The Industry Report:

2024 State of Security and Identity

REPORT

Table of Contents

Introduction

Security is never a static proposition. Professionals across the industry and in all regions must constantly evolve their approaches, particularly as attack surfaces broaden and bad actors develop new schemes to test the resilience of both cyber and physical security.

As past trends – such as adapting security paradigms to hybrid work models – solidify into the new norm, emerging technologies are providing security professionals with new options to combat shifting threats. The rise of digital solutions, such as multi-factor authentication and artificial intelligence, are shaping a new frontier that elevates the security posture of the enterprise but also requires security professionals to modernize and level up with new skills.

We surveyed over 2,600 end users and industry partners (installers, integrators and original equipment manufacturers) across the globe whose responses helped us identify six major trends that are shaping security and identity, as well as the key enablers, disruptors and game changers that are supporting those trends.

The 2024 State of Security and Identity Report describes these trends and provides relevant information to help security teams deliver better security and greater value across their organizations.

Executive Summary

In this year's survey, end users and industry partners highlighted **six key trends** that are reshaping the security industry.

Multi-Factor Authentication Adoption Is Widespread

Mobile Identities Gain Traction in Security Applications

Sustainability Becomes Bigger Driver in Business Decisions

Biometrics Continues Its Momentum

Identity Management Points Up to the Cloud

The Rise of Artificial Intelligence for Analytics Use Cases

A Deeper Dive:

Six key trends (1-3)

Multi-Factor Authentication Adoption Is Widespread

"Please enter 12 characters, upper- and lowercase, plus a number and a special character." With these requirements, it's no wonder that 6 in 10 users admit to reusing passwords, according to security company Norton. It's also easy to see why the security industry is moving toward the eventual end of passwords with the creation of new standards such as FIDO, or Fast Identity Online, which uses "standard public key cryptography techniques to provide phishing-resistant authentication." And while passwords aren't going away anytime soon, they're increasingly seen as just one part of the authentication puzzle. As society evolves toward this "password-less" future, new and more secure authentication options are emerging. Multi-factor authentication or MFA is relatively easy to implement and can be the first step toward a more comprehensive Zero Trust strategy. An increasing level of end-user acceptance is driving rapid adoption of MFA across a broad range of industries, making it a top priority for many security professionals: 85% of survey respondents rated MFA among the most important trends for the coming year.

Mobile Identities Gain Traction in Security Applications

The ubiquity of mobile devices makes them a natural fit for extended identity applications, and the incremental adoption of mobile ID continues, with 72% of respondents calling out mobile identity as a Top 3 trend. Organizations are steadily upgrading legacy hardware in favor of multi-tech readers that can handle both plastic and mobile device-based credentials. Moreover, mobile devices are increasingly used to support MFA and other use cases across the network security landscape. End users appreciate the convenience that comes with authenticating themselves via a device they already carry, and administrators find it easier to manage identity via software. Mobile devices are less likely to be lost or stolen, and their built-in security safeguards mean that even if they are misplaced, one's identity likely won't be compromised.

Sustainability Becomes Bigger Driver in Business Decisions

There is a push and pull in the realm of sustainability. Companies are being pushed toward more climate-friendly practices by a range of government regulations and mandates, and they are being pulled in that direction by consumers' growing desire to do business with firms they perceive as sensitive to sustainability issues. In security, this is driving heightened interest in the supply chain, as professionals seek out solutions that require fewer resources, use fewer consumables and create less waste. Over half of our respondents (56%) rated sustainability as a top priority for 2024, with many companies looking to partner with suppliers who can demonstrate that they take seriously their commitment to minimizing their environmental impacts.

