



HID 2026 State of **Security** and **Identity** Report

Table of Contents

Introduction	3	Smart Supply Chains Drive Sustainable RFID Adoption	19
A Deeper Dive: 7 Key Trends (and 1 Bonus Trend to Watch)	5	Investment Patterns Shift Toward Continued Integration	21
Identity Management Dominates Strategic Planning Activity	9	BONUS: Ethical Considerations and Privacy Concerns at an All-Time High	23
Mobile Credentials Reach Critical Mass	11	Looking Forward	24
Biometrics Expands Beyond MFA into Core Access Control	13	Conclusion	25
Real-Time Location Solutions Emerge for Safety and Efficiency	15		
Physical-Digital Identity Convergence Accelerates	17		



Introduction

The security perimeter has collapsed. Not because of cloud, not because of remote work—but because organizations finally realize that the person badging into Building 3 and the user logging into Salesforce are the same human, and treating them differently is the vulnerability.

Gone are the days when security operates in a vacuum. Instead, security is poised to touch every part of the organization, as security leaders find a seat at the table and help navigate the future of their companies.

Convergence has been an overarching theme in the last year or so, with the proliferation of security program optimization and integration of solutions for seamless response. However, the transformation seen in this year's survey takes this optimization even farther, conveying just how much today's end-user organizations require (and plan to utilize) more cross-functional integration to power their security programs.

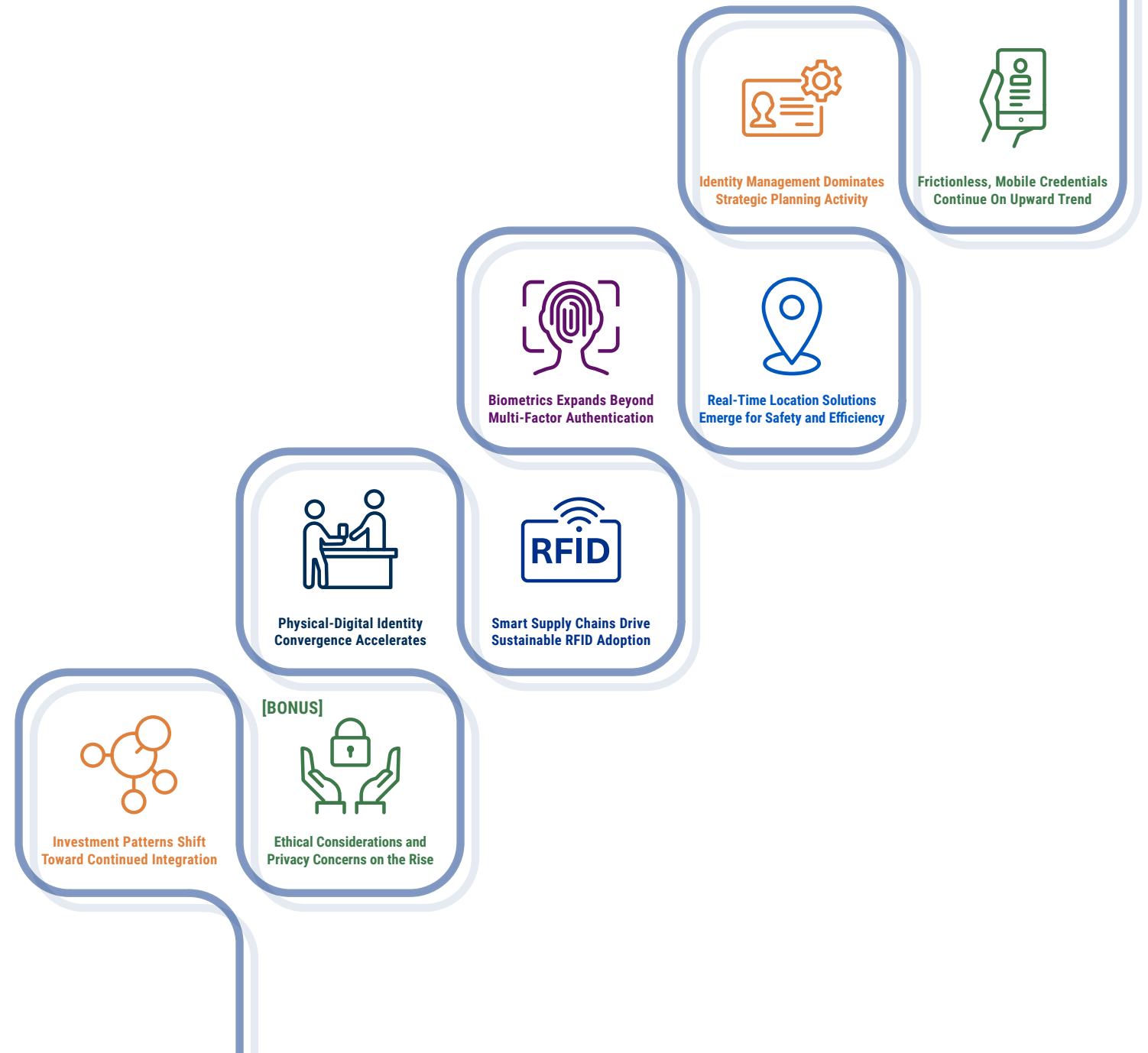
Identity management is emerging as a top strategic priority for end users as organizations no longer view access control as simple credential management. They are adopting comprehensive identity governance across physical and digital platforms, prioritizing integration between solutions to streamline security program operations.

