The Industry Report:

2023 State of Security and Identity

REPORT

The Industry Report:

2023 State of Security and Identity

Supply Chain Issues Continue to be a Factor

Sustainability Becomes Bigger Influence on Suppliers and Users

Hybrid Work Environments Push Cloud-Based Access Management Further into the Mainstream

Digital ID Adoption Accelerates More Rapidly than Ever

Contactless Biometrics Reach an Impressive Momentum

Table of Contents

Introduction

We are witnessing profound changes in the security industry, and many of you reading this are an integral part of that change. Digital transformation and modernization are reshaping the landscape as we know it, driven by pressures both external and internal to the security industry. The 2023 State of Security and Identity Report chronicles the emerging keys to both sustaining and enhancing baseline operations and how to empower security teams to create more value for the organization and its people.

This year, we surveyed* over 2,700 end users and partners and took notice of five trends shaping the market and the key enablers, disruptors and game changers that are underpinning them.

This document is intended to detail the most pressing topics facing the industry in pursuit of collective and continuous improvement.

A Deeper Dive:
The 2023 Security and Identity Landscape

Executive Summary

1. Supply Chain Issues Continue to be a Factor

The extraordinary supply chain disruptions and challenges organizations worldwide have struggled with for the past several years continue to be a factor, with 71% of respondents indicating "supply chain issues" as a top trend in the security and identity industry for 2023. Similarly, 74% of respondents said supply chain issues negatively impacted them in 2022. When asked if they anticipate supply chain issues will ease in 2023, respondents provided a true split – 50% believe they will ease and 50% believe they will not. From a macro perspective, supply chain disruptions are expected to improve, although labor shortages and high demand will continue to strain global supply chains, including the availability of semiconductors. These integrated circuit chips form the backbone of many security and identity products, including control panels, readers, sensors, detectors, credentials, passports and peripherals.

2. Sustainability Becomes Bigger Influence on Suppliers and Users

There is growing consensus that governments, organizations and individuals must take more action to address environmental concerns. End users are increasingly demanding that suppliers provide footprint transparency in terms of their operations, product sourcing and research and development practices. So much so that sustainability has taken center stage in business decisions, including purchasing decisions made by end users and supplier decisions made by integrators and installers. Seventy-six percent of survey respondents indicate that sustainability is of increasing importance for their customers, with 62% stating that sustainability is "very important" or "extremely important" to their customers.

3. Hybrid Work Environments Push Cloud-Based Access Management Further into the Mainstream

Even before the pandemic, digital transformation and the convergence of physical and logical access moved more and more access management capabilities to the cloud. Now, with 81% of survey respondents offering a hybrid work model of in-office and remote work, identity management delivered "as a service" rather than via on-premises infrastructure will expand into 2023. With this adjustment, IT and security teams, particularly in smaller organizations, must consider the underlying governance that accompanies cloud-first mandates, including technology decision-making processes that incorporate engagement with audit, privacy, IT operations and information security. As an example, 67% of respondents state that MFA and passwordless authentication are most important to adapting to hybrid and remote work, with 39% indicating that data strategy, framework and tools are required components to facilitate this new work structure.

Executive Summary

4. Digital ID Adoption Accelerates More Rapidly than Ever

Digital identities are an extension of physical ones; they offer a new way to securely verify who we are so we can transact safely, work productively and travel freely. Digital IDs include mobile IDs, which are digital IDs stored on and authenticated via mobile devices. The acceleration of digital wallet adoption is expanding to use cases beyond just payments, including employee badges, drivers' licenses, national IDs and passports. To illustrate this adoption curve, 47% of integrators and installers indicate that their customers are using mobile identities for identity verification.

5. Contactless Biometrics Reach an Impressive Momentum

Modern iris and facial recognition technologies are on the rise as reliable, contactless biometric modalities for both on-premises and remote authentication. While challenges to widespread adoption of biometrics have largely centered on privacy concerns, these perceptions are starting to soften because of these technologies' convenience. Respondents indicating various stages of biometric adoption illustrate this point, with 26% stating they currently use biometrics (contact or contactless) and another 33% stating they plan to test or implement a form of biometrics within the next one to five years. This means new considerations will begin to arise within the value chain, including how to control the environment and ensure privacy as new technologies fuel speed and seamless performance.

