ✓ **Internal Theft and Fraud:** Employee dishonesty, vendor fraud, and fraudulent delivery remain constant threats, requiring advanced monitoring and verification.
- ✓ **Workplace Violence:** Protecting employees — particularly remote or lone workers — requires immediate visibility and rapid emergency response.
- ✓ **Massive Inventory Shrinkage:** Unexplained loss directly impacts profits, making proactive loss prevention a strategic priority.
- ✓ **Global Supply Chain Attacks:** Espionage and blended cyber-physical threats require high-risk perimeter security and continuous real-time protection for both people and assets.

The scale and complexity of these threats make it clear that reactive approaches alone are no longer adequate.

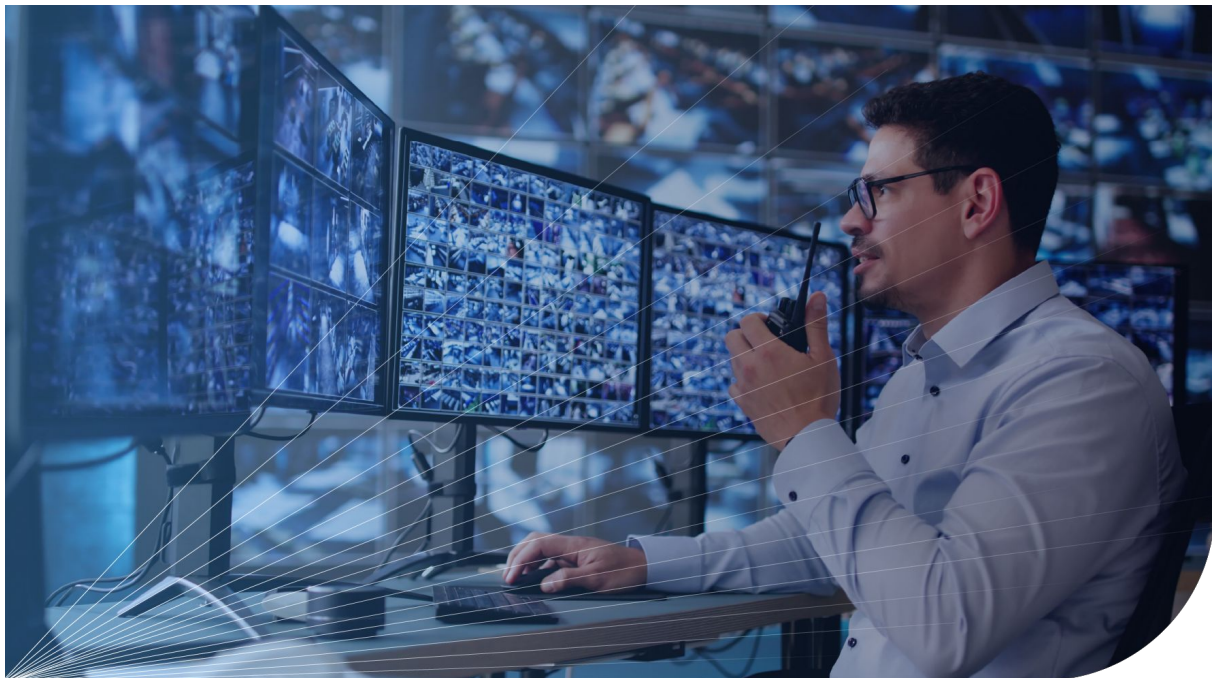




## The Limits of Legacy “Reactive” Security

Even with these threats clearly identified, many organizations remain tied to reactive systems. Traditional security tools — CCTV, standalone alarms, and siloed access control — create critical operational gaps:

- ✓ **Alert Fatigue:** Frequent false positives overwhelm teams, making it harder to recognize genuine emergencies.
- ✓ **Delayed Response:** Incidents often escalate before staff or law enforcement can intervene.
- ✓ **Costly Inefficiency:** Heavy reliance on on-site guards increases labor costs and limits a company’s ability to effectively scale across multi-site operations.
- ✓ **Staff Frustration:** Without real-time context, security personnel are less effective and more likely to experience operational burnout.



