



2025 Trends in Access Controllers Report

How Modern Challenges Are
Influencing Technology Innovation



Table of Contents:

Introduction	3
The Relationship Between Physical Access Control and Controllers	4
Key Functions of Controller Hardware	5
Top Priorities for Controller Selection	6
Mobile and Cloud Adoption for Controllers	9
Cybersecurity Considerations	11
Trends in Controller Selection, Sourcing and Specifications	14
The Future of Access Control	19

Introduction

Advances in cybersecurity, edge computing and Internet of Things (IoT) are helping to make access controllers more secure, intelligent and versatile. This report explores key trends driving controller technology evolution and highlights how they influence today’s security landscape.

In 2024, Mercury surveyed more than 450 individuals in Europe and North America on these trends to understand their role in shaping the controller market and the broader access control challenges the industry faces. In this report, we describe key findings and their implications for the future of access control.

About the Respondents

Respondents represent three main categories:

- Administrators (50%): Responsible for overall management of access control systems, including configuration, setting policies and maintaining security.
- End users (23%): Handle daily operations like monitoring access and generating reports.
- Partners (27%): System integrators, installers, consultants or original equipment manufacturers (OEMs).

The industries most heavily represented included higher education (17%); health care (15%); local, state and federal government (13%); banking, insurance and finance (10%); and K-12 education (7%).



The Relationship Between Physical Access Control and Controllers

In a physical access control system (PACS), controllers enforce policies that restrict who can enter specific areas based on access permissions or privileges. Controllers connect to access control readers to identify users via methods such as prox and smart cards (badges), biometric scans and mobile identities.

Controllers have evolved from performing basic authorization functions to providing a range of related capabilities, making the choice of controller platform more significant than ever for security leaders as they build out their PACS strategies.

According to our survey, 72% of respondents identified the controller as a critical or important factor when designing their physical access control system, emphasizing the controller's central role in determining who can and cannot enter secure areas. A further 16% considered it moderately important, recognizing controllers' contribution to a facility's overall security when used with other security measures.

“ 72% of respondents identified the controller as a critical or important factor when designing their physical access control system. ”



Key Functions of Controller Hardware

As a critical component of a security infrastructure, controllers can offer a range of essential features that make them integral to any organization’s security strategy.

These features collectively make physical access controllers a fundamental component in maintaining a secure, efficient and adaptable security environment.



Authorization

Controllers decide what authenticated users can do at access points, using predefined permissions and factors like time, location or temporary rules.

Integration

Controllers connect with devices like card readers and locks, controlling access and alerting security to unauthorized attempts. Modern designs also link easily with cameras and alarms for added security.

Edge Computing

Edge-enabled controllers handle access decisions and credential checks locally, reducing reliance on central systems and improving speed during outages or high traffic.

Data Management

Controllers log access events with timestamps and user data, offering reliable records for security monitoring and compliance.

Scalability

Modular controllers support growth, allowing facilities to add devices and manage access across multiple sites through central software.