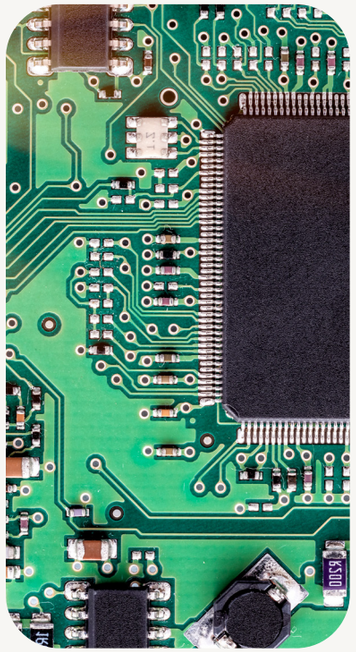
1. Supply Chain Issues Continue to be a Factor

1. Supply Chain Issues Continue to Be a Factor

When you hear the words, “supply chain,” what comes to mind? Most likely a headache. Consumers and businesses alike have felt the global supply chain stress. In fact, survey respondents indicate that supply chain issues are the number one concern, regardless of size or industry.

For example, CNBC recently reported that Boeing attributed a $3 billion loss in the third quarter of 2022 to, at least in part, supply chain issues. In fact, Boeing expects its supply chain challenges to continue through 2023.[1] And 78.3% of leading manufacturing companies cited supply chain disruptions as a main business challenge with only 10.8% believing that the situation would have improved by the end of 2022, according to the National Association of Manufacturers Q3 2022 Manufacturers’ Outlook Survey.[2]

According to our 2023 survey, 74% of respondents say they were impacted by supply chain issues in 2022, with half of them unsure if things will improve in 2023. Most affected are commercial real estate companies (CRE), with 78% citing supply chain problems as their main concern. And although organizations in the healthcare industry say that they were less affected by supply chain issues in 2022, they are still concerned that these problems will continue into 2023.



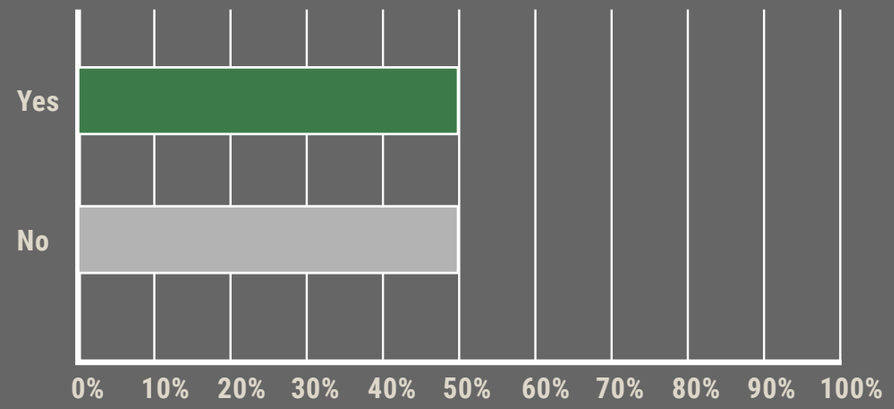
More than two-thirds of organizations with fewer than 1,000 employees indicate that they were highly impacted by supply chain issues in 2022, but they are also the most optimistic that these issues will resolve in 2023.

A persistent problem is the shortage of semiconductors, also known as integrated circuit chips or IC chips. Semiconductors power nearly everything in our digitally driven world and have become the backbone of security and identity components, including readers, control panels, sensors, detectors, credentials, passports and peripheral devices, such as printers.

Analysts identified several factors contributing to the semiconductor shortage and nearly all are linked to the COVID-19 pandemic.[4] The rollout of 5G broadband cellular technology and trade sanctions on China prior to the pandemic caused Chinese makers to place large orders for chips before the sanctions went into effect.

Pent-up demand for vehicles and other goods means manufacturing in several sectors has officially come back from early shutdowns in the pandemic. At the same time, the globalization of supply chains and vulnerable, human-driven processes added to existing labor and materials challenges. Predictions vary on how long the shortage will last.

Do you anticipate supply chain issues will ease in 2023?



Survey respondents are evenly split – 50% each – when asked if supply chain issues will improve.

Early in 2022, U.S. Commerce Secretary Gina Raimondo referred to the semiconductor shortage as a “national security” issue because manufacturing companies in the United States were at the mercy of imports of semiconductors from foreign semiconductor plants.[5]

In August 2022, President Joe Biden signed the “Chips and Science Act,” which aims to make the United States more competitive with the Chinese semiconductor industry by investing billions of dollars into domestic science research and domestic semiconductor manufacturing.[6] Still, more needs to be done.