The 2026 State of Security and Identity Management Report, which included more than 1,500 end users and industry partners (installers, integrators and original equipment manufacturers), reveals an industry reaching a critical inflection point. The complexity of managing fragmented identity systems (cited by 52% as their primary challenge) has collided with escalating threats where attackers exploit the seams between physical and digital security. The result: a fundamental restructuring of how organizations approach identity, access, and security architecture.

Executive Summary: Key Trends for 2026

The 2026 landscape centers on a single pattern: organizations are dismantling the artificial boundary between physical and digital identity at unprecedented speed. The seven trends that follow are not disconnected observations—they are interconnected manifestations of this convergence imperative.

1. Identity Management Dominates Strategic Planning Activity
 2. Frictionless, Mobile Credentials Continue On Upward Trend
 3. Biometrics Expands Beyond Multi-Factor Authentication (MFA) into Core Access Control
 4. Real-Time Location Solutions Emerge for Safety and Efficiency
 5. Physical-Digital Identity Convergence Accelerates
 6. Smart Supply Chains Drive Sustainable RFID Adoption
 7. Investment Patterns Shift Toward Continued Integration
- BONUS:** Ethical Considerations and Privacy Concerns on the Rise



A Deeper Dive:

7 Key Trends (and 1 Emerging Trend to Watch)



Identity Management Dominates Strategic Planning

In this year's survey, identity management for secure access emerges as a critical component of modern security strategies, with 73% identifying it as a top trend, the highest across all categories. This represents a shift from credential management to comprehensive protection through identity governance spanning physical and digital security. Managing multiple systems is the primary challenge (52%), driving 60% of respondents to plan spending increases in this area. Organizations seek unified platforms managing employee credentials, visitor access, MFA and Physical Identity and Access Management (PIAM) simultaneously. Persistent obstacles include limited budgets (41%), user friction (42%), regulatory compliance (29%) and cloud integration challenges (27%). However, forward-thinking organizations recognize that consolidation delivers long-term return on investment (ROI) through reduced overhead, improved security and enhanced user experience. The market has largely committed to identity management platforms, with focus shifting from "if" to "how."



Frictionless, Mobile Credentials Continue On Upward Trend

Mobile credentials have transitioned from an emerging to baseline technology, with 74% of respondents having already deployed (36%) or planning deployment (38%) of these credentials. Security improvements now drive adoption (50%), with convenience (34%) taking more of a backseat this year compared to last year's report as organizations recognize mobile credentials' robust protection through biometric authentication and encrypted communication.

Hybrid deployments continue, with 84% of end users maintaining mixed credentials, acknowledging diverse user groups and use cases that require flexibility. For those who have not deployed, cost concerns intensify as the primary barrier (44%), alongside expertise gaps (37%) and complexity perceptions (32%). Five-year outlook shows confidence, however: 80% predict mostly mobile or balanced environments, though only 8% expect fully mobile, reflecting ongoing hybrid needs.



