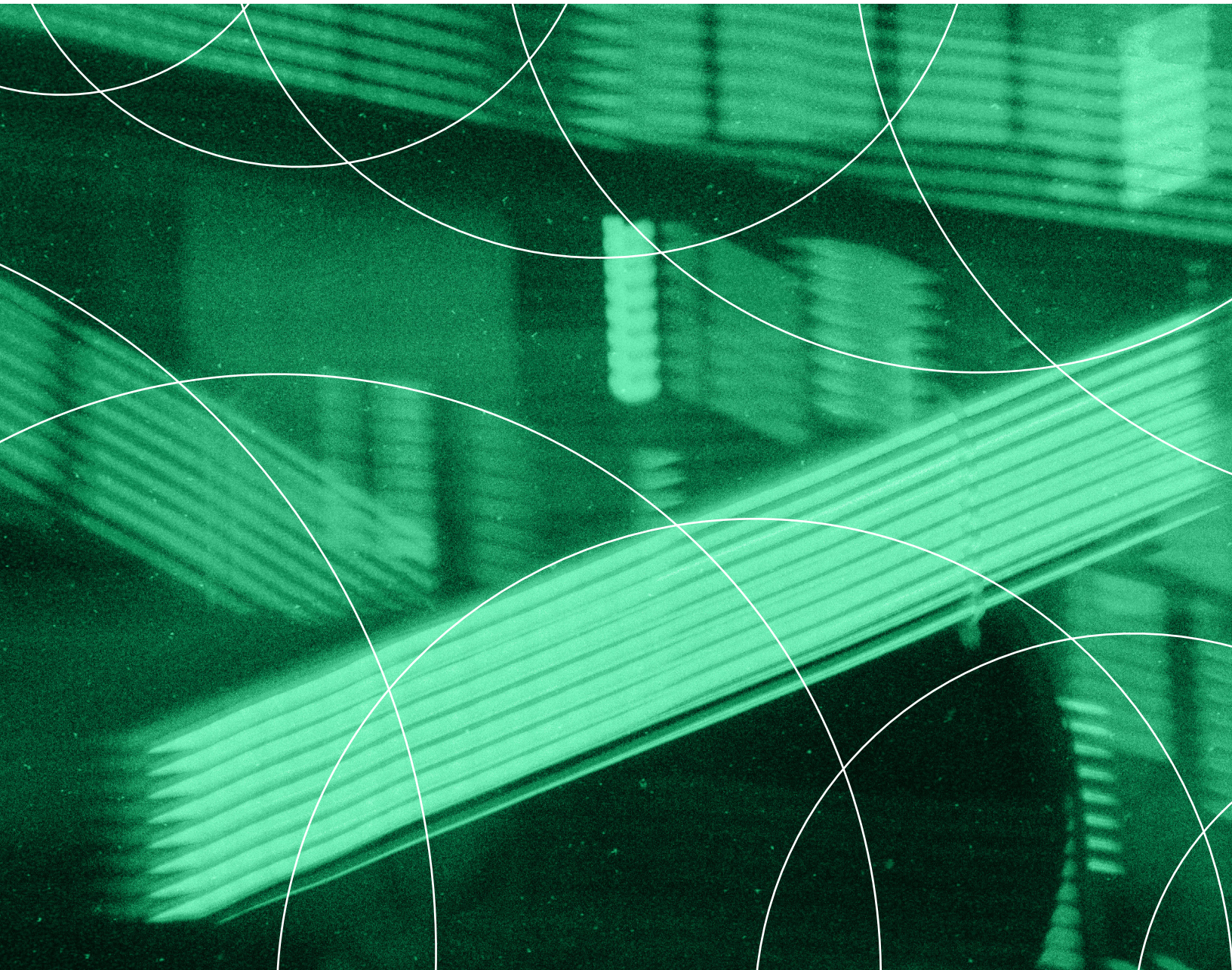
FORRESTER®

Sustainably Scale Security Operations With The Right Smart Buildings Partner

Security Leader Results From The November 2023 Thought Leadership Paper, “Cracking The Code: Unleash Your Smart Buildings Strategy With The Power Of Facility Data”