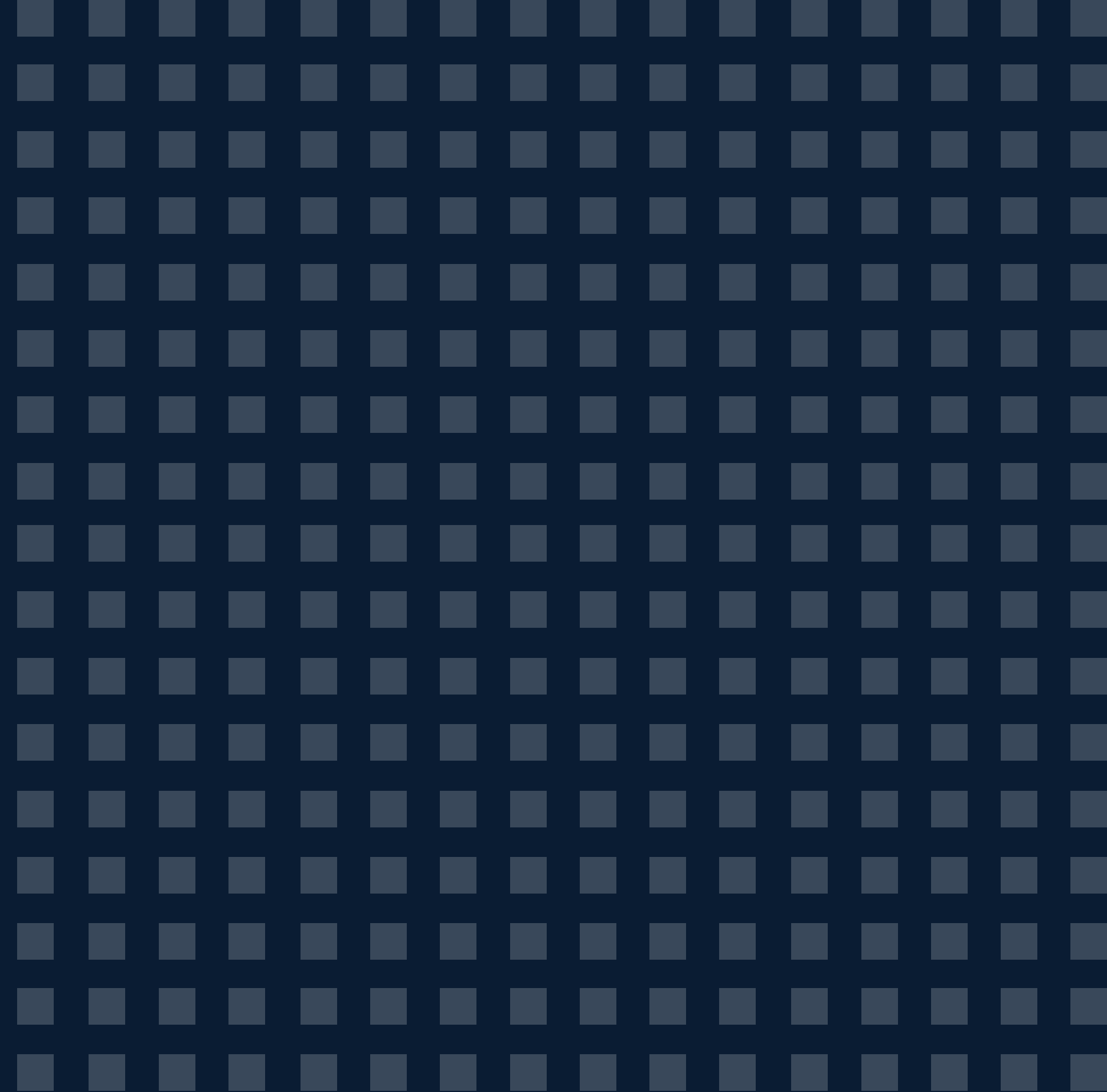
Interoperability

Controllers work with devices from different brands by supporting open standards, ensuring adaptability to new technologies and changing needs.

Cybersecurity

Built-in encryption, authentication and tamper protection secure data and maintain system integrity.

Top Priorities for Controller Selection



Modern controllers offer increasingly extensive feature sets. However, our survey showed that foundational aspects remain central to purchase decisions.

Respondents identified their three top priorities when selecting a physical access controller as:



Together, these factors ensure that access control systems can operate efficiently, securely and within budget, addressing the most pressing needs of modern organizations.

Additional priorities, in order of importance, included:

- **User-friendly management interface (28%)**
- **Compatibility with a variety of access credentials (25%)**
- **Configurability (23%)**
- **Physical durability and tamper resistance (23%)**

However, when asked about their current controllers, the features reported as “not” available in their current systems included a user-friendly management interface (24%), cloud enablement (23%), interoperability with other security systems (21%) and cybersecurity (21%).

This indicates a potential disconnect between the decision-maker’s preferences and how their current controllers perform against those expectations. It can also indicate a lack of knowledge regarding the capabilities or features of modern controllers, as many of these features may be missed due to a lack of knowledge or insufficient training about existing hardware. As a result, this can shape how individuals and organizations approach future technology investments.

What Impacts Controller Specifications

As security leaders continue to identify the ideal mix of features necessary to meet the security goals of the organization, implications to the broader business must be considered. According to respondents, selecting the right controller for an organization comes down to several factors.

These factors reflect the growing complexity of modern security infrastructures and the need for access control systems to evolve alongside broader technological and business shifts. As organizations prioritize cybersecurity and data protection, it's clear that staying ahead of regulatory requirements is a critical factor in selecting the right controller. Compatibility and interoperability are also key, as businesses rely on a mix of systems and devices that must work seamlessly together now and in the future. The increasing adoption of mobile solutions, cloud-enabled systems and edge computing highlights a shift toward more flexible, scalable and real-time solutions that can adapt to the changing needs of the workforce and the organization.