Biometrics Expands Beyond MFA Into Core Access Control

Biometric technology maintains momentum, with 45% of respondents viewing it as a strategic priority, 34% indicating they have already deployed biometrics, plus 23% planning implementation. Fingerprint recognition leads modalities (71%), followed by facial recognition (50%), with accuracy and reliability dominating priorities (70% end users, 85% partners). Privacy concerns have risen substantially, from 31% in the 2025 survey to 67% this year, expressing ethical concerns over biometric use. Around 31% of respondents are actively implementing safeguards for biometrics within their organization as a result. Investment outlook further demonstrates the progression of biometrics on the adoption curve, with 60% of end users likely to increase spending in the coming years. Barriers include costs, privacy concerns, and unclear ROI, requiring targeted messaging around compliance and security enhancement.



Real-Time Location Solutions Emerge for Safety and Efficiency

Real-time location solutions emerge as a significant 2026 trend, with 42% of end users identifying it as a strategic priority and 40% indicating they have deployed the technology. Worker safety and compliance dominate adoption drivers (69%), followed by asset management (59%), demonstrating dual value in protecting people and resources. Implementation barriers include high costs (33%), organizational relevance (33%), integration complexity (29%) and privacy concerns (29%). Notably, 38% of partners report customer unfamiliarity, indicating substantial education opportunities. The technology spans diverse use cases, including in healthcare for equipment tracking, in manufacturing for safety monitoring and in logistics optimization. Growth expectations remain high as 53% anticipate expansion, though measured scaling suggests organizations are validating ROI before widespread deployment.



Physical-Digital Identity Convergence Accelerates

Physical-digital identity convergence represents a frontier transformation, with 75% of organizations stating they have deployed (29%) or are evaluating (46%) converged solutions. This unified approach enables single credentials to access buildings, networks and cloud applications, reducing risk while enhancing user experience. However, substantial barriers persist, including budget constraints (51%), implementation complexity (37%), and expertise gaps (34%). Security concerns intensify as 30% recognize that platform compromise could grant unauthorized access to both facilities and data. Impeding adoption is an awareness gap, with 15% indicating they are unaware of available solutions. The 25% with no integration plans need clearer value propositions demonstrating enhanced security, operational efficiency, and improved compliance.



Smart Supply Chains Drive Sustainable RFID Adoption

RFID technology shows steady growth rather than revolutionary change, with 54% of current usage demonstrating near-mainstream status in applicable industries. Primary applications focus on operational efficiency: asset tracking and inventory management (both 29%), delivering faster inventory tracking (62%), improved visibility (41%) and loss prevention (37%). Adoption barriers include perceived high tag/reader costs (35%), integration complexity (33%) and expertise gaps (28%). RFID technology options have expanded significantly, offering dozens of tag types for diverse environments, from water-resistant glass tags to harsh industrial applications. While 27% report no implementation challenges, 46% haven't adopted, indicating many organizations are not realizing -or have yet to evaluate- the benefits of RFID technology.



Investment Patterns Shift Toward Continued Integration

Organizations are expressing the desire to shift from standalone solutions to more integrated platforms that deliver comprehensive capabilities and unified identity management. Investment priorities reveal this strategic evolution: a stronger focus on identity management leads (60% increasing spend), followed by real-time location systems (53%) and biometrics (60%). Mobile credentials have transitioned to a baseline expectation at 74% adoption. With this proliferation of technology, integration complexity remains the universal barrier of bringing it all together, as 52% struggle with identity management systems, 37% with physical-digital convergence and 33% with RFID. Budget constraints were most impactful on physical-digital integration (51%), mobile credentials (44%) and identity management (41%). Platform consolidation delivers compelling benefits: improved efficiency (44%), simplified management (30%), and enhanced visibility (16%), multiplying exponentially when identity management, access control, biometrics and RTLS converge into cohesive solutions.



Emerging Trend: Ethical Considerations and Privacy Concerns at an All-Time High

Privacy and ethical considerations are emerging as critical factors in 2026 security decisions, with 67% of end users expressing concern about biometric implications and 29% reporting concerns with RTLS.

Privacy challenges extend across technologies: 29% cite data privacy as a barrier to real-time location systems adoption, creating tension between worker safety (69% adoption driver) and individual privacy rights. Mobile credentials face 19% privacy-related resistance, while 30% hesitate on physical-digital integration due to security concerns. Organizations are responding through policy development (36% considering safeguards), though 12% remain unconcerned, potentially underestimating regulatory risks.

