Six Shifts in Security:
Where the industry is heading

The power behind **your mission**

Executive summary

Looking ahead to 2025, security is becoming exponentially more complex, yet the stakes have never been higher. To stay one step ahead of threats while juggling heavy workloads and budget limitations, security teams need more sophisticated, data-driven solutions and services that simplify management.

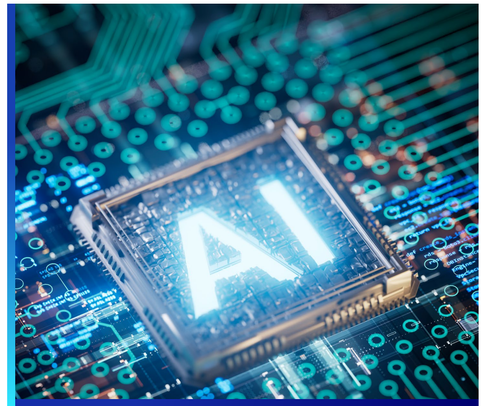
In its original 2021 report, Johnson Controls explored six of the main “shifts” transforming security, based on what was top-of-mind for security leaders at the time and the types of solutions they were seeking. These leaders noted shifts toward more robust data around building occupancy, more practical and easy-to-implement solutions, more seamless integrations, and others. However, the security landscape is dynamic, not static, and fruitful conversations with our customers in the field and via our advisory councils and regular listening sessions have since revealed how trends and customer priorities have changed over time.

Based on industry insights, here are the six latest shifts illustrating the continued evolution of the security landscape:

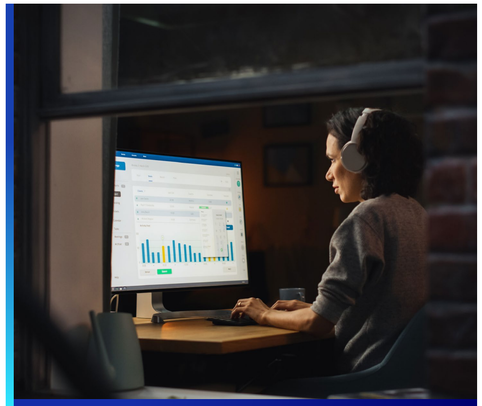
1 Advancing threat detection

2 Customizing asset protection

3 Automating for proactive and efficient service Delivery



4 Implementing analytics stategically



5 Securing remote access

6 Embracing holistic ESG

1

Advancing Threat Detection

Physical and cybersecurity threats are becoming more complex by the day. In fact, it seems like every news cycle brings headlines revealing threat actors' latest "wins." While many are sticking to the tried-and-true tactics they've relied on for years, such as phishing or ransomware in the cybersecurity realm or unauthorized access to spaces or assets on the physical security side, threat actors are also surprisingly agile – raising the stakes for security teams who are expected to be prepared for any number of scenarios.

In this evolving threat landscape, security leaders must progress from basic threat prevention to more proactive, sophisticated detection to stay ahead of diverse threats. As such, solutions that provide 360-degree visibility of assets, thereby eliminating blind spots in physical and cyber infrastructures, are essential to creating peace of mind. Having a comprehensive view of assets and leveraging advanced threat detection supports a quicker response time to incidents and can help resolve issues before they escalate.

It seems like every news cycle brings headlines revealing threat actors' latest "wins."

2

Customizing Asset Protection

The verdict from customers is in: one-size-fits-all security solutions no longer do the trick. Instead of standardized solutions, security teams are now seeking highly customized offerings that meet their unique needs. Different divisions within organizations often have different security vulnerabilities, so the most effective solutions on the market are those that can be tailored to address cross-departmental use cases.

However, solution providers should be careful not to introduce unnecessary complexity to products or services for the sake of customization. Just as we found in 2021, security teams still want solutions that are intuitive, scalable, and make their lives easier, not harder.

One-size-fits-all security solutions no longer do the trick.