Cybersecurity

When asked if they try to stay current with evolving cybersecurity and data protection standards and regulations, an overwhelming majority (90%) said yes.



Backward/Forward Compatibility

A total of 86% of respondents said backward and forward compatibility is important for their organization's future security infrastructure plans.



Interoperability

76% of respondents said interoperability is important because their organization uses a wide range of devices and systems.



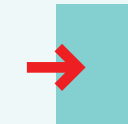
Mobile

More than half (57%) said they use or plan to use mobile solutions.



Cloud

Over half (52%) said their controllers are cloud-enabled for improved scalability, centralized management, real-time monitoring and easier software updates.



Building Occupancy

Approximately 53% reported integrating building occupancy and utilization with their controller configuration.



Edge Computing

44% of respondents are exploring or have adopted edge computing in their security ecosystem.

Mobile and Cloud Adoption for Controllers



Cloud adoption in physical security refers to the growing trend of organizations moving their physical security systems, such as video surveillance, access control and alarm monitoring, to cloud-based platforms, allowing for remote access, centralized management and improved scalability compared to traditional on-premises systems. Even before the COVID-19 pandemic made it crucial for many organizations to adopt strategies for digital transformation, cloud adoption was on the rise as physical and logical access control moved into the space.

For cloud-enabled controllers, the rise in adoption rates indicates a greater reliance on networked and remotely managed options that provide more flexibility and connectivity across the enterprise. In fact, 50% of respondents reported that cloud connectivity was one of the most important trends influencing their decision-making when purchasing controllers.

The reasons included improved scalability, centralized management, real-time monitoring and easier software updates, advantages long reported by early adopters of cloud technology. Access credentials stored on mobile devices are also gaining traction. Such devices are now ubiquitous.

Many people, particularly those of younger generations, use them for critical tasks like payment transactions and travel documentation. Empowering users to keep access credentials on mobile devices is a logical step for organizations seeking seamless and enhanced access control.

Mobile credentials streamline security processes and enhance user experience while providing the robust security features associated with cloud-based solutions. 55% of respondents identified the importance of controllers' compatibility with various credentials, including mobile credentials, as part of their selection process.



Cybersecurity Considerations



The growing reliance on networked access control systems means that cybersecurity becomes an essential feature of a controller and its related parts, including access readers and central servers. Communication among these components provides a broader vulnerability without proper protections in place. A breach in these systems can have detrimental consequences, compromising physical security and the integrity of an organization's IT infrastructure.

As previously mentioned, 33% of respondents named cybersecurity features as one of their top three requirements when selecting a controller, while 21% said their current controllers are missing this critical component.

Many organizations use a broad system of networked devices that can — without the proper protocols — provide a larger attack surface that weakens an organization's whole infrastructure. A vulnerability in controllers could be exploited to target the organization more broadly, meaning proper configuration, stringent permissions and ongoing software updates and bug fixes become critical. This increasing convergence between IT and physical security makes it essential for security leaders to prioritize cybersecurity to protect the organization from cyberattacks.



Meeting Compliance and Regulatory Requirements

Meeting compliance and regulatory requirements requires robust cybersecurity to protect critical data, especially for health care, finance and government entities subject to GDPR, HIPAA or PCI DSS regulations. This requires strong security measures to safeguard physical and digital access to sensitive information. A breach through a single solution, such as a controller, can put an organization out of compliance, potentially resulting in fines, legal consequences and reputational damage.

“ More than 71% of respondents said advanced cybersecurity — hardware-based protections such as ARM TrustZone, OSDP (Open Supervised Device Protocol), secure boot CPU and the use of the latest cryptographic techniques — is one of the most important current trends influencing their decision-making around purchasing controllers. ”

For these reasons, 90% of respondents reported that their organizations try to stay connected with evolving cybersecurity and data protection standards and regulations. More than 71% of respondents said advanced cybersecurity — hardware-based protections such as ARM TrustZone, OSDP (Open Supervised Device Protocol), secure boot CPU and the use of the latest cryptographic techniques — is one of the most important current trends influencing their decision-making around purchasing controllers.

Controller vendors must prioritize robust security practices to ensure reliability and compliance. This includes actively analyzing and patching common vulnerabilities and exposures (CVEs), performing static code analysis and threat modeling and providing a clear software bill of materials (SBOM). By following a strict, secure software development process, vendors help organizations maintain a transparent software supply chain while meeting global standards and regulatory expectations.