These limitations leave organizations exposed, even with robust legacy systems in place. While traditional tools are valuable for investigation and post-incident evidence, they cannot keep pace with the speed, scale, and sophistication of today’s threats.



# What Are The 4 Imperatives for a Proactive Security Transformation?

The limitations of legacy systems and the increasing complexity of threats are widening the gap between what security teams are expected to deliver and what traditional tools can support. Closing this gap requires a shift from reactive security to a proactive operating model.

Proactive security is more than adding cameras or alarms. At its core, it's about:

- ✓ **Detecting risk as it emerges**
- ✓ **Verifying threats in real time**
- ✓ **Acting decisively before incidents escalate**

Achieving this requires a modern security foundation that blends technology, intelligence, and human judgment to prevent loss, protect people, and safeguard operations at scale.

Leading organizations are now aligning around these four imperatives to define proactive security in 2026 and beyond. Across industries, security leaders are increasingly adopting technology-driven loss-prevention strategies to assess risk, manage shrink, and prevent incidents before they occur.

What follows are the four key imperatives required to make that transformation:

- 1. Building a Unified Security Platform**
- 2. Embracing AI and Video Analytics**
- 3. Gaining Real-Time Visual Awareness**
- 4. Deploying the Virtual Guard**





# IMPERATIVE #1

## Building a Unified Security Platform: Overcoming Silos

Organizations of all sizes face growing security challenges, from rising crime rates and workplace threats to evolving compliance requirements and operational complexity. Investing in modern security is essential, but separate, siloed tools for video surveillance, access control, alarms, sensors, and intercoms quickly lead to inefficiency, blind spots, and operational vulnerabilities.

The solution is a unified security platform. By consolidating all devices into a single, easy-to-use system, organizations can streamline management, reduce risk, improve coordination, and gain the visibility needed to detect threats and prevent incidents before they escalate. Just as importantly, unification reduces the total cost of ownership (TCO) by leveraging existing infrastructure rather than forcing costly system replacements.

Key benefits of a unified platform:

- **Total System Integration:** Eliminates blind spots by connecting CCTV, access control, and alarms into a single, real-time operational view.
- **Centralized Control:** Enables 24/7 remote management through cloud-based access to all security systems across all locations.
- **Consistent, Scalable Security:** Improves risk governance by enforcing policies consistently, continuously detecting anomalies, and allowing quick expansion to new sites, cameras, and sensors without retrofitting connections or rebuilding infrastructure.

A fully integrated security platform provides the foundation for proactive security, enabling teams to act quickly, consistently, and with full awareness across all locations.



**YOU SHOULD KNOW: CHeKT supports this shift by acting as a connective layer across existing security infrastructure. Rather than forcing organizations to replace everything at once, this approach enables a practical transition toward unified visibility and control — an essential foundation for proactive security.**



## IMPERATIVE #2

# Embracing AI and Video Analytics: From Detection to Prevention

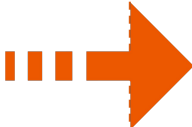
Historically, security technology focused on detection and response, but advancements in AI allow organizations to shift from reacting to preventing incidents. Agentic AI goes beyond simple automation, interpreting data, making decisions, and executing actions with minimal human intervention — a first line of defense in corporate offices, logistics, and data centers. When applied correctly, AI acts as a force multiplier — amplifying human judgment rather than replacing it.

**Industry research shows** 93% of security decision-makers plan to use technology to reduce the likelihood of threats, while nearly half plan to use it to strengthen human capabilities for improved detection and prevention.

