brivo® SIW SECURITY INFOWATCH.COM

State of the Market: Access Control Systems

The increasing preference for cloud-based solutions is evident in our year-over-year surveys, as security professionals acknowledge the need for adaptable solutions to address the evolving demands of physical space management. Our survey regarding the current state of physical access control systems reveals that it’s critical to distinguish between typical premise-based access control systems, legacy software hosted on cloud servers and deployments whose every component has been purpose-built to constitute a highly secure cloud-based access control platform.

Content

Executive Summary

The rise in cloud-based access control adoption mirrors the broader trend of business cloud adoption. Today, the cloud is a crucial backbone for many U.S. companies.[1]

- 94% of enterprises use cloud services.
- 67% of enterprise infrastructure is now cloud-based.
- 92% of businesses have a multi-cloud strategy in place or in the works. The
- average enterprise uses 1,295 cloud services.
- The average employee uses 36 cloud-based services every day.

Accenture reports that 94% of businesses are undertaking digital transformation initiatives.[2] Today's business environment is predominantly cloud-friendly. Transitioning from on-premises physical security systems to contemporary cloud-based technology aligns with the digital objectives of most businesses, especially when the upgrade incorporates support for mobile users and data integration capabilities beneficial to both security and business operations.[3] Hence, the shift to cloud-based access control is no longer an uphill battle.

Security professionals increasingly report enhanced overall security through the adoption of cloud-based access control.[4] Our survey indicates:

- 28% of end users anticipate significant upgrades or expansions of their electronic physical access control systems soon.
- Over half of the respondents expect to transition to cloud-based access control within the next five years, as per the following breakdown:
  - Short-term (0-12 months): 14%
  - Medium-term (1-2 years): 16%
  - Long-term (3-5 years): 21%

Budget and ROI are the biggest obstacles to upgrading existing access control to modern technology. Still, these challenges can be addressed by understanding the significant return on investment available from a true cloud access control system.

End users have highlighted challenges with current access control systems and express two primary expectations for access control modernization:

- 74% anticipate time efficiency improvements of up to 30% following an upgrade.
- 82% expect cost savings of up to 40% after system modernization.

However, they also have genuine concerns about migrating to cloud-based access control, which is valid given that all cloud access control systems are not alike. To make informed decisions, it's essential to evaluate available cloud access solutions based on four core factors:

- Addressing current access control system pain points
- Overcoming upgrade-related challenges
- Ensuring a cybersecure access control system deployment
- Achieving a satisfactory ROI

This report delves into these concerns, comparing the capabilities of true cloud-based access control systems against premise-based and legacy cloud- hosted systems, facilitating an organization-specific business case for a cloud- based access control upgrade.

[1] Zippia. "25 Amazing Cloud Adoption Statistics [2023]: Cloud Migration, Computing, And More" Zippia.com. Jun. 22, 2023, https://www.zippia.com/advice/cloud-adoption-statistics/
[2] Accenture. "Total Enterprise Reinvention | Infographic" Accenture.com. May 10, 2023. https://www.accenture.com/content/dam/accenture/final/capabilities/strategy-and-consulting/strategy/document/Accenture-Total-Enterprise-Reinvention-Infographic.pdf
[3] Brivo. "2023 Top Security Trends" Brivo.com. Feb. 10, 2023, brivo-trends-report-2023.pdf. https://www.brivo.com/security-trends/
[4] Ibid.

PHYSICAL ACCESS CONTROL EVOLUTION

The commercial physical access control industry initially began with simple electric door strikes and wired push-button manual door controls. Today, after 60 years and numerous product evolutions, physical access control systems are no longer standalone. They have morphed into expansive computer-based networks that employ a mix of centralized control panels, electronic credentials, credential readers, electronically controlled door locks, software and an intricate communication infrastructure. Although the primary objective remains to ensure authorized access based on specific privileges, the contexts surrounding these systems have radically changed.

Access control systems were traditionally device-centric for about 50 years. Now, they are also data-centric, deriving their value from data generation, system integration, and their capacity to ensure convenience while upholding privacy and robust cybersecurity standards.

