Seven forces driving the next era of security

The power behind **your mission**

Executive summary

Security is no longer just about cameras, locks and guards — it's a data-driven, digitally integrated and business-critical discipline. Organizations expect security to protect and drive business intelligence, operational efficiency, user experience and corporate responsibility.

Drawing on conversations with industry leaders and feedback from our customers during security advisory council sessions, we've identified seven forces defining security strategies in the coming year. These forces demonstrate how security is moving from a reactive function to a central enabler of organizational resilience and success.

From harnessing video analytics for business intelligence to aligning security with ESG goals, these trends reflect the realities security leaders face today: balancing innovation with risk management and delivering protection and business value.

Trend #1:

Harnessing video analytics as a driver of business intelligence

From surveillance to strategy

Video analytics has evolved from a reactive surveillance tool to a proactive platform for business intelligence. In fact, global information security spending is projected to climb from approximately $193 billion in 2024 to $213 billion in 2025 — a 10–11% increase — **with further growth of around 12.5% in 2026, reaching $240 billion**. Organizations use it to reduce risk and gain insights that shape operations and strategy.

Benefits

- People counting, heat mapping and space utilization to optimize real estate and hybrid work strategies.
- Flow analysis to enhance retail layouts and product placement.
- Troubleshooting tools that isolate root causes and reduce downtime.
- Johnson Controls solutions like **OpenBlue Companion** and **C•CURE 9000 v3.0** provide real-time occupancy insights and area control, helping organizations improve space utilization, enforce limits and enhance safety while reducing costs.

Technology deployment models

Organizations are adapting hybrid deployment models. Edge analytics enables faster, bandwidth-efficient processing directly at the camera level, while centralized or cloud-based analytics provide cross-location, enterprise-wide insights. Most organizations now pursue a hybrid edge-cloud approach to balance speed, depth and scalability.

Stakeholder expansion

As a result, video analytics no longer sit solely within the purview of security teams. IT, operations, HR, real estate and retail divisions are all stakeholders, broadening security's role across enterprises. Increasingly, video management systems integrate with other building and security platforms, enabling more coordinated responses and insights that ripple across the business. Solutions like the **Metasys Building Automation System** already integrate these diverse data points, helping organizations unify HVAC, fire, lighting and security insights within a single platform.

Trend #2

Structuring security budgets around strategic outcomes

Security budgets are evolving from ad hoc, reactive expenditures to structured, lifecycle-based investments. Rather than scrambling to respond to new threats or outdated equipment, organizations are building long-term plans that align security upgrades with broader business objectives.

Maturing budget practices

- Refresh cycles and programmatic upgrades are now tied to IT budgets, enabling more consistent planning.
- **Security now accounts for over 13% of IT budgets** (up from 8.6% in 2020).
- The C-suite increasingly demands ROI justification, whether in the form of student enrollment in education, improved customer experience in retail or reduced service calls in enterprise environments.

Best practices emerging

Organizations are adopting phased budgeting approaches to maintain flexibility in the face of shifting priorities. Many are piloting emerging technologies — particularly AI — before scaling them enterprise-wide, ensuring maturity and alignment before committing significant investments. Cross-functional planning between security, IT and operations is becoming the norm, embedding security more deeply into organizational strategy.

Trend #3

Applying AI-powered security with guardrails and human oversight

AI is transforming the security industry, accelerating capabilities from video analytics to automated reporting. Yet the consensus is clear: AI should augment, not replace, human judgment.

Adoption in action

Current use cases range from chatbots and copilots to triaging emails, monitoring videos and deploying drones for alarm verification. Organizations find that a balance — 80% efficiency gains from AI paired with 20% human oversight — delivers productivity and accuracy. In practice, AI-driven security adopters **estimate they are detecting threats 30% faster and achieving a 40% boost in return on security investment**, underscoring the ROI of responsible deployment when paired with human oversight.

Agentic AI is advancing this model by functioning as ‘co-workers’ that take on repetitive or multi-step tasks. These agents can act autonomously with limited oversight while keeping humans in the loop where judgment is critical. Just as importantly, they enable proactive workflows — anticipating risks, initiating responses and streamlining operations before issues escalate.