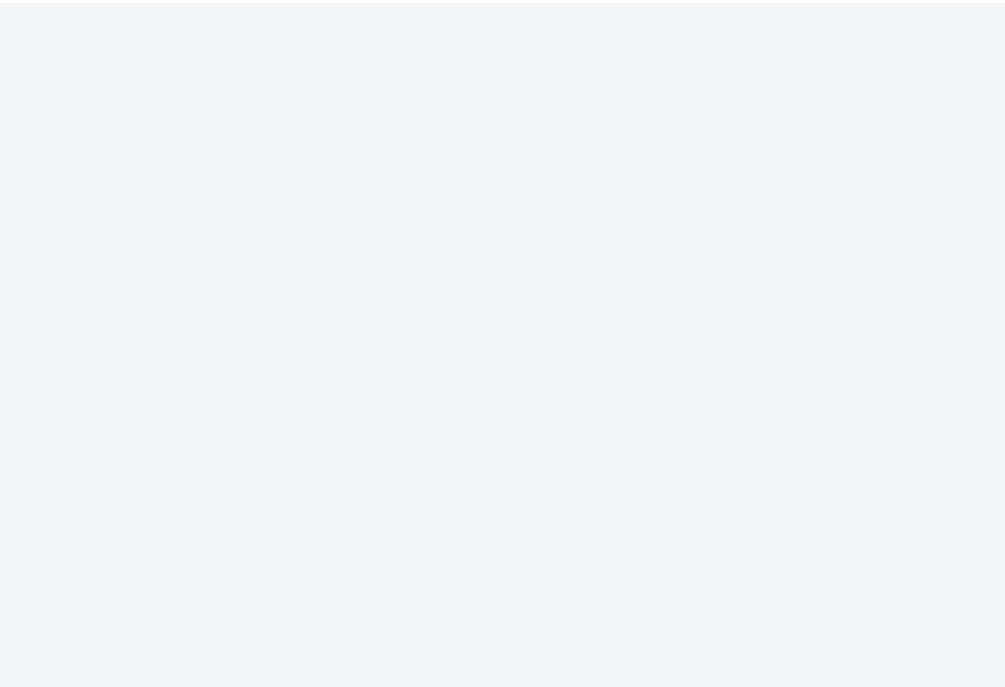
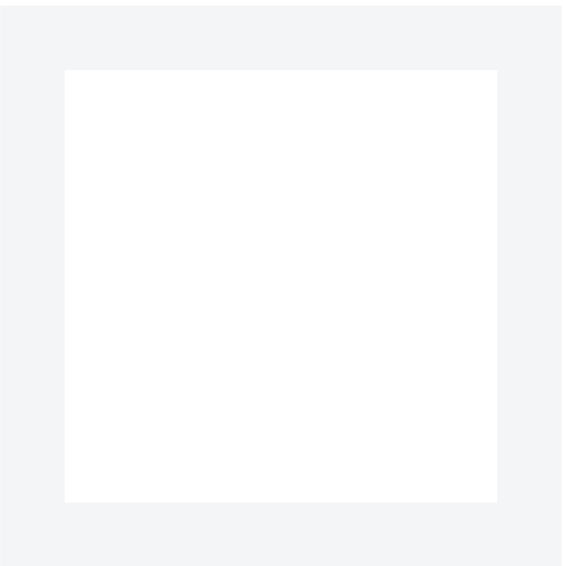
How Edge Processing and IoT Are Transforming Access Control

As organizations adapt to evolving security demands, edge processing and IoT offer immediate, impactful benefits that align closely with current industry priorities. Edge processing enables localized decision-making at the access point, allowing controllers to process access requests and verify credentials directly. This reduces dependency on centralized systems, improves response times and ensures continuity during network disruptions.

With nearly 44% of survey respondents exploring or adopting edge computing, this trend reflects the growing need for fast, reliable, decentralized security solutions. Smart door controllers and IP-based access readers exemplify how edge devices transform access control by minimizing latency and enhancing scalability.

IoT integration is another driver of innovation, with 37% of respondents identifying it as a top trend. By enabling controllers to interact with systems like HVAC, lighting and occupancy sensors, IoT fosters intelligent building management and adds value beyond traditional access control. These capabilities optimize energy efficiency, improve building utilization and provide actionable insights, making IoT a critical component of future-ready security ecosystems.

Security leaders can use these advancements to build scalable, interoperable systems that improve efficiency, reduce operational costs and meet the demands of modern infrastructures. By emphasizing edge and IoT, organizations can position themselves for success today while laying the groundwork for future innovations.