THE CURRENT ACCESS CONTROL DEPLOYMENT LANDSCAPE

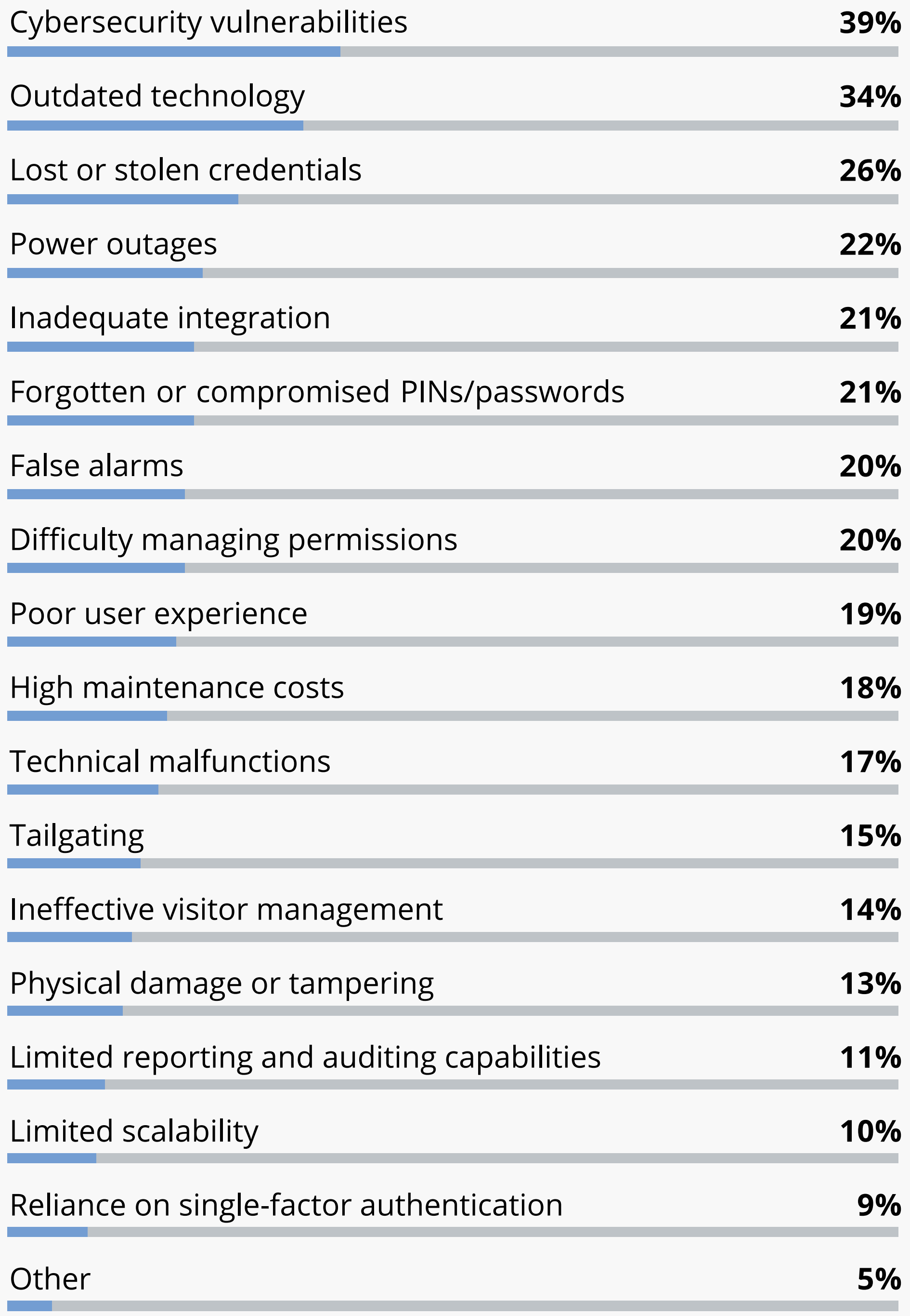
Many of today's access control systems are a mix of technologies from various manufacturers spanning different product generations. This variety is often due to incremental growth over time, further complicated by business mergers or acquisitions. Products generally have a lifespan of 10 to 20 years; even if they function as intended, they may no longer deliver the needed value.

End users cite cybersecurity vulnerabilities and outdated technology as their primary concerns (see Figure 1 below). The top six pain points/challenges, except for power outages, can be addressed by a well-engineered modern cloud access control system. Today's employees and visitors prefer using digital credentials on their smartphones over an access card and using the phone's biometrics and/or Apple or Google Wallet for multi-factor authentication.

A mature cloud access control platform will have an application programmer's interface (API) and existing seamless integrations with various systems such as HR, workplace experience, identity management, property management, elevator control, video surveillance, computer vision, intercoms, biometrics, club membership, visitor management, and time and attendance, among others. Certified partners will provide custom API integrations to their customers.

FIGURE 1. CHALLENGES REGARDING EXISTING PHYSICAL ACCESS CONTROL SYSTEMS

What pain points or challenges do you currently face with your access control systems that you would like to address or improve? (Please select all that apply.)



CHANGING BUSINESS TRENDS AND FACILITY TECHNOLOGY LANDSCAPES

Evolving workforce demographics and the impact of global events like the COVID-19 pandemic have reshaped workplace expectations. Workers no longer expect to be always on-site, working in assigned spaces. They prefer flexible hours, hybrid environments (two or more different work settings including home), multiple accommodations and more conveniences, including convenient facility access via smartphone.

For numerous organizations, these elements have added layers of complexity to the management of access control permissions. For some, managing these privileges has become impractical due to the heightened demands on staff time. There's an emerging inclination to grant broader area access and endorse 24/7 access rights, which deviates from the foundational "least privilege" access control philosophy.

There is also rising awareness and concern about cloneable access cards. Numerous supermarkets and pharmacies presently feature kiosks capable of replicating mechanical keys and access cards. Notably, one kiosk provider has highlighted its deployment of over 4,000 such units throughout the U.S.

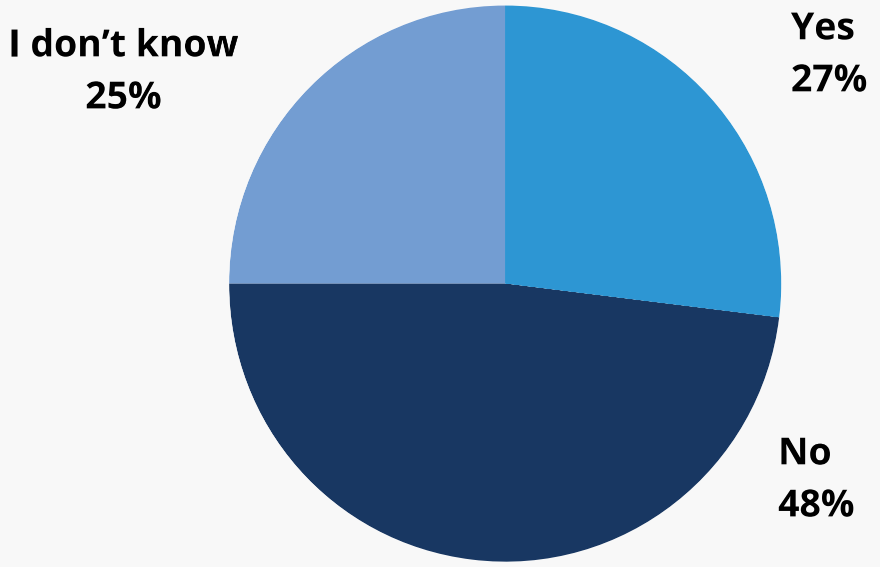
The ease and flexibility of issuing and revoking mobile device access credentials alleviates the administrative strain and eliminates the complexities and costs of card and key fob management. This is one reason there's a mounting interest in modernizing access control systems.