A FORRESTER CONSULTING THOUGHT LEADERSHIP PAPER COMMISSIONED BY JOHNSON CONTROLS, MARCH 2024

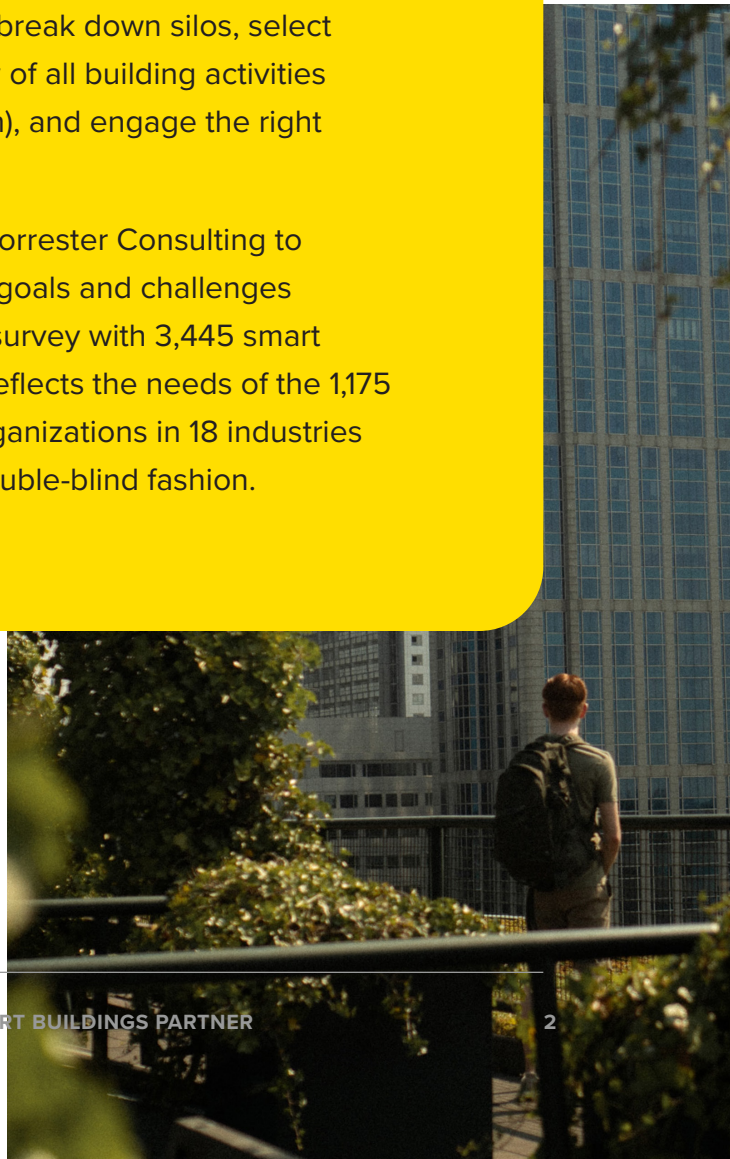


Executive Summary

Smart building technologies can enhance operational efficiencies and improve occupant experiences in enterprises across verticals. Smart building and facility management solutions monitor the design, construction, and operation of buildings, including lighting and HVAC systems. These environments revolutionize organizations that occupy any type of building, including government and commercial offices, financial services branches, and healthcare facilities. The most common use cases driving initial deployment focus on enhancing energy, space, operations, security, or environmental sustainability initiatives.

Despite the apparent benefits of deploying smart building technologies, organizations struggle to unlock the full value. This is largely due to the existence of organizational silos that impede collaboration, nonintegrated technologies that fail to provide a single centralized view of the environment, and a lack of technical skills to optimize systems. To unlock the full synergies of smart building technologies, organizations must break down silos, select technology platforms that offer a consolidated view of all building activities (from security to energy usage and space utilization), and engage the right external partners to manage ongoing operations.