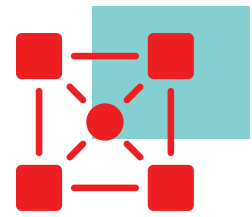


Trends in Controller Selection, Sourcing and Specifications



The broader trends regarding controller selection, sourcing and specifications tell the story about the importance of technology innovation, a more significant focus on interoperability and the need for secure hardware options.

Taking a closer look, the data highlight multiple areas where manufacturers should spend time and resources developing technology to meet these criteria to help organizations achieve their goals.



Compatibility and Interoperability

Respondents emphasized the importance of controllers that work seamlessly with other elements of their security ecosystems.

In fact, 76% said interoperability is important because their organizations rely on a wide range of devices and systems. A further 86% said backward and forward compatibility is critical for device selection and infrastructure planning.

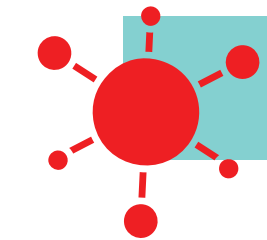
This focus on backward and forward compatibility underscores the importance of delivering products that maintain form, fit and function (FFF) while being future ready. Respondents' emphasis on compatibility suggests a strong preference for solutions that minimize large up-front capital expenditures by allowing for gradual system upgrades. A phased approach, such as a multi-year migration plan, enables organizations to modernize their infrastructure while maintaining operational continuity. This aligns with the desire for scalable solutions that adapt to evolving security needs without requiring complete overhauls, ensuring long-term value and investment protection.



Power Over Ethernet

Power over Ethernet (PoE) allows devices to receive power and data through a single Ethernet cable, reducing the cabling required and simplifying the installation process.

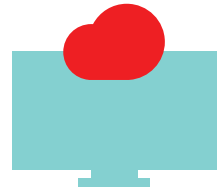
When asked about specific use cases, respondents stated that IP cameras had the potential to impact physical access control the most, with 79% of respondents choosing that option. This was followed by PoE door controllers (69%) and PoE readers (66%).



Expanding Uses for Access Data

Data unlock new ways to add value to the organization. Decision-makers seeking this capability can choose controllers designed for data-driven decision-making. Approximately 53% of respondents have integrated building occupancy and utilization with their controller configurations to provide the organization with more insights to make better decisions.

For 37%, IoT integration — connecting access control with other intelligent systems like lighting, HVAC and occupancy sensors — is a key trend influencing buying decisions, enabling more cohesive and efficient building management.



The Impact of Edge Devices

Edge devices are physical devices or networked endpoints deployed on-premises (the “edge” of the network) capable of processing data and making decisions locally without continuous connectivity to a centralized server or the cloud. In physical security, edge devices can reduce latency and bandwidth usage while speeding up responsiveness.

As edge devices are adopted in physical security, end users predict IP cameras with access control features (68%), smart door controllers (63%) and IP-based access control readers (49%) will have the most impact on physical access control.



Cloud Enablement

Organizations increasingly recognize the advantages of cloud-based access control technology, with 50% of respondents citing cloud connectivity as a key factor influencing their controller purchasing decisions.

Benefits such as improved scalability, centralized management, real-time monitoring and easier software updates are driving this shift, as reported by early adopters. Cloud adoption and enablement are part of the growing trend of shifting systems such as video surveillance, access control and alarm monitoring to cloud-based platforms, enabling remote access, centralized management and better scalability.



Cybersecurity-First Adoption

While respondents indicate that keeping up with cybersecurity best practices is important, many systems are perceived to lack critical protections that can keep organizations safe from external threats.

Networked access control systems enhance efficiency and integration by connecting controllers, readers and central servers. However, this interconnectedness can introduce potential security gaps. As IT and physical security merge, organizations should focus on cybersecurity by implementing proper configurations, enforcing strict permissions and applying regular software updates to maintain robust protection.

The Potential of AI

While still emerging, AI-enabled systems have the potential to enhance security operations, aligning with overall trends toward intelligent, adaptive and efficient control systems. Organizations seeking to stay ahead of emerging technology can choose modern controllers with built-in application environments. This offers the flexibility to adopt new solutions without replacing hardware and adapt as the future of AI in access control unfolds.