ACCESS CONTROL UPGRADE PLANNING

While some access control systems meet current organizational needs, Figure 2 below shows that 27% of survey respondents plan substantial physical access control upgrades or expansions soon. Those who do not indicate it is because their current system satisfies all their needs. Others report they do not plan to upgrade due to funding considerations, uncertainty about workplace real estate plans, or upcoming changes.

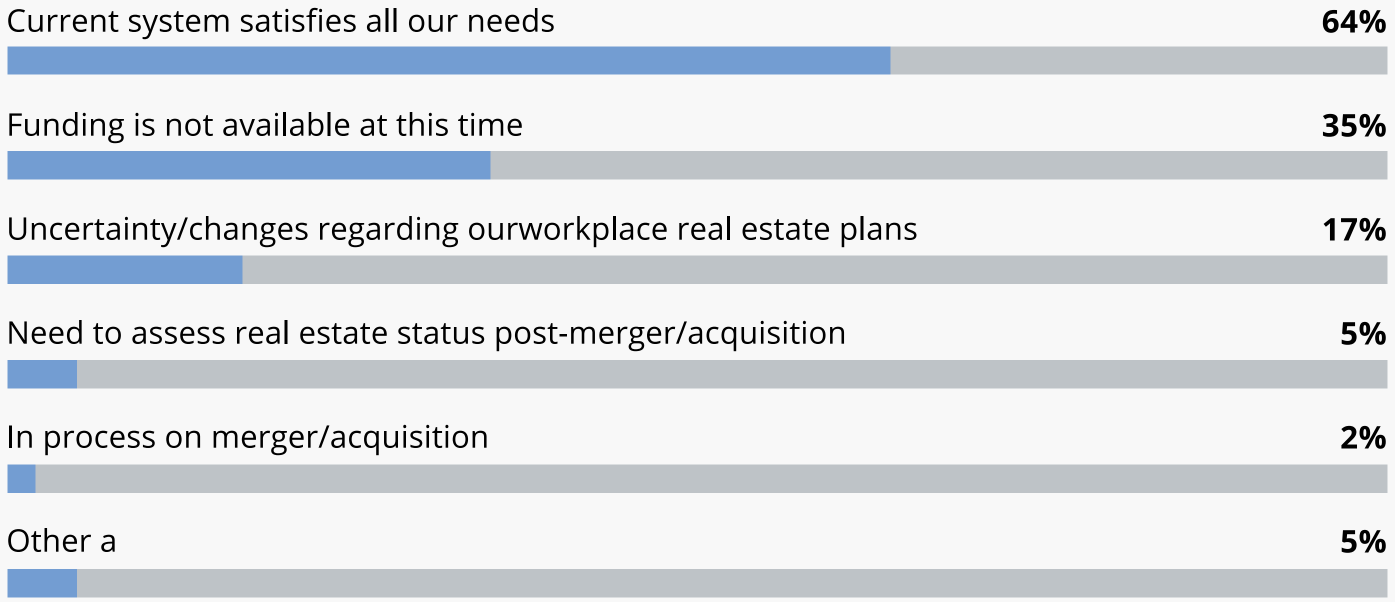
FIGURE 2. CURRENT ACCESS CONTROL UPGRADE PLANNING

Are you planning to substantially upgrade or expand your electronic physical access control systems in the near future?



Base: All respondents (n=155).

Why are you not upgrading your physical access control system?
(Please select all that apply.)