Organizations with fewer than 1,000 employees are most optimistic that supply chain issues will ease in 2023.

2. Sustainability Becomes Bigger Influence on Suppliers and Users

2. Sustainability Becomes Bigger Influence on Suppliers and Users

In the past, security professionals tended to focus on risk mitigation: What can go wrong and what can we do about it? However, the game is changing, and security teams are now operating with additional considerations in mind. The growing consensus is that governments and organizations — not just individuals — must take immediate action to change the course of climate change.

Sustainability has taken center stage in business decisions, including the security and identity industry. End users are increasingly demanding that suppliers provide footprint transparency in terms of their operations, product sourcing and research and development practices.

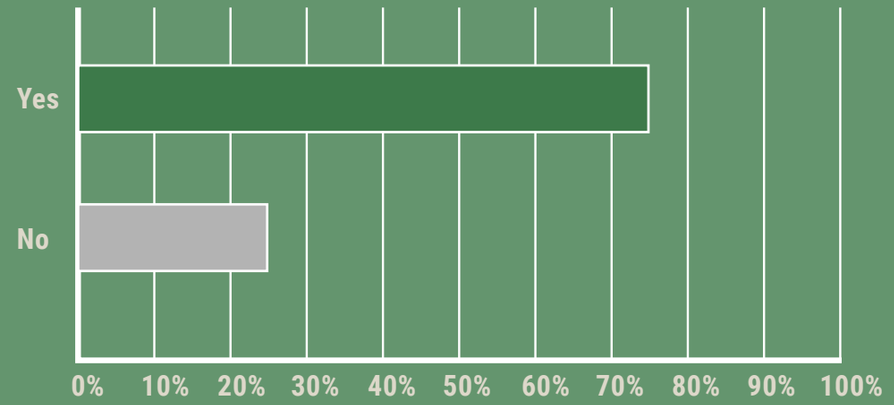
In fact, 87% of respondents to our survey say that sustainability ranks as “important to extremely important” to their customers, while 76% say they have seen the importance of sustainability increasing for their customers.

For example, 43% of companies in the financial services industry, 34% of healthcare companies and 32% of commercial real estate companies indicate that their customers consider sustainability “very important.” In addition, 31% of financial services organizations, 31% of government agencies and 27% of healthcare companies say their customers are extremely concerned about sustainability.

And according to a 2022 global innovation survey by Boston Consulting Group, two-thirds of companies ranked climate and sustainability as a top corporate priority.[7] Sustainability is no longer a value-add but a must-have practice for organizations; 80% of respondents say their customers demand it.

However, sustainability is no longer something purely driven by corporations — customers are also demanding it. In addition, today, “consumers are even more likely to prefer brands that offer robust sustainability credentials and a strong purpose,” according to McKinsey & Co.[8] And sustainability in the supply chain will be key to future operations.[9]

Have you seen the importance of sustainability increase for your customers?



Over 75% of survey respondents indicate sustainability as an increasingly important purchasing decision.

What does this mean for the security and identity industry? Forward-thinking providers know that sustainability plays an important role in technology deployment decisions. Security teams are already leveraging the cloud and IoT to deliver seamless end user experiences using connected architecture, multi-applications and mobile devices for secure access that simplifies complexities, optimizes processes and reduces resources.

As consumers urge businesses to share information on things such as energy use, waste reduction and resource optimization, organizations must define a clear sustainability strategy to be better positioned to adapt to, as well as anticipate, environmental, social and regulatory changes, both in the short- and long-term.

87%: number of survey respondents that say sustainability is “important” or “extremely important” to their customers.

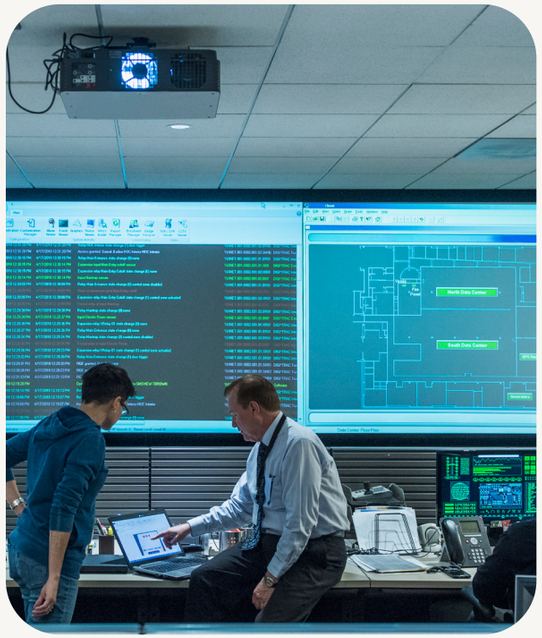
3. Hybrid Work Environments Push Cloud-Based Access Management Further into the Mainstream