In August 2023, Johnson Controls commissioned Forrester Consulting to evaluate the state of smart buildings, including the goals and challenges of security leaders. Forrester conducted an online survey with 3,445 smart buildings leaders to explore this topic. This report reflects the needs of the 1,175 security leaders surveyed. Leaders represented organizations in 18 industries and 25 countries. The study was conducted in a double-blind fashion.



Key Findings

Siloed teams and systems and a lack of technical skills prevent organizations from sustainably scaling and standardizing security operations. Improving sustainability and scaling/standardizing operations are security leaders' top goals. Yet, security and sustainability teams aren't collaborating today, and 57% of respondents note their security teams lack 24/7 visibility into all systems.

Advanced organizations rely on external partners to manage and scale operations. Security teams that have overcome challenges and have 24/7 visibility into all security systems rely on external partners to manage global security operations center (GSOC) operations.

Smart buildings partners and platforms give security leaders actionable insights to achieve their goals. Smart buildings require integration of all relevant building systems, and smart building features like motion sensors and smart lighting have both secure and sustainable implications. Security leaders seek to collaborate more closely with their sustainability cohorts and to find a smart buildings partner to provide one digital platform, providing security and sustainability teams with access to trusted insights and security teams with access to AI-driven recommendations to improve security operations.

Sustainably Scaling And Standardizing Security Operations Is The Top Priority

In addition to protecting their organizations' facilities, occupants, and assets, security's physical and cyberoperations have a key role to play in improving efficiencies and reducing an organization's carbon footprint. When exploring security respondents' top priorities, we found that:

- **Sustainability is a top organizational and security-level priority.** Sustainability remained a top-three organizational priority across similar studies that Johnson Controls commissioned from Forrester in 2021 and 2023. Furthermore, 57% of security respondents say finding ways to improve security operations while being sustainable is a top priority in the next 12 months.
- **Security leaders are focused on scaling and standardizing their GSOCs.** To operate more effectively and efficiently, respondents are focused on standardizing and streamlining operations. Top priorities include: improving the scalability of their GSOCs (64%); integrating standard operating procedures (SOPs) with their GSOCs (60%); and better integrating OEM security products, assets, and SOPs with security operations (52%) (see Figure 1). Existing Forrester research highlights the focus on and the importance of security operations; when comparing operations, oversight, GRC, and vendor risk and compliance priorities, global security and risk teams said that operations are their top focus.[1]

FIGURE 1

Importance Of Smart Buildings Partner Attributes

(Showing “Valuable” and “Extremely valuable”)

Base: 841 smart buildings decision-makers at the director level or higher for secure buildings at global enterprises that have a GSOC
Source: A commissioned study conducted by Forrester Consulting on behalf of Johnson Controls, August 2023

Siloed Teams And Systems Are Slowing Progress

While scalability and standardization of operations are the goals, this is not the reality today. Security teams struggle due to lack of collaboration, integration, and technical skills.

- **Sustainability is a security priority, but these teams don't talk today.** A significant gap remains with sustainability being a top organizational and security-level priority, and only 26% of security leaders say their organization collaborates with sustainability teams today. To ensure security teams are focused on the right improvements and enabling access to the right metrics/insights to track progress against sustainability goals, these teams must formally work together.
- **Teams need integrated SOCs and systems to better detect and respond to threats.** Cyberattacks are multidimensional, yet most security teams lack visibility into all those dimensions. Physical and cyber teams tend to report into different parts of the business, and 57% of our study respondents say their organization lacks 24/7 visibility into all security systems. Sixty-three percent also struggle to manage, verify the uptime, and maintain the health of their physical security systems. For many, this leads to issues getting information from all necessary systems, which prevents them from appropriately understanding and responding to facilities threats (see Figure 2). Insights are needed across both physical and cyber because attacks may target both systems (e.g., trying to disable cameras before breaking into a building, stealing/copying an employee's badge to enter a facility, and planting malware on a machine or using a USB drive to steal data off a system).
- **Lack of technical skills are a top security operations challenge.** In this commissioned study, 73% of security leaders say their organization lacks the technical skills to optimize