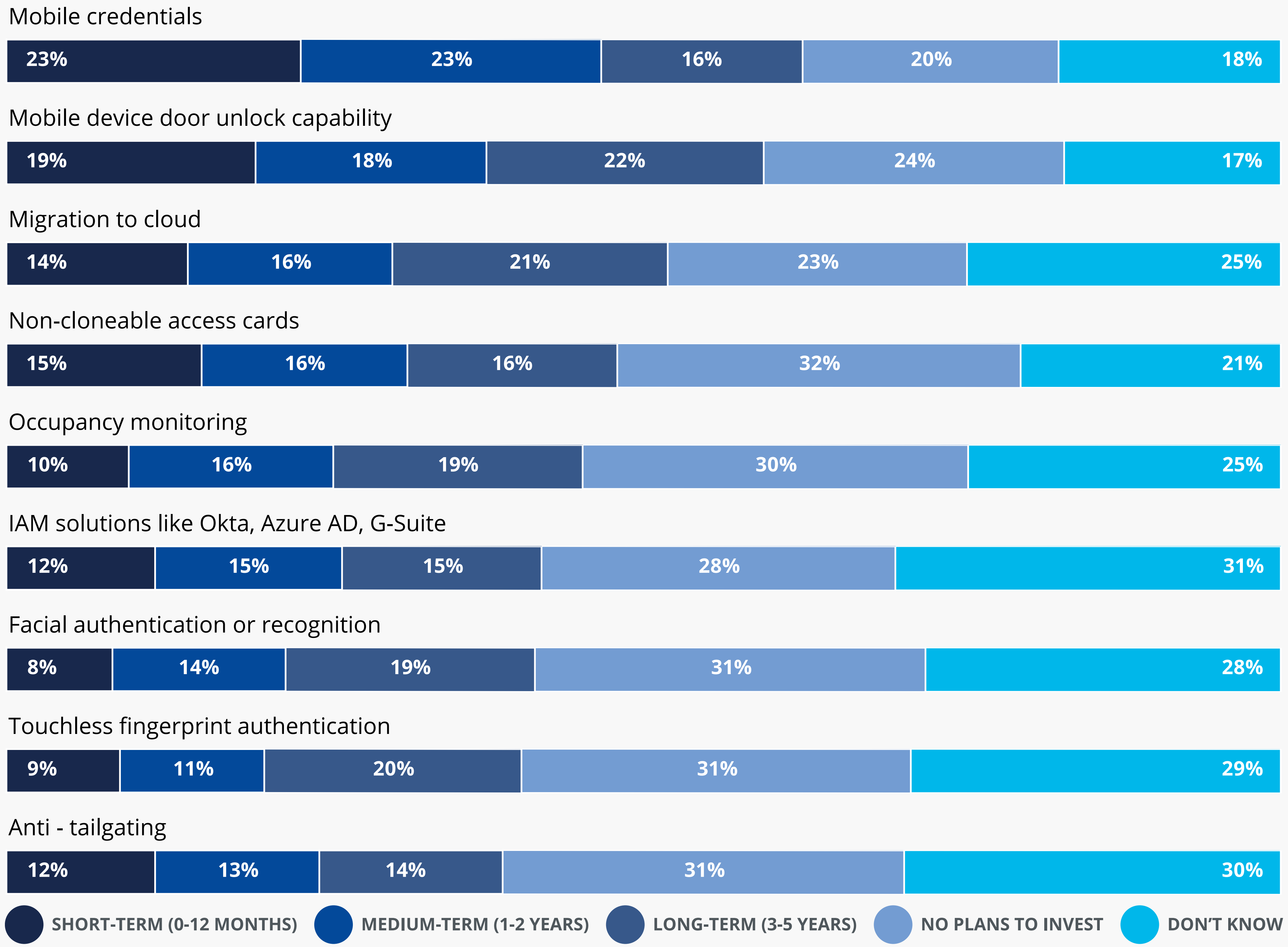


USER EXPECTATIONS FOR ACCESS CONTROL SYSTEM MODERNIZATION

As shown in Figure 2, 27% of respondents are eyeing significant access control upgrades. Figure 3 shows that 62% plan to use mobile credentials within five years, with 23% planning to do so within the next year. Fifty-nine percent of respondents plan to implement mobile device door unlock capabilities within the next five years. Consistent with the overarching trend of businesses migrating to the cloud, 51% of respondents aim to switch to a cloud-based access control system in the upcoming two years.

FIGURE 3. PLANNED ACCESS CONTROL IMPROVEMENTS.

Which access control improvements do you plan to implement in the following timeframes?



CURRENT STATE OF CLOUD-BASED PHYSICAL ACCESS CONTROL OFFERINGS

True cloud access control systems allow multiple end users to share the same cloud-native application and its pools of computing resources. A true cloud system utilizes cloud computing technology in ways legacy and single-customer applications can't. As depicted in Table 1 below, transitioning from "Cloud Hosted Legacy System" to "True Cloud Access Control" showcases a distinct advancement in technological maturity, scalability, automation, integration capabilities and security features deemed essential by end users.

TABLE 1. CLOUD ACCESS CONTROL SYSTEM OFFERINGS

CHARACTERISTIC	Cloud-Hosted Legacy System	Single-Tenant Web Application	True Cloud Access Control
ARCHITECTURE	Legacy access control system, with server hosted in a cloud virtual machine (VM) instead of on-premises.	Software designed for a cloud VM environment, with each customer having its own VM.	Fully cloud native application, taking full advantage of cloud computing characteristics and capabilities.
SCALABILITY	Fixed capacities, requiring over-provisioning hardware to account for peak activity periods.	Manual scaling, such as changing VM size or subscribing to more processing power.	Automatically scales computing and storage resources up or down based on demand without manual intervention, including for parallel event, alarm, rule, and notification processing with no loss in performance at any volume.
UPDATES	Manual intervention to update operating system or application software or apply security patches. Server and/or application downtime is usually required.	Updating update operating system or application software and applying patches may be manual or automated. Some server and/or application downtime is usually required.	automatically (i.e., server, web client and mobile apps), ensuring that security patches and new features are rolled out seamlessly.

CHARACTERISTIC	Cloud-Hosted Legacy System	Single-Tenant Web Application	True Cloud Access Control
RESILIENCE OF SERVERS AND APPLICATIONS	Hot or cold redundant servers, especially across separate geographical regions, are typically found only in crucial infrastructure deployments, due to high cost. Server software crash recovery is not automatic. Required manual recovery and may involve significant downtime and the involvement of both the access control software manufacturer and the installing/ maintaining service provider. When server is offline, facility access control operations continue to run based on controller hardware capabilities. Administrative actions and manual access control such as unlocking doors are not available.	Server redundancy in the same or different geographical location is sometimes available as an extra cost option. Server software crash recovery is not automatic. Required manual recovery and may involve significant downtime, and the involvement of both the access control software manufacturer and the installing/maintaining service provider. When server is offline, facility access control operations continue to run based on controller hardware capabilities. Administrative actions and manual access control such as unlocking doors are not available.	High-availability deployment that runs two instances of its web application. Each instance is typically deployed in two different geographic regions, selectable by the end user. Every cloud component in the platform has a redundant counterpart, including load balancers, web servers, application servers and database servers — to eliminate single points of failure. Data is synchronized between the two instances. Inside each instance, the health of each component is continually checked and restarted automatically when necessary. Upgrades are very thoroughly tested and instant rollbacks can be quickly performed if a software problem occurs. Such measures assure that the system is available with at least 99.9% uptime.
DATA BACKUP AND RECOVERY	Database backups are either manual or automatic and may or may not be off-site. Manual recovery from database failures is required and is typically complicated and lengthy, involving server downtime. Typically, backup and recovery capabilities are less than ideal due to deployment funding limitations.	Backup of applications and data is usually performed automatically in the cloud on a periodic basis. Recovery from database failures requires manual action. Database recovery is usually simple for cloud-based backups but typically requires system downtime.	Data backup is nearly continuous to more than one geographic location. Two distinct instances of the system are processing data. A data failure occurs in one instance of processing, the alternate instance continues data processing while the other data processing instance is restored. If a data storage location experiences a failure, an alternate data storage location continues data storage and retrieval while the failed data storage location is restored. This approach assures 99.9% uptime for data processing and storage.
INTEGRATION	May have a licensed SDK. It is not designed to easily integrate with modern APIs or cloud services out of the box.	May have an open API but integration capabilities are typically constrained by fixed processing resources, and lack of parallel processing capability.	Open API is designed to easily integrate with other cloud services, APIs and even IoT devices. Many existing integrations are likely to exist for popular HR and building systems.