Trend 1

Identity Management Dominates
Strategic Planning Activity





Identity Management Dominates Strategic Planning Activity

Identity management software has emerged as an essential component of modern security strategies, with 73% of physical security professionals identifying it as a top-three trend, the highest ranking across all categories surveyed for 2026. Industry partners echo this, with 61% prioritizing this trend as important to their business and their customers. This represents a shift from viewing credential management as merely access control to now embracing comprehensive identity governance that spans both physical and digital realms.

The stakes have never been higher. The complexity of managing multiple systems has become the primary challenge in identity management, with 52% of respondents citing this as their most significant barrier. As threat actors increasingly exploit the seams between physical and digital domains—now armed with AI-powered tools that can generate deepfakes, synthesize biometric spoofs, and automate credential stuffing at scale—security leaders recognize that fragmented systems create vulnerabilities. The fragmentation of traditional security systems, where access control, visitor management, and digital authentication operate in silos, is no longer sustainable in an era where seamless integration determines operational efficiency and security effectiveness.

Investment patterns reflect this strategic importance, with 60% of organizations planning to invest in identity management, suggesting a market that has largely committed to identity management platforms, with the question shifting from “if” to “how” to optimize these investments.

Organizations are expressing the desire to bridge identity management through comprehensive platforms. The ability to manage employee credentials, visitor access, MFA and PIAM from a unified solution represents the future of security operations. This approach enables organizations to provide safe, convenient access to facilities and systems as a solution for their unique needs rather than forcing compromises with point solutions.

Limited budget and resources remain persistent obstacles, cited by 41% of respondents. Additionally, other challenges exist to full adoption of identity management today: user friction with authentication (42%), regulatory compliance requirements (29%) and integration challenges with cloud applications (27%) all introduce barriers.

However, many respondents recognize that consolidating identity management delivers long-term ROI through reduced administrative overhead, improved security posture and enhanced user experience.

Trend 2

Frictionless, Mobile Credentials
Continue On Upward Trend



Frictionless, Mobile Credentials Continue On Upward Trend

The majority of those surveyed reported deploying or planning to deploy mobile credentials in this year's survey, with 74% of organizations stating they either have already deployed them (36%) or are actively planning deployment (38%). This marks the transition from emerging technology to expected baseline capability, which is a marked shift reflected in the fact that while 52% still identify frictionless access and mobile credentials as a top trend, this represents a decline from previous years as the technology becomes normalized rather than novel.

The driver for adoption has evolved significantly. Security improvements now lead at 50%, surpassing user convenience (34%), indicating that organizations view mobile credentials as a robust security enhancement rather than merely a convenience feature. This perception shift aligns with the reality that mobile credentials leverage advanced security-centric capabilities and mutual authentication, reducing risk from lost cards and forgotten passwords through biometric authentication and encrypted communication. The ability for security leaders to better manage credentialing is also a testament to its increased adoption rates.

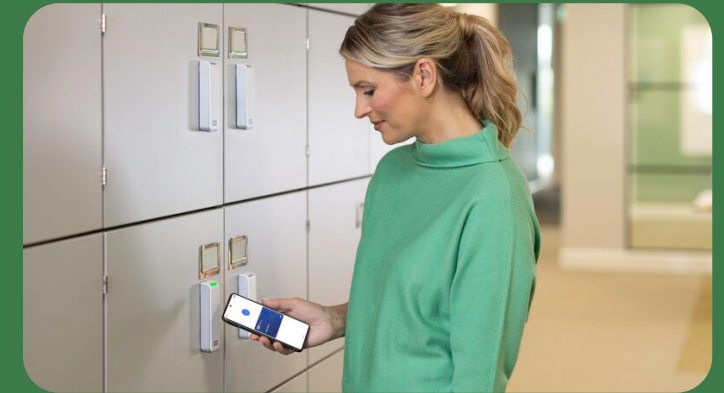
Partner perspectives reveal interesting dynamics. Among those surveyed, industry partners reported the biggest drivers of mobile credentialing were user convenience (77%), with security improvements at 57% and cost savings at 42%. However, partners also face distinct challenges: 63% cite the preference for physical credentials as a reason for not deploying more mobile credentials to their customers, with perceived cost and the need for a visible ID card both at 31%.