Respondents cited the following as the most impactful use cases for AI:



Video surveillance integration

56%



Facial recognition and biometric authentication

54%



Predictive security and threat prevention

46%



Behavioral analysis and anomaly detection

44%

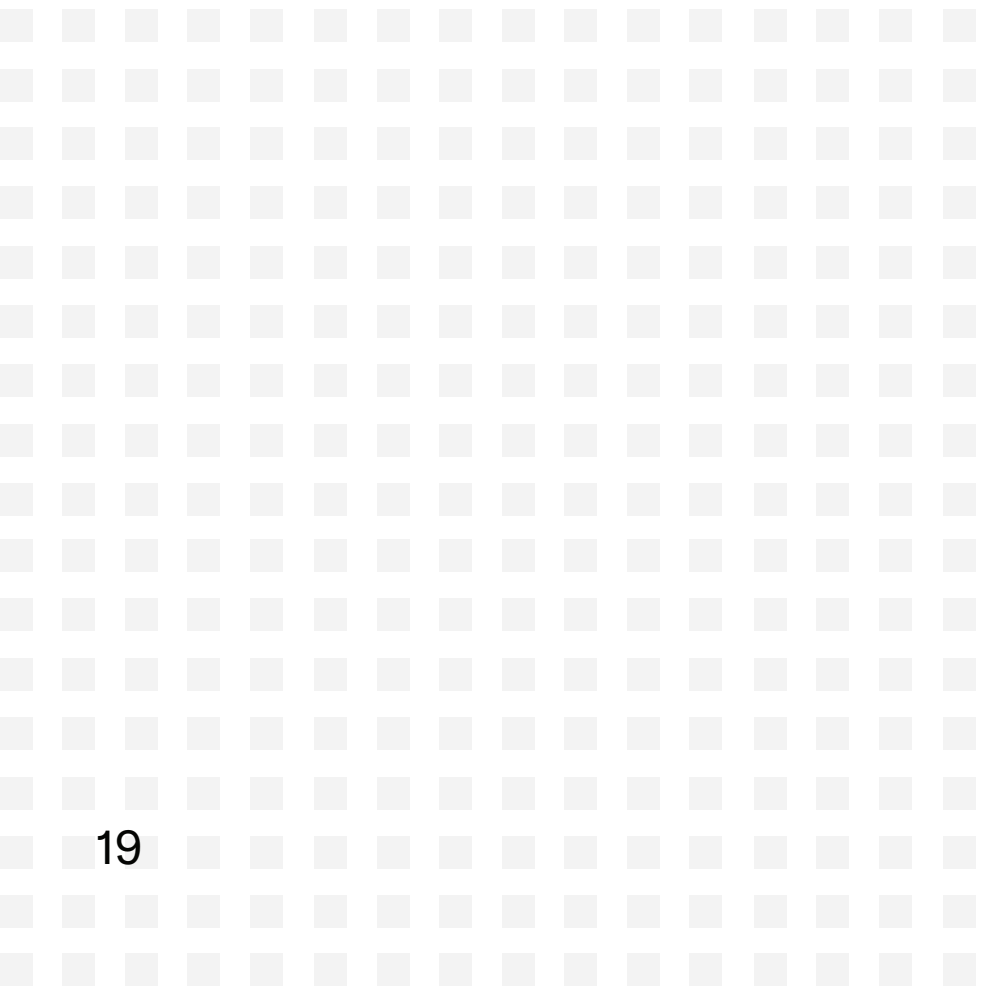
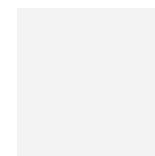
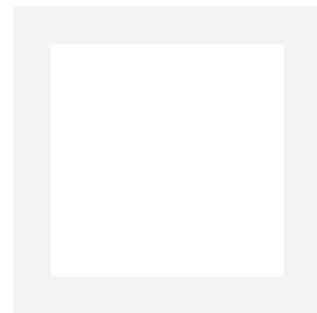


System efficiency improvements

31%

The Future of Access Control

Physical access control systems are evolving to meet modern challenges, with technology innovation driven by trends in mobile and cloud adoption, cybersecurity and AI integration. The growing reliance on networked devices and cloud-based solutions has highlighted the importance of scalability, centralized management and cybersecurity, with security leaders increasingly prioritizing these factors when selecting controllers. As the market shifts toward more intelligent, interoperable and secure systems, these advancements will shape the future of access control and enable more efficient, scalable and resilient security infrastructures across industries.





Mercury Security

11165 Knott Avenue, Suite AB

Cypress, CA 90630

mercury-security.com

Part of 

© 2025 HID Global Corporation, part of ASSA ABLOY. All trademarks are owned by HID Global Corporation, ASSA ABLOY and/or their respective owners and may not be used without permission. All rights reserved.