73%

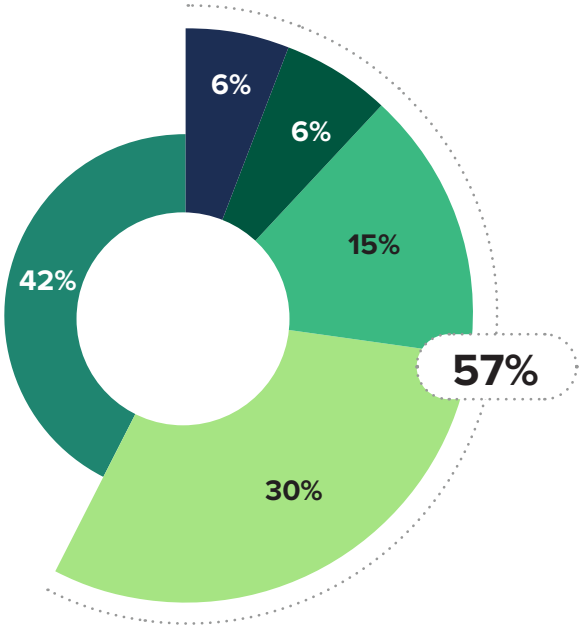
of security leaders say their organization lacks the technical skills to optimize building systems using insights it's collected.

building systems using insights they've collected. Exisiting Forrester research shows this is not only an organizational challenge, but it's also a top security challenge as well.[2] Our global benchmarking data validates that security teams are operations-focused and that technical skills are the most commonly identified skills gap among security teams.

FIGURE 2

Most Organizations Lack 24/7 Visibility Into All Security Systems

- The team does not have access to alerts/ monitoring from building systems
- The team has access during business hours to alerting/monitoring from most building systems, but not all
- The team has access during business hours to alerting/monitoring from all building systems
- The team has 24/7 access to alerting/monitoring from most building systems, but not all
- The team has 24/7 access to alerting/ monitoring from all building systems



65%
My organization often struggles with getting information from all necessary systems for full context of security threats.

63%
My organization's security teams struggle to understand the full context of threats/risks to facilities.

Base: 1,175 smart buildings decision-makers at the director level or higher for secure buildings at global enterprises
Note: Percentages may not total 100 because of rounding.
Source: A commissioned study conducted by Forrester Consulting on behalf of Johnson Controls, August 2023

Securing The Business Requires The Right Smart Buildings Partner

Smart buildings provide leaders with a clearer picture of what's going on inside organization-operated spaces, which helps them better manage, renovate, and create new spaces to be more efficient, sustainable, safe, and secure. For the purposes of this study, Forrester defines smart buildings as those that converge information from various connected systems in a facility (e.g., HVAC, lighting, security) to provide data-driven insights and measurable information that is shareable across multiple operational technology (OT) and IT systems. To overcome challenges and achieve their goals, we found that security leaders are engaging external partners to help manage and scale their organizations' operations. They want one smart building platform to improve access to insights and provide recommendations to inform decisions.

- **Smart buildings can help security teams improve operations in a sustainable way.** Moving forward, 49% of security leaders say their organization must collaborate more with sustainability, and 57% say they must find ways to improve security operations while being sustainable. Smart buildings can help them achieve this. For example, smart lighting and motions sensors can drive energy efficiencies while improving threat deterrence and detection. More broadly, physical security systems can provide insights like occupancy data; if organizations know where people are in a building, they can be more sustainable in their use of energy, power, and lighting in that building. Hitching onto enterprisewide objectives like smart buildings and sustainability can help security leaders get the funding and resources they need to protect their facilities and occupants.
- **Advanced organizations rely on partners to scale and sustainably improve their operations.** We looked at respondents whose organizations currently have 24/7 visibility into all their security systems and found that these leaders' organizations are more likely to have GSOCs in place. They also have a strong appetite to engage external partners to manage their operations. Given the importance of scaling

their security operations in a sustainable way, there is significant value in using external partners with strong security and sustainability expertise.

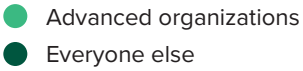
49%

of security leaders say using AI/ML to drive data-backed security ops decisions is a top GSOC priority.