CHARACTERISTIC	Cloud-Hosted Legacy System	Single-Tenant Web Application	True Cloud Access Control
ON-DEMAND SELF-SERVICE	Not applicable.	Not applicable.	On-demand self-service, such as for adding readers and end-user mobile devices, is maintained as applicable for both end-user customers and installing/maintaining service providers.
BROAD NETWORK ACCESS	Not available.	Anytime, anywhere access is available via the internet.	Anytime, anywhere access is available via the internet.
RESOURCE POOLING	Not applicable.	Not applicable.	Utilized to maximize cost-effectiveness for both cloud platform providers and all subscribers.
RAPID ELASTICITY	Not applicable.	Not applicable.	Utilized to maximize system performance capabilities.
CLOUD-CONNECTED HARDWARE	On-premises devices and controllers are not engineered for cloud connectivity or to be cloud-managed.	On-premises devices and controllers are not engineered for cloud connectivity or to be cloud-managed.	On-premises devices and controllers are designed from the ground up to work seamlessly with the cloud platform. Cloud-managed firmware updates are performed quickly and automatically.
SECURITY	Legacy systems have few to no cybersecurity features built into software or hardware. Computer and network security measures are to be added to the deployment and manually kept updated.	Systems hosted on public clouds benefit from the cloud providers' built-in infrastructure security. However, application security will vary based on how well-engineered the web application is. The on-premises hardware still requires network security measures to be added to the deployment and manually kept updated.	The cloud and on-premises elements of the system are engineered for high security, and the cloud platform provider provides detailed information about the platforms' security. Ideally, the platform provider is enrolled in the STAR registry of the Cloud Security Alliance, which includes providing a downloadable detailed self-assessment
DATA PRIVACY AND COMPLIANCE	Legacy systems typically have few data privacy or compliance features built into the system, due to the age of their design.	May or may not have privacy features or facilitate manual user management of data privacy, depending on the age of the system software.	Typically, compliant with the strongest set of privacy and compliance requirements across its customer base, which all customers benefit from.
FUTURE READINESS	Due to the rapid advance of cloud computing technology, legacy systems become more obsolete over time.	Single-tenant web applications make limited use of cloud technology advances, so their capabilities and performance do not advance in step with the state of cloud technology.	True cloud access control platform providers keep their application engineering in step with cloud technology advancements and keep their open APIs advancing per customer requirements and leading API design and development practice.

USER EXPECTATIONS FOR ACCESS CONTROL SYSTEM MODERNIZATION

When contemplating an upgrade to a cloud-based access control system, the system's security, data privacy and compliance are deemed "extremely important" by a predominant portion of the survey participants. Other notable considerations include system reliability and cost, as depicted in Figure 4.

Anywhere, anytime remote access management, along with accessing and opening doors remotely, are the top two capabilities respondents would value from an upgrade to cloud-based access control.

FIGURE 5. CAPABILITIES DESIRED FROM CLOUD-BASED ACCESS CONTROL

What capabilities would you value from an upgrade to cloud-based access control?

(Please select all that apply.)