To mitigate risks like false positives and deepfakes, organizations are enforcing:

- Legal approvals and IT alignment before deployment.
- Privacy-by-design principles and cybersecurity safeguards.
- Employee training on responsible use, ensuring human review remains in the loop.

With government agencies like CISA issuing new guidance and breaches regularly making headlines, data security is inseparable from AI adoption. Customers expect security platforms to handle sensitive information responsibly, protecting privacy as AI becomes more deeply embedded in operations.

Platforms in practice

Offerings like **Connected Security Services** show how AI can be applied responsibly in building and security environments. By pairing proactive monitoring with predictive insights, the service helps facilities detect issues early, optimize performance and ensure human oversight remains central. As agentic AI matures, platforms will increasingly shift from reactive tools to proactive teammates that learn, adapt and optimize continuously.

Trend #4

Delivering consumer-grade experiences through security platforms

Users increasingly expect their security platforms to deliver the same seamless, intuitive experiences they encounter in consumer technology, from e-commerce sites to rideshare apps.

Desired features

Enterprises are asking for intuitive dashboards, real-time alerts, self-service ticket creation, online billing and lifecycle tracking. Pain points include repetitive data entry, lack of personalization and limited mobile integration.

Best-in-class benchmarks

Platforms that anticipate user needs, offer personalization and integrate services frictionlessly are setting the bar. Unified portals are especially appealing, enabling organizations to consolidate multiple tools into a single hub that reduces learning curves and accelerates resolution.

Why it matters

In practice, this consumer-grade experience directly impacts adoption and satisfaction. Platforms that minimize friction empower users, speed up problem resolution and elevate the role of security within the broader digital ecosystem.

Trend #5

Managing expanded identity and access in a mobile world

Mobile credentialing and biometrics are redefining identity and access management, blending convenience with new challenges:

- BYOD credentialing raises ongoing privacy concerns, though younger generations tend to be more accepting.
- Biometric-based (BYOF) access is gaining traction but presents compliance and auditing challenges, particularly in regulated sectors such as finance and critical infrastructure.
- Due to government mandates, specific industries remain bound by physical credential requirements, creating a hybrid environment.

Balancing demands

Enterprises must balance seamless, mobile-first access with privacy, cybersecurity and regulatory requirements. Done right, expanded identity and access solutions improve convenience and support a stronger, more resilient security posture.

Trend #6

Advancing detection technology with multisensory approaches

Security is rapidly evolving from a camera-centric system toward multisensory detection, leveraging a broader array of inputs to improve situational awareness.

Expanded toolkit

Audio analytics, smart sensors, chemical detection, thermal monitoring and drones are increasingly deployed to capture and contextualize security events. Smart sensors like **HALO** now offer downloadable updates and customizable modules such as air quality levels and system health statuses, expanding their utility over time.

Challenges ahead

While powerful, these technologies can be costly and difficult to integrate into legacy systems. Customers consistently stress the need for automation-ready platforms, to reduce false alarms and streamline responses. Providers who solve for advanced capability and ease of use will be best positioned to lead in this space.