3. Hybrid Work Environments Push Cloud-Based Access Management Further into the Mainstream

Digital transformation continues to exert pressure as the global pandemic accelerated the adoption of cloud technologies across many sectors. The convergence of these factors means identity-as-a-service (IDaaS) is quickly becoming the expectation.

In fact, the identity access management (IAM) market is expected to grow at a 22.7% compound annual growth rate to $41.9 billion by the end of 2031.[10] As such, SaaS-delivered identities represent huge opportunities in the security industry.

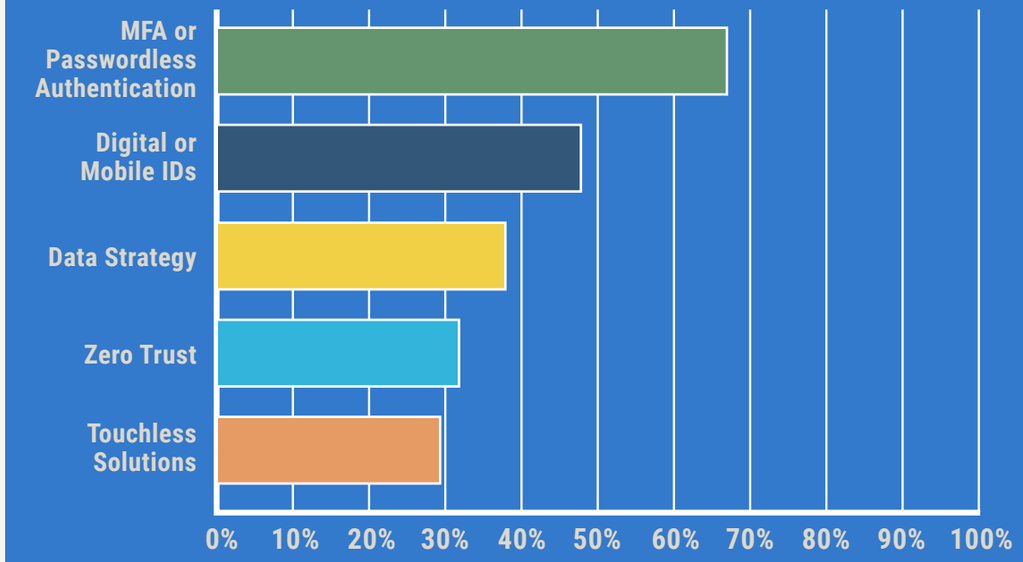
Prior to the pandemic, digital transformation and the convergence of physical and logical access caused enterprises to migrate more of their access management capabilities to the cloud. Now, as 81% of respondents to our survey say they are offering a hybrid work model, more companies will deliver identity management “as a service” rather than via on-premises infrastructure in 2023.



From organizations welcoming back their workforces and instituting hybrid models to commercial real estate firms creating frictionless tenant experiences, the right IAM tools enable identity governance and administration capabilities to manage users in response to the continued evolution of resources.

Security teams are beginning to rethink access strategies, accounting for new risks and implementing a software-based approach to IAM in the cloud. IDaaS solutions are easier to deploy, cost-efficient, adaptable and easy to manage.

What are the most important technologies or approaches needed to adapt to hybrid and remote work?



67% of respondents indicate that MFA or passwordless authentication is a top priority to enable hybrid and remote work.

Forty-three percent of government agencies and 33% of financial services companies plan to use IDaaS, while mid-size to large organizations are most likely to explore using the technology, according to our survey. As an example, 67% of respondents state that multifactor authentication and passwordless authentication are most important to adapting to hybrid and remote work, while 48% point to the importance of mobile and digital IDs. Additionally, 39% indicate that data strategy, framework and tools are required components to this new work structure.

Our survey also indicates that although partners plan to offer IDaaS, most organizations aren't quite ready to implement it yet. Consequently, partners will need to help their customers understand the value of implementing IDaaS tools to increase security and reduce costs.

Hybrid or fully-remote work models are now in place for 81% of organizations responding to the survey.