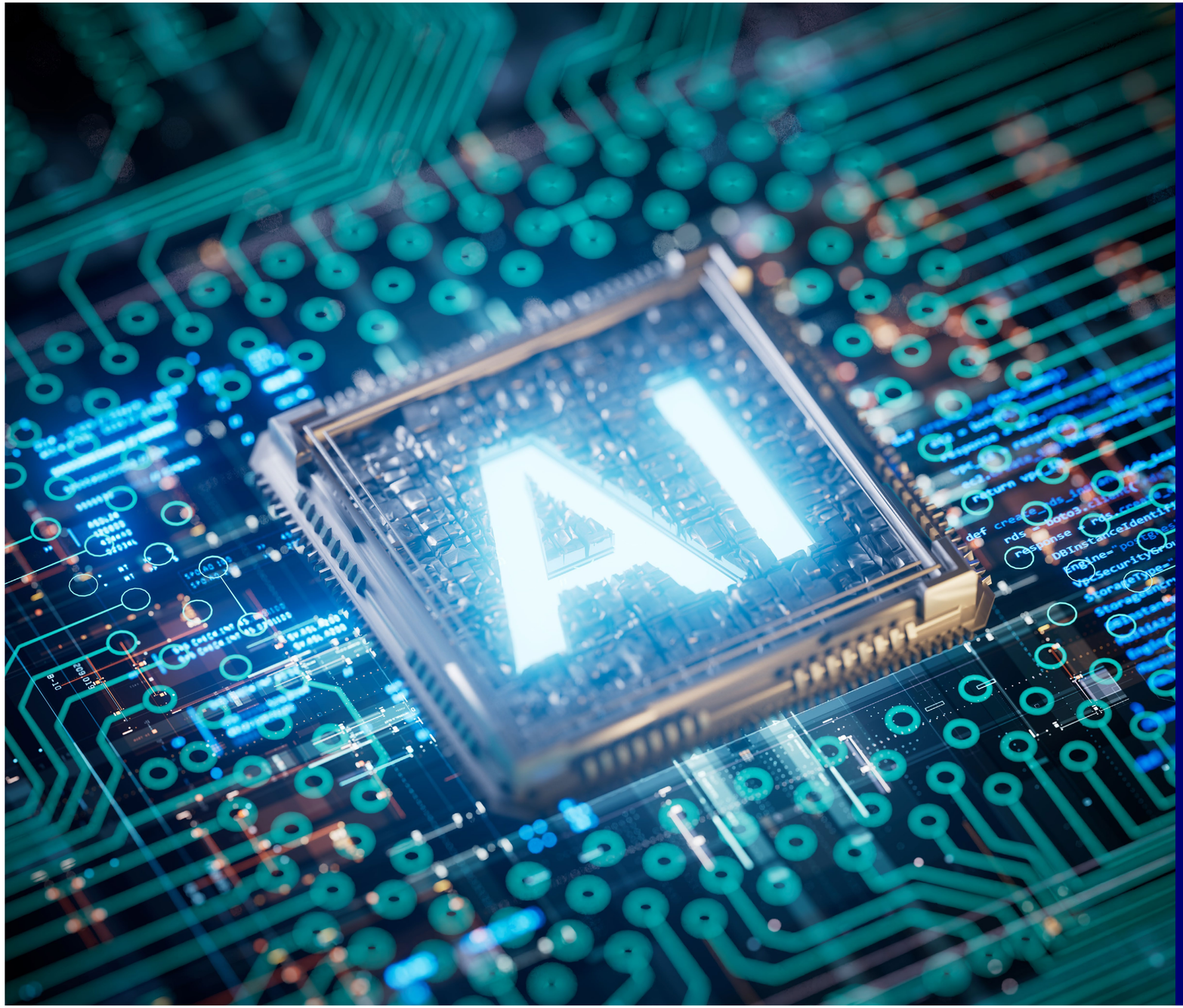
3

Automating for Proactive and Efficient Service Delivery

In recent years, security leaders have been focused on investing not only in security products, but also in problem-solving services. This movement has continued to gain steam, especially as modern security teams are stretched thin and looking for ways to maximize their time, money and resources. Service models are affordable and accessible options that allow teams to offload certain security functions and risks to solution providers.