The AI attributes deemed most crucial to adopt over the next few years include:

- ✓ **Earlier threat detection at the perimeter:** Uses AI and machine learning to identify, assess, and respond to unauthorized access and suspicious activity before incidents escalate.
- ✓ **Always-on, AI-Driven Threat Analysis:** Continuously analyzes data from cameras and sensors to surface anomalies and prioritize genuine threats faster than human operators alone.
- ✓ **Intelligent Access & Behavior Monitoring:** Applies AI-driven facial recognition, license plate recognition, and live video analytics to manage restricted areas and detect high-risk behaviors — such as loitering, crossing secure boundaries, or climbing fences or barriers — providing operators with actionable context, not just alerts.

By leveraging AI to detect and analyze emerging threats in real time, organizations can act decisively before incidents occur, strengthening both security and operational efficiency.



**YOU SHOULD KNOW: One connection to the CHEKT Video Control Panel brings AI analytics, cameras, alarms, and IP speakers together — delivering real-time intelligence to stop threats to a business before they become losses**



## IMPERATIVE #3

# Gaining Real-Time Visual Awareness: Enabling Immediate Action

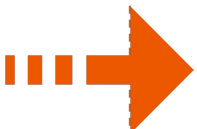
Innovative security decision-makers leverage AI not as a replacement for staff, but as an analytical and advisory tool to enhance their ability to respond to risks more effectively. Unlike passive video recording, modern surveillance networks continuously monitor and alert teams to emerging threats.

The powerful combination of AI paired with a security operator enables remote operators to continuously monitor activity using cameras, recorders, and analytics to detect threats as they happen, enabling quick responses to physical attacks or workplace violence, internal theft in stock rooms, and inventory loss on manufacturing floors.

Real-time insights empower confident, proactive responses:

- **Holistic Situational Clarity:** Combines multi-camera feeds and real-time video to give operators full context as incidents unfold, enabling immediate, informed intervention.
- **Operator Confidence & Rapid Response:** Delivers actionable alerts with visual verification, enabling security teams to act decisively, reduce escalation, and prevent loss across sites.
- **Smarter Investment and Risk Decisions:** Leverages analytics from video, access control, and security systems to identify trends, measure ROI, and prioritize risk reduction — while providing operational insights into customer flow, compliance, and overall business performance.

Real-time visual awareness enables security teams to detect and respond to issues immediately, providing a proactive layer of protection that bridges the gap between detection and action.



**YOU SHOULD KNOW: CHeKT enables this level of clarity by delivering real-time, visual context alongside alerts, allowing teams to verify events instantly and act with confidence. This operational visibility becomes a cornerstone of proactive security.**



## IMPERATIVE #4

# Deploying the Virtual Guard: Extending Coverage Without Compromise

Staffing limitations often leave organizations stretched thin, resulting in coverage gaps — especially across multi-site or expansive properties with long perimeters, isolated areas, and high-risk sites such as distribution centers, construction zones, and large enterprise campuses.

The “digitization of guards” integrates human teams with technology to extend monitoring coverage remotely, enabling faster risk detection, and allowing personnel to focus on high-priority issues. Strategic deployment of technology alongside mobile or on-site guards improves efficiency, reduces labor costs, and ensures rapid response.

This hybrid coverage results in:

- ✓ **Expanded Remote Coverage & Proactive Detection:** Enables operators to monitor multiple sites via a cloud-based dashboard, verify alerts in real time, and detect suspicious behavior, unauthorized access, or perimeter breaches — extending coverage without adding headcount.
- ✓ **Centralized Control & Operational Efficiency:** Allows security leaders to arm/disarm alarms and manage high-risk zones from a cloud-accessible interface. This helps maintain consistent protection, streamline investigations, reduce false alarms, and optimize resource allocation.
- ✓ **Cost-Effective Security Operations:** Supports strategic deployment of human guards and mobile patrols, lowers reliance on expensive on-site coverage, and maximizes return on investment across multi-site operations.

Innovative security leaders are adopting a hybrid approach combining technology with strategically placed human guards or mobile patrols. It offers the best of both worlds — broad tech coverage and focused human judgment.