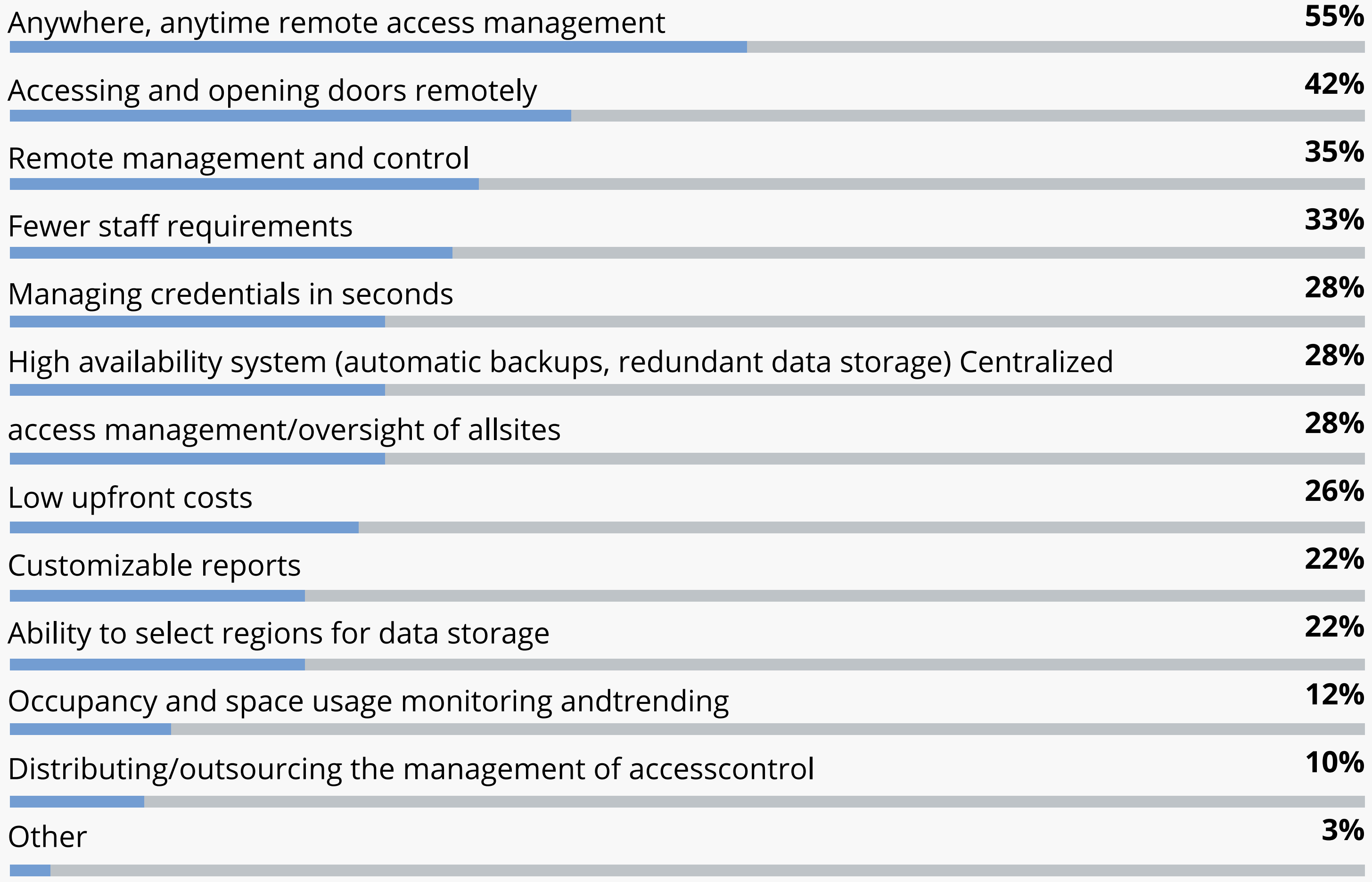
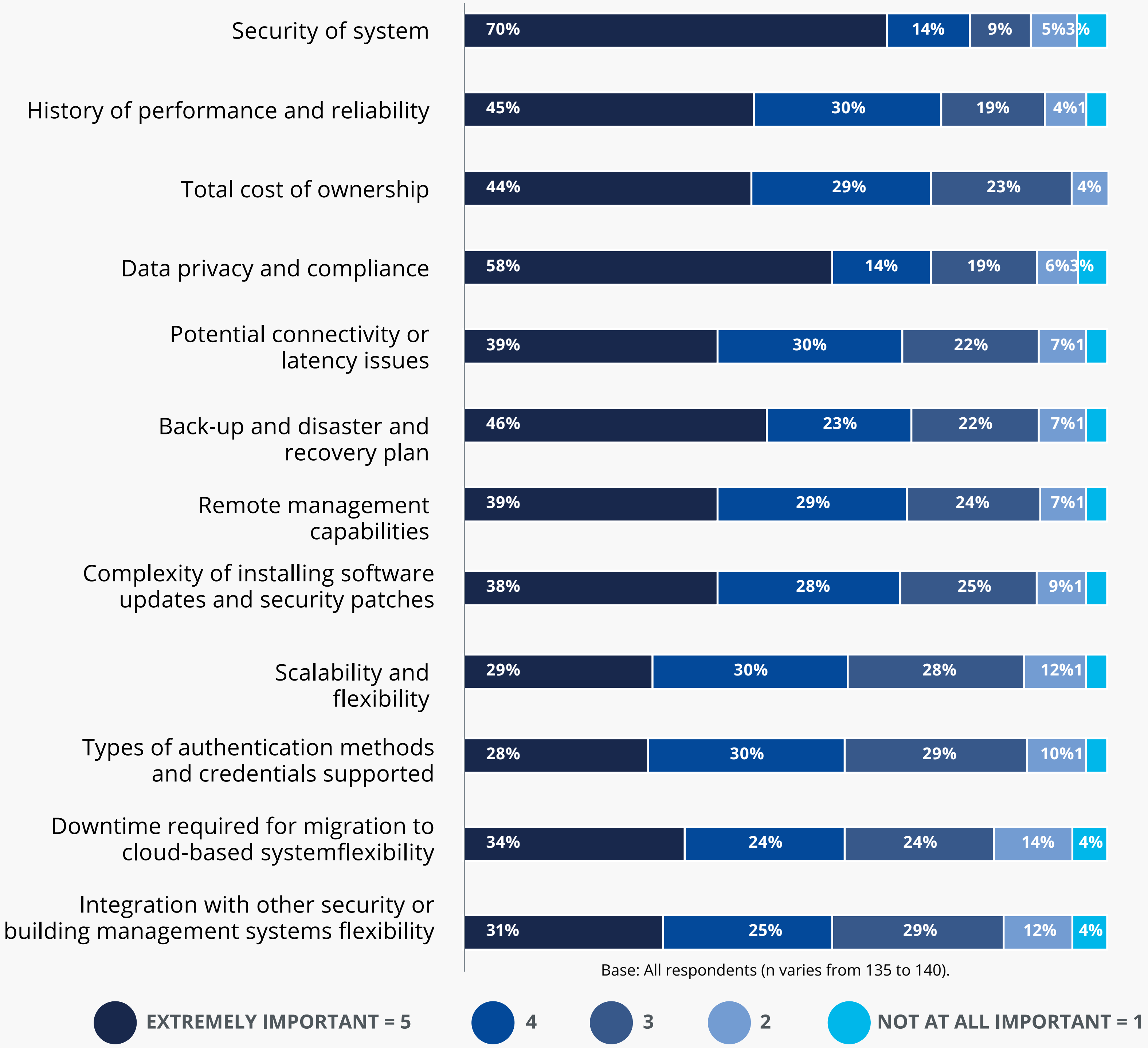


FIGURE 4. KEY FACTORS WHEN UPGRADING CLOUD-BASED ACCESS CONTROL SYSTEMS

When upgrading to a cloud-based access control system, how important are each of the following?