- **These more advanced organizations that rely on partners have better visibility into systems and threats.** Integrated systems and the right partners help security leaders overcome their top challenges. Organizations that have 24/7 access to alerting and monitoring of all systems and rely on partners to manage their operations struggle less with accessing information to understand the full context of threats, responding appropriately to threats, and managing and verifying the uptime and system health of video surveillance and access control systems (see Figure 3).
- **Respondents want one smart buildings platform and the latest technology to achieve their organizations' security and sustainability goals.** Improving scalability, efficiency, and sustainability requires security leaders to have easy access to a unified view of operations. Seventy-four percent of security leaders want access to one digital platform for all sites and use cases, including security, health, and sustainability (see Figure 4). Their top requirement is that partners use the latest technology: Nearly half of respondents say that using AI/ML to drive data-backed security operations decisions is a top priority in the next 12 months.

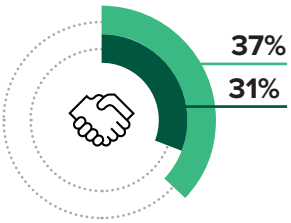
FIGURE 3

Advanced Organizations Rely On Partners And Have Better Visibility Into Systems And Threats

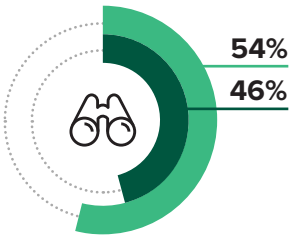


TOP PRIORITIES DURING THE NEXT 12 MONTHS

Finding a partner to manage all aspects of security operations



Finding a partner who can manage GSOC operations remotely 24/7, reducing staffing resources and costs



BUILDING SECURITY CHALLENGES

My organization often struggles with too many false positive security alerts which leads to misallocation of resources.

My organization often struggles with getting information from all necessary systems for full context of security threats.

My organization sometimes struggles to understand the proper response to facility threats/potential threats.

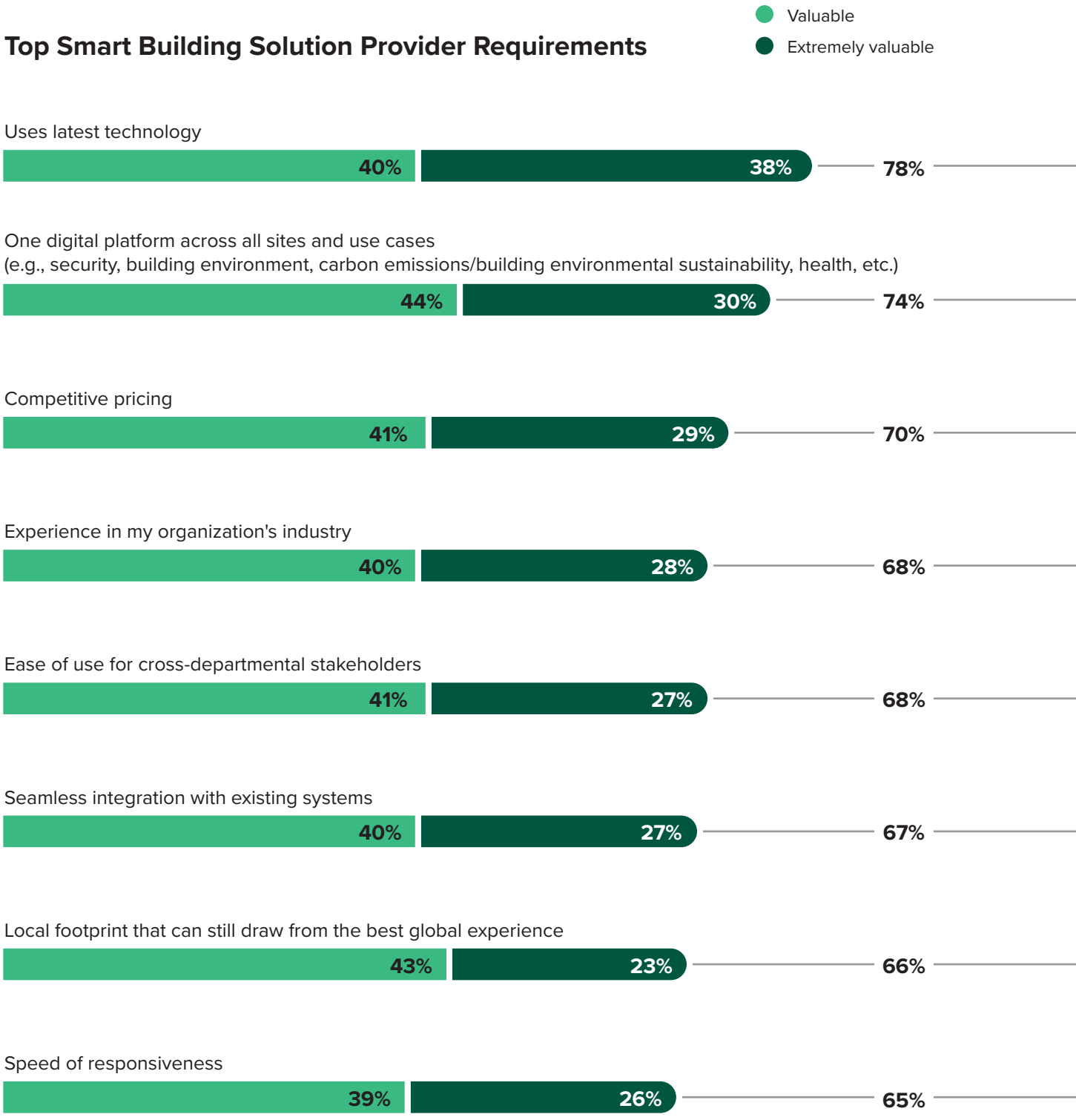
My organization sometimes struggles with managing, verifying the uptime, and system health of its video surveillance or access control systems.