The hybrid reality persists, with 84% of end users maintaining a mix of mobile and physical credentials. This balanced approach acknowledges that one size doesn't fit all. Different user groups (employees, visitors, contractors) and use cases (secure areas requiring visible badges, temporary access, VIP access) require flexibility in which form factors are used and how credentialing is managed.

Cost concerns have intensified as a barrier, with 44% of end users citing perceived implementation costs as their primary obstacle to deployment (as opposed to 24% in 2025). This represents a notable increase in cost sensitivity, likely reflecting broader economic pressures or insufficient demonstration of ROI. Additional adoption barriers include a lack of in-house expertise (37%), perceived complexity of managing mobile credentials (32%), lack of hardware infrastructure (32%) and the preference for physical credentials (32%).

For those organizations, partners are needed to communicate the long-term value of mobile credentialing: reduced card production and replacement costs, elimination of physical credential management overhead and enhanced security that prevents costly breaches.

Looking five years ahead, 80% predict a mostly mobile or balanced mix environment, with only 12% expecting mostly physical credentials. This trajectory demonstrates confidence in mobile technology's advancement, though only 8% expect fully mobile environments. This indicates that while mobile will continue to rise, physical credentials will remain an important part of the identity mix.



Real-Time Credential Management with Mobile Wallets

Mobile wallet credentials give administrators real-time control over every stage of the credential lifecycle.

- Issue credentials in real time without printing cards
- Grant immediate access to new hires
- Update access rights as roles change
- Revoke access instantly for lost devices or former users

Mobile credentials reduce delays, manual effort, and security gaps.

Trend 3

Biometrics Expands Beyond MFA
into Core Access Control



Biometrics Expands Beyond MFA into Core Access Control

Biometric technology is experiencing significant momentum, with 46% of security professionals viewing biometrics and AI-enhanced verification as a strategic priority. Current adoption stands at 34% among end users, with an additional 23% planning deployment. This means that biometric authentication is shifting from a niche application to a more mainstream identity management strategy.

Technology preferences remain consistent, with fingerprint recognition leading at 71% and facial recognition second at 50%. This stability suggests the market has identified its preferred methods of biometric modalities based not only on user acceptance, but also on proven performance across organizations. But implementation priorities reveal what truly matters: accuracy and reliability dominate at 70% for end-users and an even higher 85% for partners, reflecting the mission-critical nature of biometric deployments and the need for product performance that delivers consistent reliability.

The partner-driven landscape presents both opportunities and challenges. Partners show notably higher emphasis on preventing spoofing and fraud (49% versus 43% for end users), suggesting integrators are encountering sophisticated threat scenarios that demand advanced security features. Integration with existing systems ranks as a top-three priority for 46% of end users, but is notably higher for partners (64%), underscoring the importance of connecting biometrics with other security technologies.

Privacy and ethical concerns have risen substantially, with 67% of organizations reporting moderate or high concern about biometric use. Nearly 30% say privacy concerns influenced their decision not to deploy biometric solutions in 2025. This includes 31% who are very concerned and actively implementing safeguards. The heightened awareness reflects growing regulatory scrutiny, particularly around facial recognition, and demonstrates that organizations are taking the safe management of biometric data seriously. Biometric solutions must comply with [applicable regulations](#), such as HIPAA in healthcare, when biometrics are used to match a patient to a medical record. They must also protect biometric data using encryption at rest, including database and file-level encryption, and encryption in transit using secure transport protocols to prevent unauthorized access.

There's a divergence among partners and end users when it comes to increasing biometric investments. Among end users, 60% are very likely or somewhat likely to increase biometric investment, while partners show more interest, with 84% considering it very likely or somewhat likely for customers to increase their biometric investments. This gap signifies a little more skepticism on the end user side and may indicate the need for partners and manufacturers to provide more education around the use and adoption of the technology.

For organizations not considering biometrics, the barriers differ from those of other technologies. While cost remains a factor, privacy concerns and the lack of clear ROI present unique obstacles that require targeted messaging around compliance, security enhancement and operational efficiency gains.