Base: All respondents (n varies from 135 to 140).

ASSURING MAXIMUM RETURN ON INVESTMENT

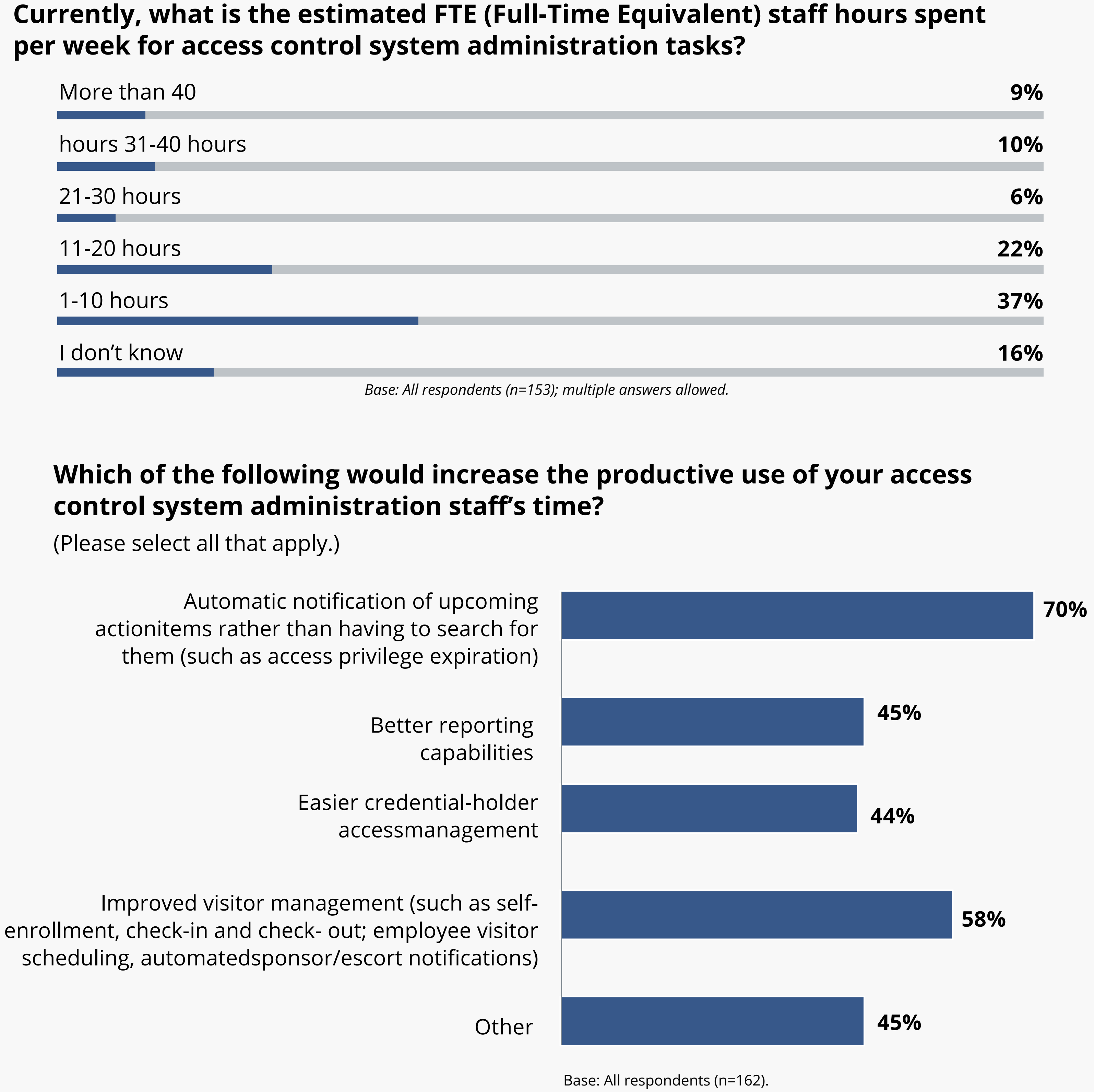
Upgrading to a true cloud access control system brings tangible and intangible ROI benefits. On the intangible side, enhancements that contribute to workplace convenience and boost employee contentment take the lead. A significant intangible asset lies in the system's inherent continuous improvement, analogous to autonomous smartphone updates.

On the tangible front, stringent privilege management eradicates potential access vulnerabilities. Utilizing mobile device credentials effectively tackles the challenges of lost or stolen cards. Mobile credentials also serve a dual purpose by facilitating multi-factor authentication through built-in device biometrics, negating the need for additional biometric hardware and software investments.

Administrative simplicity trims down staff hours required for access management. Nearly half of respondents (47%) indicate more than 10 FTE staff hours are spent each week on access control system administration tasks. There are particular domains, illustrated in Figure 6, where optimizations can improve staff time utilization. For instance, integrating automated time and attendance systems can do away with manual punch card operations, and leveraging mobile device biometric verification at employee check-in and check-out locations eliminates time-cheating via buddy punching.