**YOU SHOULD KNOW: CHekt supports the virtual guard model by enabling remote monitoring, real-time verification, and centralized control across sites — allowing organizations to maintain constant vigilance while deploying human resources more strategically.**



# How CHeKT Delivers on the Proactive Security Imperatives

CHeKT transforms commercial security into a fully informed, responsive system by integrating AI-powered cameras, intelligent video analytics, and interior detection into your existing security infrastructure. This provides security leaders and their teams with the situational awareness needed for immediate, informed responses, verified escalation, and measurable ROI.

## CHeKT Proactive Visual Security Platform Core Capabilities:

- ✓ **Unified security ops:** Integrates seamlessly with existing systems to reduce total cost of ownership (TCO).
- ✓ **Analytics to alarms:** Instantly converts AI insights into actionable events.
- ✓ **Remote visual monitoring:** Pairs live video with alerts to show exactly what triggered an alarm.
- ✓ **Cloud integration:** Securely manage devices, events, and footage from anywhere.
- ✓ **Custom alarm zones:** Quickly define high-risk areas for more focused protection.
- ✓ **Intuitive interface:** Direct access through a dashboard or mobile app to live video, maps, event histories, alarm data, and interaction tools.
- ✓ **Real-time response:** Live video alarms enable immediate action via triggered security lighting, audio alerts, live 'talk-downs', and quick emergency dispatch.

## Why Organizations Choose CHeKT:

- ➡ **Strategic Advantage:** Shifts security from a reactive cost center to a proactive, prevention-first business asset through features like seamless integration, a cloud-based interface, and AI-powered detection of threats.
- ➡ **Operational Efficiency:** Streamlines security and extends coverage without increasing headcount via real-time visual verification, automated deterrence, remote monitoring, and verified escalation to law enforcement.
- ➡ **Business Impact:** Prevents loss, reduces shrink, and provides measurable ROI through reduced insurance premiums, headcount, and streamlined investigations using verified video footage.



# Proactive Visual Security: From Cost Center to Strategic Asset

In today's environment, every unprotected dollar represents lost revenue, and every minute without visibility is a missed opportunity to prevent theft, fraud, or harm. Security has evolved beyond a back-office function — it is now a strategic lever that directly impacts the bottom line. Rising threats, from organized retail crime, internal theft, workplace violence, and supply chain attacks, demand proactive solutions that stop incidents before they occur.

CHeKT transforms security from a reactive cost center into a proactive, prevention-first operational advantage. Security teams gain the visibility, tools, and confidence to detect threats early, respond decisively, and protect people and assets, all while improving efficiency and business outcomes.

By adopting CHeKT Proactive Visual Security, organizations can protect people, preserve assets, and strengthen business performance.

- ✓ **Stop losses before they happen** by detecting theft, fraud, and operational risks early.
- ✓ **Keep people safe** with real-time visibility and rapid response.
- ✓ **Empower law enforcement** with verified, actionable intelligence.
- ✓ **Maximize ROI** by reducing shrink, claims, and operational friction.

CHeKT Proactive Visual Security helps transform security from a reactive cost center into a strategic business asset — delivering measurable value to your organization.



**Ready to transform your security operations?**

**Contact us today** for a demo or to discuss how CHeKT can help protect your people, assets, and operations.



With CHeKT, video isn't an afterthought — it's the frontline. Every camera, every alarm, and every AI tool work seamlessly in one cloud platform to prevent crime in real time. What was once reactive is now proactive.

We provide security integrators, monitoring centers, and the people they protect a Proactive Visual Security Platform that seamlessly integrates with the systems they use everyday and enables them to quickly identify what triggered an event, and the tools they need to instantly verify, deter, and ensure an immediate response.

Today, our platform powers proactive security for thousands of companies worldwide. With the backing of Alarm.com (NASDAQ: ALRM), we're scaling fast while staying independent and true to our dealer-first roots.

For more information, visit [www.chekt.com](http://www.chekt.com)