A Deeper Dive:

Six key trends (4-6)

Biometrics Continues Its Momentum

In support of a seamless end-user experience, security professionals continue to explore the possibilities around biometric identification — the use of attributes such as facial characteristics, voice or fingerprint for authentication. Biometrics offer a means to validate identity quickly, accurately and securely, elevating the end-user experience by combining efficiency and security. This is a developing area; there is still some concern among consumers about privacy when it comes to biometric markers. By and large, however, we're seeing continued acceptance, as people come to appreciate the exceptional convenience of authentication that can happen literally in the blink of an eye, and half our respondents (50%) this year flagged this as an area of top interest.

Identity Management Points Up to the Cloud

As emerging Zero Trust architectures are proving to elevate the security posture of the enterprise, professionals are increasingly turning to cloud-based identities. Over a third of respondents (36%) said the rise of cloud-based authentication or identity management delivered as a subscription service is an important trend right now. Such applications integrate easily with other security technologies and can be managed quickly and effectively by security teams regardless of their physical location. With a cloud-based authentication service providing direct-to-the-end-user authentication, security professionals can deliver easy enrollment and trusted authentication, even in regulated industries such as healthcare and financial services, as well as government and critical infrastructure. These services make it easy to establish, create, manage and use identities through a secure cloud delivery model.

The Rise of Artificial Intelligence for Analytics Use Cases

The AI boom is everywhere, and consumers are enthralled by the possibilities. It is no different in the security realm, where AI as a trend has emerged for the first time this year. AI promises to elevate a range of functions and drive efficiencies. AI-driven analytics in particular can give security professionals deeper, faster insights to help guide their decision-making. AI analytics tools are increasingly available right out of the box, through third-party as-a-service offerings, and 44% of survey respondents are already leveraging the power of such tools. From recognizing "out of the ordinary" user behavior to noting unusual patterns in a person's walk, AI analytics can deliver critical security information when and where it is needed.

Multi-Factor Authentication Adoption is Widespread

Multi-Factor Authentication Adoption is Widespread

The use of multiple factors for identity, beyond just username and password, continues its ascent. Consumers have adapted to this model, becoming accustomed to receiving a text message, for example, to validate their access to online banking, shopping and other services.

Some 83% of end-user respondents said their organization currently uses multi-factor authentication (MFA). For many, this represents the first step on the longer journey toward Zero Trust an overall approach to security that calls for organizations to maintain strict access controls and to never trust anyone – internal or external – by default. This strategy "requires you not to trust anything active within your IT environment," according to experts at the Cloud Security Alliance, who note that "a Zero Trust approach starts with multi-factor authentication."

Size is a factor when looking at which organizations in particular are working toward a Zero Trust authentication model. In our survey, for example, while 16% of those with over 100,000 employees and 14% of those with between 5,001 and 9,999 employees have implemented Zero Trust, just 5% of those with under 100 employees have done so. Likewise, 24% of those in the 100,000+ category are in the process of implementing Zero Trust, as are 14% of those in the 5,001-to-9,999 range, while just 9% of those with under 100 employees are on that path. (Still, it is worth nothing that 31% of those under-100 companies plan to go in that direction.)

Where Zero Trust represents a strategic shift, MFA is one of several key tactics that organizations can use to achieve that goal. MFA "is the first step to a true Zero Trust journey," the Cloud Security Alliance notes, yet "a surprising number of organizations have not yet implemented an MFA requirement to access systems and data."

While Zero Trust can seem complicated, with numerous controls and safeguards making up a holistic strategy, MFA is relatively easy to achieve. That being the case, the coming year will likely see increased adoption of security tools that support MFA, including FIDO, or Fast Identity Online, an open standard based on public key cryptography that replaces passwords with fast, secure logins powered by cryptographic credentials that never leave the user's device. By storing the private keys on the device and not on a server, FIDO prevents the keys from being breached through a single attack on the corporate network or cloud service.

As organizations look for straightforward means to advance toward their Zero Trust goals, they must prioritize robust authentication protocols and encryption mechanisms.