Migrating to a subscription-based cloud access model mitigates the substantial capital outlay previously needed to upgrade on-premises systems hardware and software. Cloud-managed software and firmware updates reduce service costs. One notable tangible advantage, typically embedded within the subscription cost, is the provision of a complimentary field hardware replacement after a predefined time period, accounting for product advancements over time.

FIGURE 6. ACCESS CONTROL SYSTEMS ADMINISTRATION



Currently, what is the estimated FTE (Full-Time Equivalent) staff hours spent per week for access control system administration tasks?

Base: All respondents (n=153); multiple answers allowed.

Which of the following would increase the productive use of your access control system administration staff's time?

(Please select all that apply.)

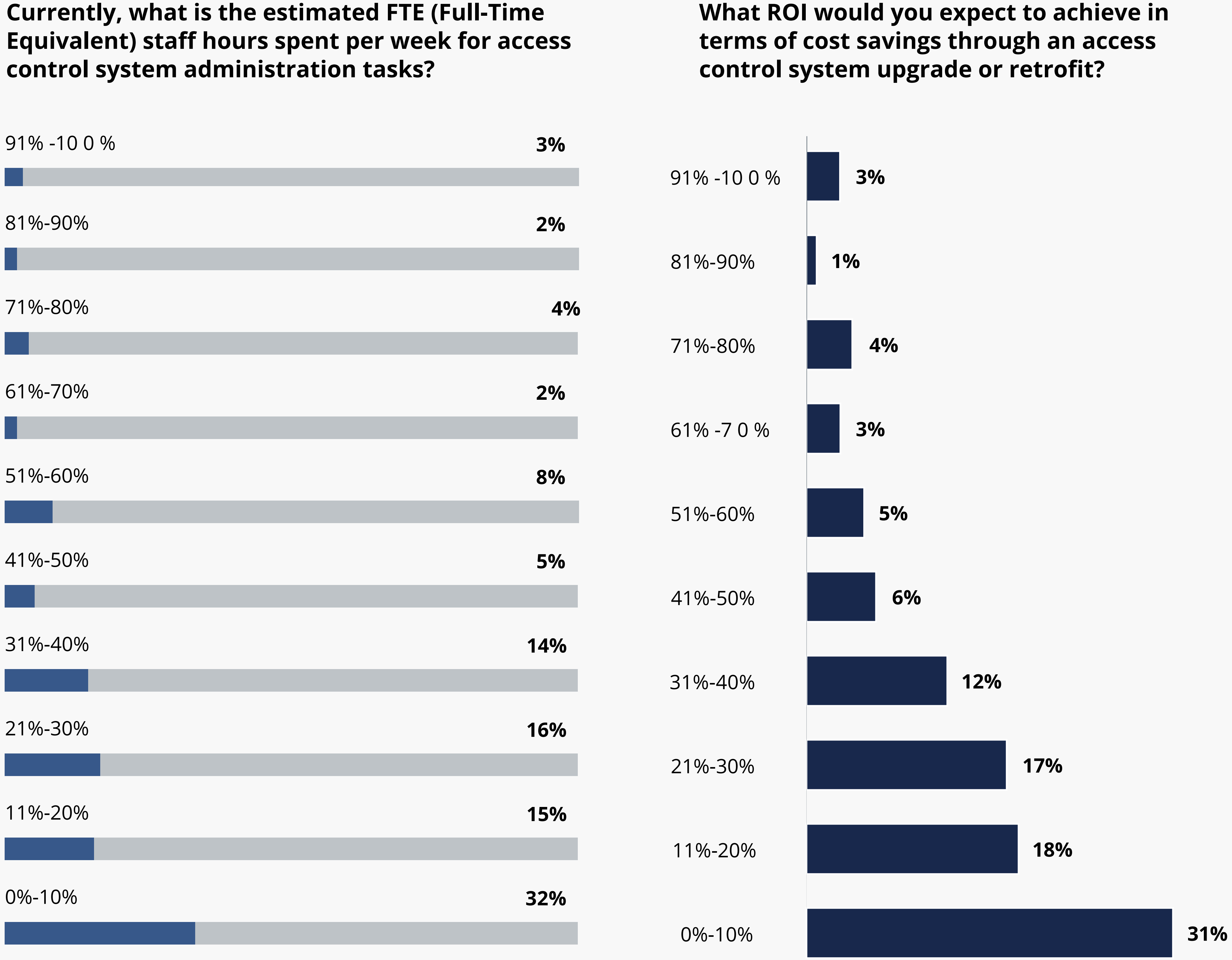
Base: All respondents (n=162).

Survey participants anticipate an average 27% ROI in terms of both time efficiency and cost savings through an access control system upgrade or retrofit (see Figure 7).

Maximizing the ROI of transitioning to a cloud- based system can benefit from collaboration with experienced manufacturer representatives familiar with the cloud access deployments and their integrations for organizations of a similar type and size as yours. Engaging in dialogue about potential integrations, gauging the expected returns and mapping out the deployment logistics (including for the integrations) are prudent steps. Documenting the ROI picture aids in determining the required funding. It also helps to enlist the support of those who would benefit from the desired integrations.

Two pivotal elements demand awareness when discussing funding for a cloud upgrade: The shift from intermittent CapEx injections to consistent OpEx commitments and the broader ROI benefits that the organization would gain beyond the facility security risk reductions. These should be of interest to those with overall digital transformation responsibilities.

FIGURE 7. ROI EXPECTATIONS



Currently, what is the estimated FTE (Full-Time Equivalent) staff hours spent per week for access control system administration tasks?

Base: All respondents (n=155).

What ROI would you expect to achieve in terms of cost savings through an access control system upgrade or retrofit?

Base: All respondents (n=154).

brivo

SIW SECURITY INFOWATCH.COM