3. Digital ID Adoption Accelerates More Rapidly than Ever

4. Digital ID Adoption Accelerates More Rapidly than Ever

The concept of adding authentication to transactions isn't new, but we are seeing it evolve. In the past, identity was tied to something physical, such as a customer presenting a driver's license when paying for goods or services by check. In the modern world, trusted identity is increasingly a digital phenomenon, from passports to student IDs and corporate credentials. This is changing the way security operates. A digital ID is an extension of physical identity and offers a new way to securely verify who we are. Digital IDs include mobile IDs, which are digital IDs stored on and authenticated via mobile devices, including smartphones and wearables.

A combination of factors is driving digital IDs to their tipping point in 2023. According to our 2022 State of Physical Access Control Report, 66% of users have already upgraded to mobile readers or plan to do so, while 41% of respondents say that mobile access would be one of the top features required in a new access control system. [11]

The infrastructure to support digital transactions grew during the past two years alongside the need to offer contactless transactions. In tandem, the adoption of mobile wallet apps that house digital identities on mobile devices also grew. Digital wallets comprised 48.6% of e-commerce transaction value worldwide in 2021, or just over $2.6 trillion.[12]

In addition, digital wallets are projected to rise to 52.5% of transaction value in 2025, driven by the popularity of digital wallets from major players, such as Amazon, Apple, Google and PayPal.[13] That's because they make the online shopping experience much easier while enabling users to store multiple payment applications on a single device.

In fact, a recent PACE research conducted by FIS®, a financial technology provider, finds that 32% of mobile wallet users now have three or more mobile wallets, including Apple Pay, Google Pay, Samsung Pay and others, downloaded on their smartphones.[14] Expanded capabilities allow iPhone users to add keys, IDs and digital documents directly in the wallet app. These include, but are not limited to, drivers' licenses in eight states, verifiable COVID-19 vaccination information, employee badges, student IDs and hotel room keys.

32% of mobile wallet users now have three or more mobile wallet apps.

-FIS

According to the HID survey, Commercial real estate companies (40%) are outpacing other verticals in the use of IDaaS as large commercial real estate firms are leveraging mobile access as part of their larger tenant experience apps. For example, New York City-based Silverstein Properties offers secure contactless access to its office buildings through employee badges in Apple Wallet. [15]

In addition, organizations with more than 10,000 employees have the highest use of mobile IDs. However, implementing mobile IDs was not a top priority for healthcare companies, which made up the largest portion of this group.

The commercial real estate (CRE) vertical is leading mobile ID adoption, with 40% of CRE respondents indicating they have implemented mobile IDs.

5. Contactless Biometrics Reach an Impressive Momentum

5. Contactless Biometrics Reach an Impressive Momentum

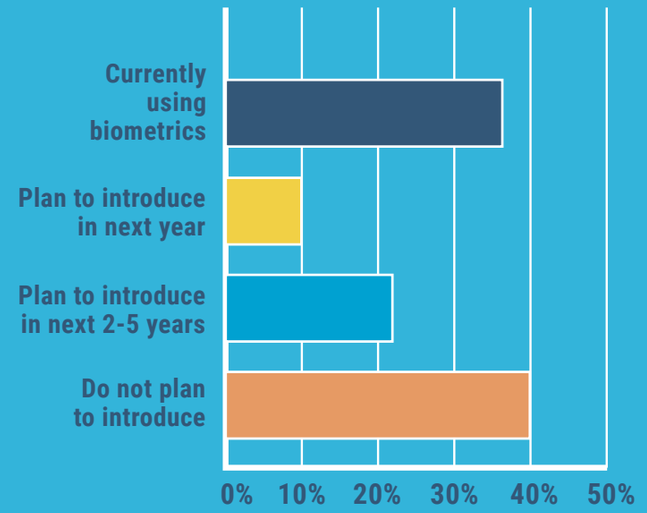
In 2023 and beyond, biometrics and cloud-based identity management solutions are poised to fuel more secure and faster interactions with technologies used to access places and experiences.

Already widely used in banking and financial services, fingerprint biometrics will expand into broader applications. Facial recognition will grow in popularity with its improved security and more seamless user identification experience. For these systems that create, delegate, deliver and present trusted identity data for access applications, biometrics will confirm that users are who they say they are, and that they are doing what was intended. In fact, biometric solutions will become the standard of today's cloud-based ID management systems.