Mobile Identities Gain Traction in Security Applications

Mobile Identities Gain Traction in Security Applications

With mobile devices practically ubiquitous, momentum continues to build around the use of these devices in support of identity.

"Mobile ID authentication can identify a mobile phone user, reliably and securely, through a greatly simplified user experience, reducing friction for the user without compromising security," the Mobile Technology Alliance reports. "Applications in payments, government identity, and access control are likely just the beginning of a long list of services to be securely simplified via mobile identity authentication."

Our survey found that two-thirds of organizations (64%) reported some level of mobile ID deployment, with that number expected to increase to 79% within the next five years. Industry partners are optimistic in their outlook, stating that 94% of their customers will have deployed mobile IDs.

While mobile ID adoption is on the rise, there is still a perceived need for physical identity cards in some sectors, with 46% of end users saying they need a visible image on their ID badge, while 59% of industry partners report their customers also have this requirement. This tends to be industry-specific: For example, high numbers of end-user respondents in government (25%), healthcare (27%), transportation (29%) and hospitality (26%) say the need for their ID to remain visible at all times impacts their use of mobile IDs.

All are industries with a high degree of in-person interaction, or security requirements where it's especially important to visibly match the individual to a verifiable physical credential. (Imagine if a doctor's or pilot's face doesn't match the image on their ID badge.)

In many industries, however, mobile ID continues to gain traction, and for good reason. Among all survey respondents, 59% say it's more convenient for users, 45% laud its added security and 35% say it's more convenient for administrators.

"A significant value proposition for mobile ID authentication comes from a powerful combination of the convenience provided to users together with the enhanced data available from smart devices," the Mobile Technology Alliance reports.

End users don't have to struggle with multiple forms of identity, the mobile device is rarely out of reach, and administrators spend less time having to deal with lost credentials, as mobile devices are far less likely to be misplaced than conventional cards or fobs.

Sustainability Becomes Bigger Driver in Business Decisions

Sustainability Becomes Bigger Driver in Business Decisions

There is growing pressure on organizations to make sustainability a key consideration in their decision-making processes.

"When consumers are asked if they care about buying environmentally and ethically sustainable products, they overwhelmingly answer yes." According to McKinsey & Co., which notes that 78% of U.S. consumers say that "a sustainable lifestyle is important to them."

Businesses are responding, with 65% saying, "sustainability is top of mind," Forbes reports. Among HID's survey respondents, sustainability continues to rank high as a business priority, with both end users and partners rating its importance at a "4" on a 1-to-5 scale.

While that statistic is holding steady from the previous year's ranking, there's a growing emphasis, with 74% of end users saying they've seen the importance of sustainability increasing over the past year, and 80% of partners reporting the trend growing in importance among their customers.

While some undoubtedly are focused on sustainability because it's the right thing to do, external pressures are driving initiatives at the organizational level. Among end users, 43% say government regulations are a key driver, and 42% point to consumer requirements. Some 51% of installers point to government regulations and 64% cite consumer requirements.

Relating to internal pressures, this year we tried to delineate corporate culture and corporate mandate from the sustainability equation. Here the data is mixed. For example, 43% of end users say they are working under corporate sustainability mandates, yet only 36% cite corporate culture as a key driver of sustainability efforts. Among installers and integrators, the split is roughly the same: 50% have corporate mandates, while just 33% are driven by corporate culture.

This demonstrates that companies are feeling some outside pressure to build sustainability into their business decisions. In the security and identity industry, we will likely see continued emphasis on solutions that minimize energy use, reduce waste and optimize resource usage. That means a continued shift to cloud-based solutions and increased use of mobile devices, strategies that simplify and streamline security operations while reducing waste. Such efforts will enable providers to anticipate and respond to both changing societal expectations and continued regulatory emphasis on sustainability.

Biometrics Continues Its Momentum

Biometrics Continues Its Momentum

Biometrics continues to be a driving force of change in the security industry, with the ongoing adoption of physical traits such as fingerprint, face or voice as a means to ensure security, while also streamlining and simplifying interactions.