Trend 4

Real-Time Location Solutions
Emerge for Safety and Efficiency



Real-Time Location Solutions Emerge for Safety and Efficiency

Real-time location solutions (RTLS) represent one of 2026's most significant emerging trends, with 42% of end users and 36% of partners identifying it as a strategic priority. Current adoption at 40% demonstrates that this technology has moved beyond the experimental phase for early adopters, yet 47% have not deployed, indicating a significant opportunity for partners and providers of this technology.

The primary driver for adoption is unambiguous: worker safety and compliance dominate at 69% for end users and 61% for industry partners. This focus on safety reflects growing regulatory requirements, heightened organizational responsibility for employee well-being and the recognition that instantly knowing the location of an individual during emergencies can save lives.

Asset management and tracking follow as the secondary driver at 59% for both users and partners, demonstrating the dual value proposition of protecting both people and critical resources. In asset management scenarios, real-time location solutions reduce the time staff spend searching for equipment and help organizations keep high-value assets in service rather than replacing them prematurely. In healthcare and industrial environments, RTLS is used to locate shared equipment quickly, manage utilization across departments and reduce losses caused by misplacement or theft.

Implementation barriers reveal the practical challenges facing organizations. High costs (33%), relevancy to the organization (33%), integration complexity (29%) and data privacy concerns (29%) cluster at similar levels, indicating that successful adoption requires addressing multiple blockers to adoption at the same time.

The 38% of partners who report customers are not familiar with the technology points to a significant education opportunity that can lead to higher adoption rates in the future.

The technology's applicability spans diverse environments and use cases. From tracking critical assets in real time to optimizing how people and things move through facilities, real-time location solutions leverage powerful radio frequency identification (RFID) and Bluetooth Low Energy (BLE) technology to improve operational efficiency. Organizations in healthcare, for example, track equipment and ensure patient safety; manufacturers monitor work-in-progress inventory and enhance worker safety in hazardous zones; logistics operations optimize warehouse flows and loading dock operations.

Growth expectations are robust, with 52% anticipating moderate to significant expansion in their use of RTLS. Interestingly, only 13% expect significant expansion while 40% predict moderate growth, suggesting measured scaling as organizations validate use cases and ROI. Those 14% who remain unsure about future usage indicate this market is still defining itself, with success stories and proven implementations needed to build confidence.



Trend 5

Physical-Digital Identity
Convergence Accelerates





Physical-Digital Identity Convergence Accelerates

The convergence of physical and digital identity represents a frontier transformation in security strategy, with 75% of organizations indicating they have already deployed converged identity solutions or are actively evaluating options. This trend reflects the fundamental recognition that artificial separation between physical and digital access creates security gaps, operational inefficiencies and poor user experiences in an increasingly connected and digital world.

Organizations are seeking to establish airtight security for IT networks while simultaneously managing access to physical spaces using unified identity platforms. The vision is compelling: employees use a single credential, whether it's a physical keycard or digital credential to access buildings, networks, cloud applications and sensitive data. This approach reduces risk, enhances experience and provides better visibility into identity-based security across the enterprise.

However, barriers to integration remain substantial. Lack of budget tops the list at 51%, reflecting the reality that converging physical and digital systems often requires significant infrastructure investment and potentially replacing legacy systems. Concerns about implementation complexity (37%) and lack of internal expertise (34%) cluster at similar levels, indicating that organizations recognize the technical challenges ahead.

The security and privacy concerns cited by 30% reflect the heightened sensitivity when identity management spans both physical and digital realms. A compromise could potentially grant unauthorized access to both facilities and data, raising the stakes for security architecture (and the security leaders who are tasked with protecting it). Organizations need solutions that leverage modern cryptography, zero-trust approaches, and strong authentication to provide identity protection across all access scenarios.

15% report they are not aware of available solutions, which suggests that even as technology leaders push forward with physical-digital convergence, a substantial segment of the market requires a basic understanding of what's possible and why it matters.

The 25% with no plans for integration represents organizations that either see no business case or face significant barriers to adoption. For these organizations, the value proposition must be clearer: enhanced security posture through unified identity management, improved user experience through single sign-on across physical and digital, operational efficiency through consolidated administration and better compliance through comprehensive audit trails.

Trend 6

Smart Supply Chains Drive
Sustainable RFID Adoption



Smart Supply Chains Drive Sustainable RFID Adoption

While receiving lower visibility as a top trend at 22%, RFID technology's role in enabling smart, sustainable supply chains represents steady growth rather than significant change.