The worldwide market for biometrics is expected to reach $136.18 billion by 2031.[16] And the global facial recognition market, valued at $3.83 billion in 2020, is predicted to reach $16.74 billion by 2030, growing at a CAGR of 16% from 2021 to 2030.[17]

Biometric technologies represent a major break from more conventional means of access control. This means there will be many new opportunities to use only our fingerprints or faces when interacting with access technologies. Approximately 59% of our survey respondents said they are currently using or plan to implement or at least test biometric technologies in the near future.

Does your organization currently use or have plans to use a form of biometrics in security applications?



Approximately 59% of respondents indicate they are currently using or plan to implement or at least test biometric technologies in the near future.

Using multifactor authentication — a key component to enable companies to achieve zero trust security — with biometrics as an additional authenticating factor (e.g., biometric scans to verify an individual's physical identity) can help organizations eliminate unauthorized access and fraud. The importance of this trend is exemplified in our survey data, which indicates that more than 67% of respondents consider multifactor or passwordless authentication to be the most important technology in the future of work transition.

According to ASIS International, biometrics "can help security systems differentiate between authorized persons and threats who have unlawfully acquired traditional keys or access-related mechanisms including PINs, passwords, tokens and other physical access devices. With biometrics, an authorized person must be present to gain access. And, it is very difficult, if not impossible, to steal another person's physiological characteristics."[18] Given these inherent advantages, it is likely that uses of biometric authentication will continue to expand.

67%: number of HID survey respondents who consider MFA or passwordless authentication to be the most important technology in the future of work transition.

Moving Forward

There is no doubt that our industry is undergoing a large amount of change. We must not only identify what is changing, but also take advantage of and evolve with the current trajectory. The unifying themes of the above-mentioned trends are the need to adapt faster, deliver exceptional digital plus physical experiences and capitalize on breakthrough innovations in solutions and services.

The digital experience is an enabler in reshaping security, with interconnected devices raising the bar of what can be secured and how. The cloud will power implementations efficiently across physical and logical footprints, elevating the value of data and facilitating servitization to drive specific business outcomes. Big-picture social and economic trends have disrupted business-as-usual, challenging the security industry to rethink the basics down to the concept of identity.

The growing expectation is that security, like all other facets of the enterprise, can and will leverage technology to work better and smarter now and into the future.

1. Boeing reports quarterly loss on problems in Air Force One, tanker programs

2. Manufacturers' Outlook Survey: Third Quarter 2022

3. Gartner Forecasts Worldwide Semiconductor Revenue Growth to Slow to 7% in 2022

4. When the Chips Are Down, Step Up

5. Secretary Raimondo Announces Results of Request for Information on Semiconductor Supply Chain

6. FACT SHEET: CHIPS and Science Act Will Lower Costs, Create Jobs, Strengthen Supply Chains, and Counter China

7. Are You Ready for Green Growth?

8. Future-proofing the supply chain

9. Future-proofing the supply chain

10. Identity-as-a-Service (IDaaS) Market is expected to grow at a CAGR of 22.7, reaching a Valuation of US$ 41.9 Billion from 2022-31, Says Transparency Market Research, Inc.

11. The 2022 State of Physical Access Control Report

12. Digital Wallets Will Dominate Global Ecommerce Payments by 2025

13. The Global Payments Report 2021

14. Consumer Ownership Of Digital Wallets Is Surging, But Will The Trend Hold?

15. Silverstein introduces employee badge in Apple Wallet for its World Trade Center employees and tenants

16. Biometrics Market Size worth $136.18 Billion by 2031 | CAGR: 13.3%: Notes TMR Study

17. Facial Recognition Market by Technology (2D, 3D, and Facial Analytics), Application (Access Control, Attendance Tracking & Monitoring, Emotion Recognition, Security & Surveillance, and Others), and Industry Vertical (Retail & E-Commerce, Media & Entertainment, BFSI, Automobile & Transportation, Telecom & IT, Government, Healthcare, and Others): Global Opportunity Analysis and Industry Forecast, 2021-2030

18. Securing the Green Rush

* The 2023 Security & Identity Trends Survey was conducted by HID in the fall of 2022.
A link to the 15-question survey was emailed globally to HID partners, end users and security and IT personnel across a range of titles and organization sizes representing 11+ industries. Results are comprised of data from more than 2700 respondents.

hidglobal.com

North America: +1 512 776 9000
Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +353 91 506 900
Asia Pacific: +852 3160 9800
Latin America: +52 55 9171-1108

For more global phone numbers click here

2023-03-01-security-trends-report-eb-en
PLT-06990

Part of ASSA ABLOY