Industries' adoption of biometric solutions is on the rise, as reported in the Harvard Business Review. Authors there cite a car-share service that uses facial recognition to verify drivers, as well as hotel operators that allow biometrics in place of physical documentation upon check-in, and even retailers who use a biometric palm-scan in support of contactless payments.

As a security measure, physical characteristics "can be used in a range of ways, from checking an identity claim (for example, unlocking a mobile device using one's face), to searching databases (for example, checking whether the same person has registered for a service several times), to estimating attributes of people (for example, assessing likely age)," according to the Biometrics Institute, which promotes the responsible, ethical and effective use of these technologies.

In this year's survey, 39% of installers and integrators said some of their customers are using fingerprint or palm print, and 30% said some are using facial recognition. The momentum continues to build as 8% of end users plan to test or implement some form of biometrics in the next year and 22% plan to do so in the next three to five years.

As organizations evolve away from more conventional means of validation for access control, we will likely see the continued rise of fingerprint, palm print, facial and voice recognition as a means to validate identity.

The global market for biometrics is expected to grow from $47.8 billion in 2023 to $86.1 billion by 2028, a strong indication that businesses and end users alike are coming to accept physical traits as a safe and secure means of verifying identity. Grand View Research points to "expanding applications of biometric technology in various industries and rising demand for authentication, identification, and security and surveillance solutions" as some of the key drivers here.

Identity Management Points Up to the Cloud

Identity Management Points Up to the Cloud

Identity delivered as a service, or IDaaS, continues to grow at an average rate of 20% a year, according to experts at the Identity Management Institute.

"With the evolution of the internet and the proliferation of devices that can connect to it, our online identities have become increasingly important. At the same time, the traditional methods for managing identity information are no longer adequate," they note. "New approaches are needed to secure and manage identity information in today's digital world. Cloud-based solutions, such as Identity as a Service (IDaaS), offer a promising way to address these challenges."

Delivered as-a-service -- a centralized platform for identity data, user authentication and resource-access authorization -- the rise of cloud-based solutions for managing identity dovetails with both the shift toward Zero Trust security strategies, and increasing adoption of mobile access technologies.

As organizations look to be more attentive to what end users, applications and devices they allow on the network, while also supporting the move to mobile technologies, digital transformation in the form of cloud-based identities offers a ready means to achieve those goals.

"By centrally storing and managing identity information, these solutions can help to improve security. They make it more challenging for hackers to obtain and use this data. The providers often offer additional security features, such as two-factor authentication, which can further reduce the risk of identity theft and fraud," according to the Identity Management Institute.

Cloud-based identities helps lower the cost of managing identity information, helping organizations sidestep infrastructure investments as they look to store and manage this data. Cloud also helps with regulatory compliance, making it easier to manage and delete individuals' data when the law requires it. Cloud-based identity management is also a core component of introducing mobile IDs for use in mobile access and tenant experience applications.

Given these benefits, it's not surprising to see that nearly half of end users are moving in this direction, with 24% currently using cloud-based identity management and another 24% in the process of implementing such systems.

Industry partners say their customers face several hurdles here, including existing reliance on legacy/on-prem equipment (28%), lack of budget (24%), and cloud-based identities simply not being a business priority (21%).

As security teams look to take into account new risks in their strategies, cloud-based identities offer a way forward. Cloud-based solutions are easier to deploy, more cost-effective and generally easier to manage.

The Rise of Artificial Intelligence for Analytics Use Cases

The Rise of Artificial Intelligence for Analytics Use Cases

On Nov. 30, 2022, OpenAI's ChatGPT brought generative artificial intelligence (AI) into the public eye. Since then, conversations about AI have come to dominate the business landscape. In terms of security, many see AI's analytic capabilities as the low-hanging fruit.