My organization's security teams struggle to understand the full context of threats/risks to facilities.

Base: 1,175 smart buildings decision-makers at the director level or higher for secure buildings at global enterprises
Note: Forrester defines advanced organizations as those with 24/7 access to alerting/monitoring from all systems.
Source: A commissioned study conducted by Forrester Consulting on behalf of Johnson Controls, August 2023

FIGURE 4

Top Smart Building Solution Provider Requirements



Base: 1,175 smart buildings decision-makers at the director level or higher for secure buildings at global enterprises
Source: A commissioned study conducted by Forrester Consulting on behalf of Johnson Controls, August 2023

Key Recommendations

Security operations is one of the most critical elements of a successful security team. Detecting, investigating, and responding to attackers requires a complete picture of potential threats and the talent to address them accordingly. External partners have a role to play in both offsetting skills gaps and unifying data to provide security teams with more complete and actionable insights. As security teams are focused on scaling and improving operations in a sustainable way, there is value in engaging partners with security and sustainability expertise.

Forrester's in-depth survey of 1,175 global security leaders yielded several important recommendations:

Build your strategy for a GSOC now.

The benefits of a centralized GSOC are obvious, yet organizations still struggle to break down the organizational silos that prevent this. Security professionals shouldn't be deterred by institutional malaise or inertia; they should enlist appropriate senior leadership support and approval to help break down the existing barriers. Executive support should be accompanied by an articulated strategy for building a GSOC, including detailed budget and staffing requirements and other items such as defining and tracking the appropriate KPIs to measure performance. This maximizes chances for a successful GSOC deployment and ensures that your organization is best positioned to realize all the benefits of a GSOC.

Prioritize smart building platforms that can deliver a central consolidated view of all building activities.

The consequences of not having a centralized view across a building's key features (HVAC, lighting, security, etc.) are obvious. Response times are longer, and the potential for an incident to cascade and cause more business disruption is significant. For this reason, security professionals should focus

on only deploying smart building platforms that can integrate data from multiple disparate systems and deliver it via a single platform/pane of glass. Having one smart building platform improves access to insights and simplifies decision support to any type of building issue.

