

2024 State of Security Report from HID: Mobile IDs, MFA and Sustainability Emerge as Top Trends

1 year ago



HID, a worldwide leader in trusted identity solutions, announces its [2024 State of the Security Industry Report](#), which gathered responses from 2,600 partners, end users, and security and IT personnel worldwide, across a range of job titles and organisation sizes representing over 11 industries.

The 2024 State of Security Report delves into the underlying concerns driving upcoming innovations and the technologies that underpin them, helping security leaders to be proactive in adapting to evolving challenges. Conducted in the fall of 2023, this year's survey reveals six themes, as follows:

1. Mobile identity is expected to be ubiquitous in the next five years

Given the widespread use of mobile devices, momentum continues to build around their use in support of identity. Within the next five years, surveyed end users state that nearly 80% of organizations will deploy mobile IDs. Industry partners are even more optimistic in their outlook, stating that 94% of their customers will have deployed mobile IDs.

1. Multi-Factor Authentication is widespread, despite slow but growing implementation of Zero Trust

More than 83% of end users respondents said their organization currently uses Multi-Factor Authentication (MFA), mainly due to the vulnerabilities of passwords. For many, this represents the first step on the longer journey toward Zero Trust, an approach to security that calls for organizations to maintain strict access controls and to never trust, always verify anyone – internal or external – by default. Zero Trust has been implemented in 16% of organizations with over 100,000 employees and 14% in those with up to 10,000 employees, according to the survey.

With MFA being widespread, the eventual end of passwords is imminent. The creation of new standards such as FIDO (Fast Identity Online), which uses “standard public key cryptography techniques to provide

phishing-resistant authentication,” will pave the path to new and more secure authentication options that will be part of a more robust Zero Trust architecture.

1. Sustainability becomes a growing driver in business decisions

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. Additionally, 74% of end users indicate the importance of sustainability has grown over the past year, and 80% of partners reported the trend growing in importance among their customers.

As such, there will likely be a continued emphasis on solutions that minimize energy use, reduce waste, and optimize resource usage. A shift to cloud-based solutions and increased use of mobile devices are two clear strategies to reach these sustainability goals.

1. Biometrics continues its impressive momentum

In this year’s survey, 39% of installers and integrators said their customers are using fingerprint or palm print, and 30% said they’re using facial recognition. The momentum continues to build as 8% plan to test or implement some form of biometrics in the next year and 12% plan to do so in the next three to five years.

1. Identity management points up to the cloud

Nearly half of end users are moving to cloud-based identity management, with 24% already using it 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%).

1. The rise of artificial intelligence for analytics use cases

Conversations about AI have come to dominate the business landscape, and many security professionals see AI’s analytic capabilities as the low-hanging fruit to enhance identity management. Rather than looking to AI to inform the entirety of the security system, it’s possible to leverage data analytics as a way to operationalize AI in support of immediate outcomes. In this scenario, 35% of end users reported they will be testing or implementing some AI capability in the next three to five years, with 15% already using AI-enabled biometrics.

The full report includes additional global data and further analysis. Read it in its entirety [here](#).