Trend #7

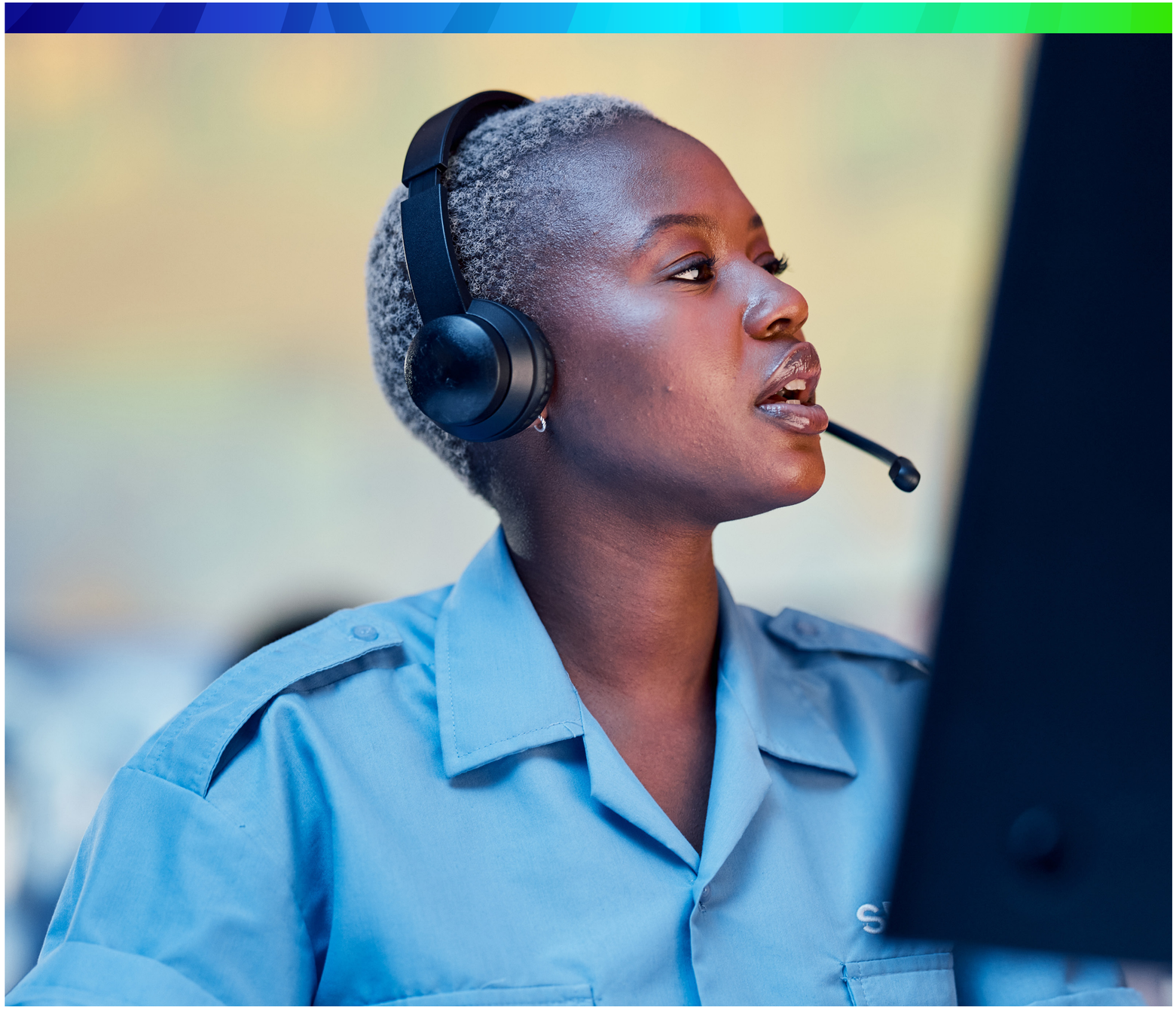
Driving efficiency and ROI with ESG as a strategic benefit

Organizations increasingly view security through the lens of efficiency and return on investment (ROI). Cost savings, operational resilience and performance optimization are the primary goals, and in achieving them, many initiatives also advance environmental, social and governance (ESG) objectives. What once was about compliance has shifted to a focus on measurable ROI, demonstrating how investments in security reduce costs, conserve resources and enhance reputations.

Shifting perspectives

- Optimized equipment lifecycles and reduced service calls deliver energy efficiency gains while lowering costs.
- Savings and performance improvements naturally align with sustainability goals, even when not the primary driver.
- Organizations are finding that efficiency-focused investments often have the added benefit of strengthening their ESG profile.
- Tools like the **OpenBlue Net Zero Advisor** help organizations quantify and validate these outcomes, tying security investments directly into measurable sustainability progress.

Forward-looking organizations see efficiency-driven security as essential to competitiveness with ESG impact as an additional advantage. Providers who can prove clear ROI will continue to earn trust and long-term investment.



Conclusion

The future of security is defined by integration, intelligence and impact. Providers and customers must embrace ROI-driven strategies that deliver safety, operational efficiency, better user experiences and support corporate responsibility efforts.

Johnson Controls is committed to helping organizations leverage these trends to build safer, smarter and more sustainable environments.

Visit **johnsoncontrols.com** or follow us **@johnsoncontrols**

Johnson Controls