AI-driven analytics "may offer greater focus and contextual insights, allowing both technical and non-technical workers to perform more efficiently," according to the International Journal of Creative Research Thoughts. With such tools, identity-management teams "can identify abnormalities and possible risks. This provides workers the knowledge they need to make the right choices."

Just 22% of end users say that are using AI to optimize the accuracy of threat detection and prediction in security programs. However, of those who are, the biggest use case is for data analytics, according to 44% of them.

Identity analytics has the potential to use AI to pore over data from a wide range of sources to rapidly unearth trends, patterns and anomalies not visible to the human eye. Such analytics can identify low- and high-risk scenarios and can help to automate risk-based decision-making.

For identity professionals, such capabilities are readily accessible in the form of software-as-a-service (SaaS) analytic products. Rather than looking to AI to inform the entirety of the security apparatus, it's possible to leverage analytics as an easy entrance point, a way to operationalize AI today in support of immediate outcomes.

Many in the security arena already are heading this way: 35% of end users surveyed report they will be testing or implementing some AI capability in the next three to five years. Some have already embraced the possibility. In addition to analytics, 11% said they are using AI-enabled RFID devices, 15% are using AI-enabled biometrics and 18% have AI supporting their physical security solutions.

Moving Forward

Security and identity are in the midst of a massive transformation, and industry professionals are challenged not only to recognize those changes but also to adjust their strategies in alignment with the current evolutions. As we look at the trends discussed above, it’s clear that there is a pressing need to adapt, deliver outstanding physical and digital experiences, and make the most of emerging technological capabilities.

Digital experiences are reshaping the way security is delivered, with cloud-supported, as-a-service offerings changing the landscape. Mobility, sustainability and AI -- the cloud makes all of these readily available, empowering more robust uses of data and helping drive optimal business outcomes. At the same time, social and economic trends continue to reshape the approach to identity, challenging those in the security industry to reconsider their core strategies.

There’s an ever-increasing expectation that in security, as in all other aspects of the enterprise, technology will be the driving force for improvement and innovation, today and in the future.

A Regional Perspective

Explore 2024 global security and identity management trends as we break down this year's survey data from different regions worldwide. From mobile IDs to artificial intelligence, we highlight the evolving landscape on a global scale.

Mobile IDs and MFA Are 2024's Top 2 Trends, with Sustainability Also a Main Focus

What three trends do you consider the most important heading into 2024? (Please select three)

	Mobile IDs Gain Traction in Security Applications	Multi-Factor Authentication Adoption on the Rise	Sustainability Takes Center Stage in Business Decisions	Biometrics Reach an Impressive Momentum	SaaS-Delivered Identities Become the Expectation
United States or Canada	73%	89%	55%	54%	36%
Latin America	86%	67%	52%	62%	33%
EMEA (Europe, Middle East or Africa)	76%	75%	64%	46%	39%
APAC (Asia Pacific)	80%	80%	71%	36%	33%

Companies with Over 50% Mobile Credential Deployments See Significant Growth Over 5 Years

What percentage of your physical access control (PAC) credentials are mobile IDs?

	51 - 75% Deployed		76 - 100% Deployed	
	Current	In 5 Years	Current	In 5 Years
United States or Canada	4%	18%	10%	21%
Latin America	8%	25%	8%	15%
EMEA (Europe, Middle East or Africa)	10%	16%	7%	27%
APAC (Asia Pacific)	9%	25%	4%	24%

A Need for a Physically Visible ID Presents a Roadblock to Mobile Adoption

What are the drivers for maintaining physical credentials?