Current usage stands at 54%, with all industries reporting RFID in use. This demonstrates that RFID has achieved near-mainstream status across the industries surveyed. In contrast, 46% of companies reported RFID technologies were not in use, which may indicate that the technology doesn't apply or a use case has not been realized.

Primary applications cluster around operational efficiency: asset tracking (29%), inventory management (29%) and supply chain logistics (16%). These use cases deliver tangible benefits, with 62% citing faster inventory tracking as their top advantage. This is a clear value proposition in fast-paced distribution and retail environments. Other benefits include improved visibility (41%), loss prevention (37%) and better customer service (28%), demonstrating the technology's ability to track critical assets in real time from anywhere.

A specialized subcategory within manufacturing and supply chain is emerging around medical devices, where RFID supports regulatory compliance and patient safety. In these environments, tags enable device identification and authentication aligned with requirements such as unique device identification (UDI), unique ID (UID) and Digital Product Passport initiatives. RFID also supports lifecycle visibility, helping organizations manage recalls, verify authorized use and reduce the risk of counterfeit or expired devices reaching patients.

The technology portfolio has expanded significantly, with providers now offering dozens of RFID tags designed to track a wide variety of assets and "things" across diverse environments. From small glass RFID tags with unlimited resistance to water and chemical absorption, to specialized tags for harsh industrial conditions, this broad assortment ensures organizations can find solutions tailored to their specific needs. Through a large range of use cases, such as tracking surgical instruments in hospitals, monitoring pallets in warehouses and authenticating IoT devices, RFID technology is versatile enough to be used in multiple markets.

Adoption barriers remain practical and persistent as the perceived high cost of tags and readers tops the list at 35%. Integration complexity (33%) and limited standards/interoperability (14%) point to the technical challenges of incorporating RFID into existing systems.

The modest 27% who report no challenges suggest RFID has largely matured for organizations that have implemented it. These success stories should be leveraged to build confidence among the organizations still evaluating adoption. With proven technology and product longevity demonstrated across millions of deployments globally, RFID represents a "set it and forget it" solution for organizations seeking reliable asset and inventory visibility.

How Three Industries Use RFID

According to this year's survey, Manufacturing and Industrial; Healthcare; and Software, Technology and Telecommunications are the top three industries deploying RFID technologies, with adoption spread across multiple use cases.

In Manufacturing and Industrial organizations, 37% use RFID for asset tracking and inventory management, 30% for IoT device authentication and 20% for supply chain logistics. Healthcare organizations report 39% use for asset tracking, 35% for inventory management and 25% each for supply chain logistics and IoT device authentication. In Software, Technology and Telecommunications, RFID adoption includes 32% for supply chain logistics and IoT device authentication, 28% for inventory management and 26% for asset tracking.

Trend 7

Investment Patterns Shift Toward
Integrated Platforms





Investment Patterns Shift Toward Integrated Platforms

Cross-trend analysis reveals a fundamental shift in how organizations approach security technology investment. Rather than selecting standalone solutions that operate in isolation, security leaders are prioritizing integrated platforms that deliver comprehensive capabilities, consolidate data and unify management. This evolution reflects the ongoing maturity of the industry, from tactical purchasing to prioritized strategic security planning.

The investment hierarchy is clear, with spending increases indicated in identity management solutions (60%), followed by real-time location solutions (53%) and biometrics (60%). Mobile credentials, having achieved 74% adoption/planning rates, have transitioned from investment priority to baseline expectation.

With all of these systems and technologies at play, integration complexity emerges as the universal barrier across all technologies, cited by majorities or near-majorities in every category. For identity management, 52% face complexity in managing multiple systems. For physical-digital convergence, 37% cite implementation complexity concerns. Even mature technologies like RFID see 33% struggling with integration.

The business case for platform consolidation becomes compelling when looking deeper into the challenges that come with managing multiple point solutions. Organizations report improved efficiency (44% in unified security management contexts), simplified management for faster incident response (30%) and enhanced visibility across systems (16%). These benefits multiply when identity management, access control, biometrics, real-time location solutions and RFID converge into cohesive solutions rather than requiring separate management consoles, different credential systems and manual data management.