Depending on their needs, customers can choose from a variety of security services like around-the-clock monitoring, managed technology and proactive maintenance, inspection and testing of security systems. Further, strides in automation are enhancing service delivery and helping to alleviate staffing challenges while improving efficiency. By taking on the brunt of menial tasks and helping to operationalize security processes, automated service can free up teams for more critical functions.

Service models are affordable and accessible.



4

Implementing analytics strategically

Data remains king in 2024, and AI is the key to unlocking more powerful insights from vast amounts of data. Over the past few years, AI has been squarely in the limelight, and we've seen huge leaps in AI innovation and adoption across sectors. This technology is continuing to be integrated into security solutions to enhance productivity, provide data-driven, predictive analytics and ultimately drive better business intelligence and decision-making. For instance, AI can augment a security team's ability to analyze video footage, prevent unauthorized access or detect faults in systems before they fail.

We've seen huge leaps in AI innovation and adoption across sectors.

5

Securing Remote Access

These days, the remote management of building systems is becoming the norm. Data collected from these systems can be analyzed remotely, allowing for the offsite monitoring, diagnostics, and servicing of these systems, including security infrastructure. With remote capabilities augmenting onsite staff and/or local technicians, organizations have truly comprehensive support and peace of mind that issues can be resolved from anywhere and anytime.

However, with more facilities being monitored and serviced remotely, there's increased scrutiny on cybersecurity and keeping these data exchanges and interactions secure. This illustrates one of the top cloud security challenges today: increasing innovation and productivity without sacrificing security. To promote secure remote access to connected assets in buildings, Johnson Controls acquired Tempered Networks in 2022 and leverages its zero trust Airwall technology to bring customers an additional layer of protection.

There's increased scrutiny on cybersecurity and keeping these data exchanges and interactions secure.

6

Embracing Holistic ESG

Prioritizing environmental, social, and governance (ESG) initiatives is valuable for today's organizations and building stakeholders in many ways. Not only does a strong ESG plan enable them to do their part to create a greener future, give back to people in their communities and manage their operations responsibly, but it's also good for business. Katie McGinty, vice president and chief sustainability and external relations officer at Johnson Controls, emphasizes that focusing on climate is completely in line with lean, strategic leadership.

While at first it may be difficult to see the tie between security and ESG, consider that strong security programs are critical for responsible corporate governance. Attacks on physical or cyber infrastructures can have devastating impacts on affected individuals, businesses and even society as a whole. When viewed through this lens, a strong security posture is necessary for organizations to increase their value, stay compliant with changing regulations and protect their bottom lines.

Attacks on physical or cyber infrastructures can have devastating impacts on affected individuals, businesses and even society.

In a world where security is no longer just a necessity but a critical component of responsible corporate governance, Johnson Controls is dedicated to providing the tools and expertise needed to protect what matters most—helping ensure our clients can focus on their core mission while we safeguard their people, assets, and reputation. Together, we are shaping the future of security, driving innovation, and creating a safer, more sustainable world.

Learn about how Johnson Controls complete building solutions and services support the evolving needs of commercial buildings, informed by direct customer feedback.

- **Security Lifecycle Management** with OpenBlue Services offers the ability to monitor and manage security devices across vendors, with remote support services and meaningful insights from skilled engineers.
- **Security Operations Centers** provide a suite of flexible bundled service packages to meet every facility's specific needs, delivered with complete onsite support or hybrid models.
- **Visual Alarm Verification** improves response times to critical alarms, reducing the risk of false alarms, and ensuring compliance with alarm verification regulations—all while providing cost savings and staff efficiencies.

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

Johnson Controls