	Need for physically visible ID (Example: badge on lanyard)	Incompatible legacy PAC hardware (Example: credential readers)	Mobile access is NOT currently a business priority	Lack of budget for mobile access	Lack of executive support for mobile access	Don't perceive significant ROI in mobile IDs
United States or Canada	**54%**	36%	32%	40%	18%	18%
Latin America	**58%**	30%	28%	35%	28%	13%
EMEA (Europe, Middle East or Africa)	**40%**	**41%**	32%	31%	20%	16%
APAC (Asia Pacific)	50%	**55%**	50%	44%	26%	14%

Multi-Factor Authentication is the Hottest Technology Currently in Use

Which of the following technologies are you currently using or planning to implement? (Select all that apply)

	Multi-Factor or Passwordless Authentication	Digital and/or Mobile Identities	Zero Trust Security Approach	IoT Capabilities for Space Monitoring and/or Health Improvement	Other (please specify)
United States or Canada	**76%**	57%	32%	20%	4%
Latin America	**52%**	61%	35%	39%	0%
EMEA (Europe, Middle East or Africa)	**75%**	75%	26%	26%	2%
APAC (Asia Pacific)	**79%**	76%	37%	29%	0%

However, Latin America Is Slower than Other Regions on the Adoption Curve

Does your organization currently utilize Multi-Factor Authentication?

	Yes	No
United States or Canada	85%	15%
Latin America	49%	51%
EMEA (Europe, Middle East or Africa)	75%	25%
APAC (Asia Pacific)	83%	17%

Cloud-Based Identity Management Struggles To Take Hold in All Regions

Is your organization using or planning to implement identity management services from the cloud (IDaaS)?

	No	Yes, we are currently using cloud-based identity management	Yes, we plan to implement cloud-based identity management
United States or Canada	**63%**	20%	18%
Latin America	**43%**	28%	30%
EMEA (Europe, Middle East or Africa)	**48%**	21%	30%
APAC (Asia Pacific)	**42%**	32%	26%

The Outlook for Artificial Intelligence (AI) is Favorable or Neutral Across All Regions, but the U.S. Has the Least Favorable Outlook

How do you perceive the emergence of AI in the Security Industry?

	Favorable	Neutral	Not Favorable
United States or Canada	35%	53%	12%
Latin America	51%	43%	5%
EMEA (Europe, Middle East or Africa)	47%	51%	3%
APAC (Asia Pacific)	50%	45%	5%

AI Has Yet To Make an Impact in Optimizing the Accuracy of Threat Detection and Prediction Capabilities in Security Programs

Is your organization currently utilizing artificial intelligence (AI) or machine learning (ML) to optimize the accuracy of threat detection and prediction in security programs?

	Yes	No
United States or Canada	**81%**	19%
Latin America	**86%**	14%
EMEA (Europe, Middle East or Africa)	**84%**	16%
APAC (Asia Pacific)	**75%**	25%

While a Majority in APAC and EMEA have Future Plans for AI in Security Applications, in North and South America the Majority Say They Have No Plans

Do you plan to test or implement AI- and/or ML-enabled security solutions?

	No, we do not have plans	Yes, within the next year	Yes, within the next 3-5 years
United States or Canada	**60%**	5%	28%
Latin America	**56%**	16%	28%
EMEA (Europe, Middle East or Africa)	42%	11%	41%
APAC (Asia Pacific)	36%	23%	40%

In Organizations that Use AI, Analytics Applications Are the Most Common Use Case

Please tell us about your use of AI in security applications.

	We use AI- and/ or ML-enabled identity analytics	We use AI- and/ or ML-enabled RFID devices	We use AI- and/ or ML-enabled biometric devices	We use AI- and/ or ML-enabled physical security solutions
United States or Canada	**47%**	15%	23%	20%
Latin America	**60%**	80%	40%	20%
EMEA (Europe, Middle East or Africa)	**39%**	17%	22%	22%
APAC (Asia Pacific)	**60%**	20%	20%	40%

By examining the trends and adoption challenges from this year's survey, you can better understand the evolving landscape and the technologies driving this evolution, helping you make informed decisions to enhance your security and identity practices.

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

2024-03-18-2024-security-trends-report-eb-en
PLT-07647

Part of ASSA ABLOY