Hire and train the right type and number of staff for your GSOC.

One of security professionals' biggest challenges in adopting any new technology is that new tools demand employees with specific skills that can be hard to attract and retain. A successful smart building deployment requires people who know what processes to automate, how to manage operations, how to measure success, and how to establish process improvement practices to get the most value of these technologies. This may require retraining or cross-training existing personnel, hiring new people with specific skill sets, or relying on your smart building supplier to supplement your staff, but skills are an essential component to leverage the value of your GSOC.

Identify, define, and document common incident response procedures.

Smart building technologies generate lots of data about incidents, ranging from energy to security issues, so you'll need to speed up investigation and response. The challenge: Investigations can be time consuming, especially if staff has to work across multiple tools to assess an incident and initiate the proper response. Defining common incident response procedures in your smart building platform can improve efficiencies and employee experience while accelerating response times to incidents and minimizing impact.

Appendix A: Methodology

In this study, Forrester conducted an online survey of 1,175 security leaders responsible for building security and smart buildings strategy. Leaders represented organizations in 18 industries and 25 countries. Respondents were offered a small incentive as a thank you for time spent on the survey. The study was conducted in a double-blind fashion. The study began in July 2023 and was completed in August 2023.

To read the full results of the 2023 study, please refer to the Thought Leadership Paper commissioned by and developed in collaboration with Johnson Controls titled, "Cracking The Code: Unleash Your Smart Buildings Strategy With The Power Of Facility Data."

Project Team:
Mandy Polacek,
Senior Demand Generation Consultant

Ben Anderson,
Demand Generation Consultant

Contributing Research:
Forrester's Technology Architecture & Delivery and Security & Risk research groups

Appendix B: Demographics

ORGANIZATION SIZE	
2 to 499 employees	**1%**
500 to 999 employees	**41%**
1,000 to 4,999 employees	**43%**
5,000 to 19,999 employees	**11%**
20,000 or more employees	**4%**

BUILDING SECURITY SYSTEMS AND STRATEGY REMIT	
Influence decisions	**73%**
Final decision-maker	**27%**

TITLE	
C-level executive	**27%**
Vice president	**40%**
Director	**33%**

DEPARTMENT	
IT	**100%**

REGIONS	
North America	**30%**
Hong Kong	**7%**
United Kingdom and Ireland	**6%**
Middle East and Africa	**6%**
India	**6%**
Latin America	**6%**
South Korea	**5%**
China	**6%**
Southeast Asia	**6%**
Central Europe	**6%**
Singapore	**5%**
Australia and New Zealand	**5%**
Japan	**5%**

INDUSTRY	
Data center	**10%**
Healthcare	**9%**
Education	**9%**
Government	**9%**
Media and/or leisure	**6%**
Construction	**5%**
Agriculture, food, and/or beverage	**5%**
Transportation and logistics	**5%**
Travel and hospitality	**6%**
Business or professional services	**5%**

INDUSTRY (CONT.)	
Energy, utilities, and/or waste management	**5%**
CPG	**4%**
Electronics	**4%**
Retail	**4%**
Financial services and/or insurance	**4%**
Chemicals and/or metals	**4%**
Mixed use residential/ commercial real estate	**4%**
Manufacturing and materials	**4%**

Appendix C: Supplemental Material

RELATED FORRESTER RESEARCH

Best Practices For Automating Security Operations Workflows, Forrester Research, Inc., August 10, 2023.

IoT Solutions Transform Smart Buildings Into Strategic Productivity Assets, Forrester Research, Inc., August 2, 2021.

Appendix D: Endnotes

[1] Source: 2023 Security Operations Benchmarks, Global, Forrester Research, Inc., August 4, 2023.

[2] Ibid.

ABOUT FORRESTER CONSULTING

Forrester provides independent and objective research-based consulting to help leaders deliver key outcomes. Fueled by our customer-obsessed research, Forrester's seasoned consultants partner with leaders to execute their specific priorities using a unique engagement model that ensures lasting impact. For more information, visit forrester.com/consulting.