Integrating many security solutions into a single, manageable platform remains difficult because few offerings in the industry can truly support this level of unification.

Bonus

Ethical Considerations and Privacy
Concerns at an All-Time High



BONUS: Ethical Considerations and Privacy Concerns at an All-Time High

Across technologies, privacy and ethical considerations have emerged as a trend in 2026, particularly as organizations deploy increasingly sophisticated biometric and location-tracking solutions in their security program. The data reveals a security industry grappling with the tension between enhanced protection and individual privacy rights, with end users demonstrating heightened awareness and caution.

Biometric technology implementation has brought privacy concerns into sharp focus. Among end users, 67% express high or moderate concern about the ethical and privacy implications of biometrics, with 31% very concerned and actively implementing safeguards. This represents a significant shift in organizational consciousness, moving privacy from a compliance checkbox to a central design consideration. When prioritizing biometric implementation factors, 50% of end users identify compliance with regulations among their top three priorities, underscoring the legal and ethical stakes involved.

Privacy concerns extend beyond biometrics. For organizations not deploying mobile credentials, 19% cite privacy concerns as a barrier, which is a notable consideration for technology often perceived as merely convenient, despite the fact that it is highly secure. Real-time location solutions face even more scrutiny, with 29% of end users identifying data privacy concerns as a barrier to adoption. This is particularly significant given that worker safety drives 69% of deployments, creating a tension between protecting employees physically while respecting their privacy.

The challenge of physical-digital identity convergence amplifies these concerns, with 30% citing security or privacy concerns as reasons for not integrating these systems. When a single identity platform spans both physical facilities and digital networks, the stakes for data protection increase exponentially.

Organizations are responding through active policy development, with 36% moderately concerned and considering policies around biometric use. However, the 12% who remain unconcerned suggest a segment of the market that may be underestimating regulatory and reputational risks.

As technology advances, successful security strategies must balance innovation with transparent privacy protections, clear data governance policies and respect for the individual's privacy. This means that ethical considerations might not be simply a matter of compliance, but a differentiator when making technology investment decisions.



Looking Forward

For the future of security, clear indicators signal a market that is prioritizing maturity across its identity management initiatives.

- **Mobile credentials are completing their journey from emerging innovation to standard expectation,** with a broad majority of organizations having already adopted this technology or are in the process of adopting it.
- **Biometric technology is evolving beyond its traditional MFA role into a primary access method,** supported by proven accuracy and user acceptance.
- **Real-time location solutions are shifting from specialized applications to mainstream adoption,** particularly in safety-critical industries where worker protection and regulatory compliance drive investment.
- **Physical-digital identity convergence is transitioning from exceptional innovation to expected capability,** with organizations recognizing that artificial separation between these realms creates vulnerabilities and inefficiencies.

Emerging considerations are reshaping strategic planning. AI-enhanced verification is gaining traction as organizations seek more sophisticated threat detection and authentication methods. Data privacy regulations continue to shape technology choices, particularly as single identity platforms span both physical facilities and digital networks.

The integration imperative has become undeniable. Organizations are looking ahead to more comprehensive identity management platforms that better consolidate credentials, authentication and access control across all domains. The breakdown of silos between physical and digital security is no longer a high-level goal; it's an operational necessity. Real-time data and analytics have emerged as the foundation for decision-making, enabling security leaders to demonstrate business value beyond protection to encompass operational efficiency, user experience and regulatory compliance.





Conclusion

Central to the theme of 2026 is the idea that identity management is part of an overall strategic foundation for organizations, particularly as AI fundamentally transforms both threat capabilities and defensive requirements.

Navigating between innovation and the ongoing challenge of integration, IT and security teams must grapple with the practical challenges of cost, complexity and privacy concerns.

Successful organizations will prioritize strategy around technology investments and align these to organizational goals, with success in phased implementation and partnerships with vendors and integrators who can bridge the gap between expertise and ongoing support.





hidglobal.com

North America: +1 512 776 9000
Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +44 1440 714 850
Asia Pacific: +852 3160 9800
Latin America: +52 (55) 9171-1108

For more global phone numbers click here

© 2026 HID Global Corporation/ASSA ABLOY AB.
All rights reserved.

2026-02-12-2026-security-trends-report-eb-en

Part of ASSA ABLOY