# **Identity & Access Management: Overview**



**What are IAM platforms?**

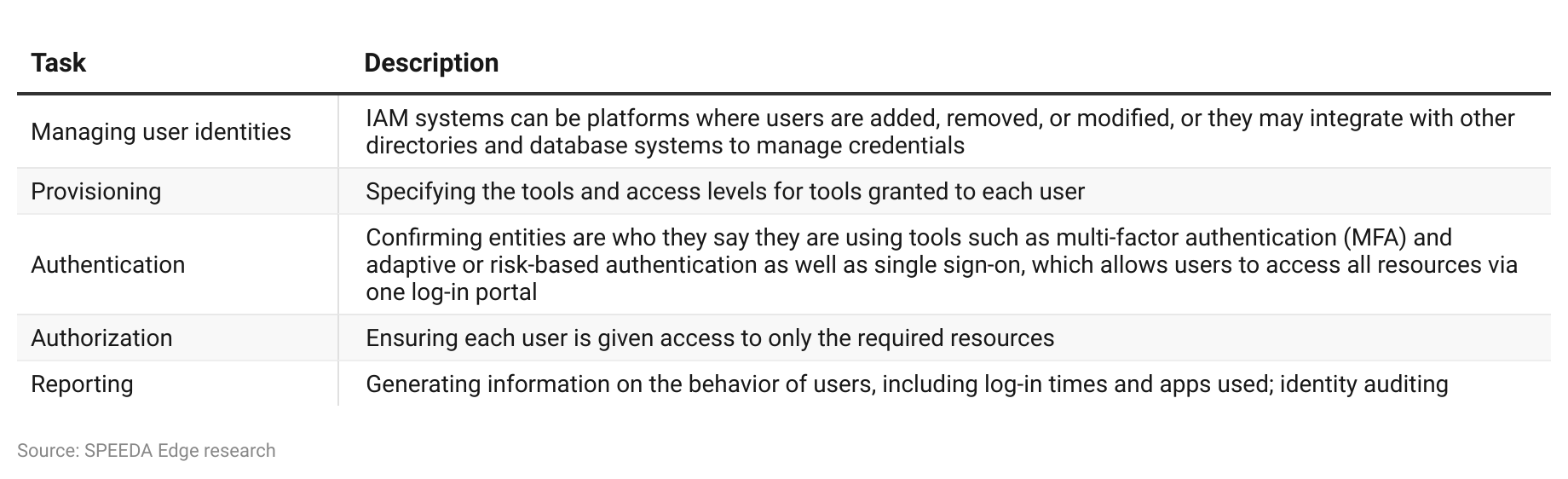
IAM comprises a framework of tools, policies, and processes used to grant the right individuals access to an organization’s resources based on the entity’s requirements and authorization policies.

Traditionally, access management has meant manually assigning an entity’s access and authorization levels to each resource. With the rise of new technologies, such as cloud computing and APIs, this process has become more complicated and error-prone, as it requires the authorization of hundreds or even thousands of entities.

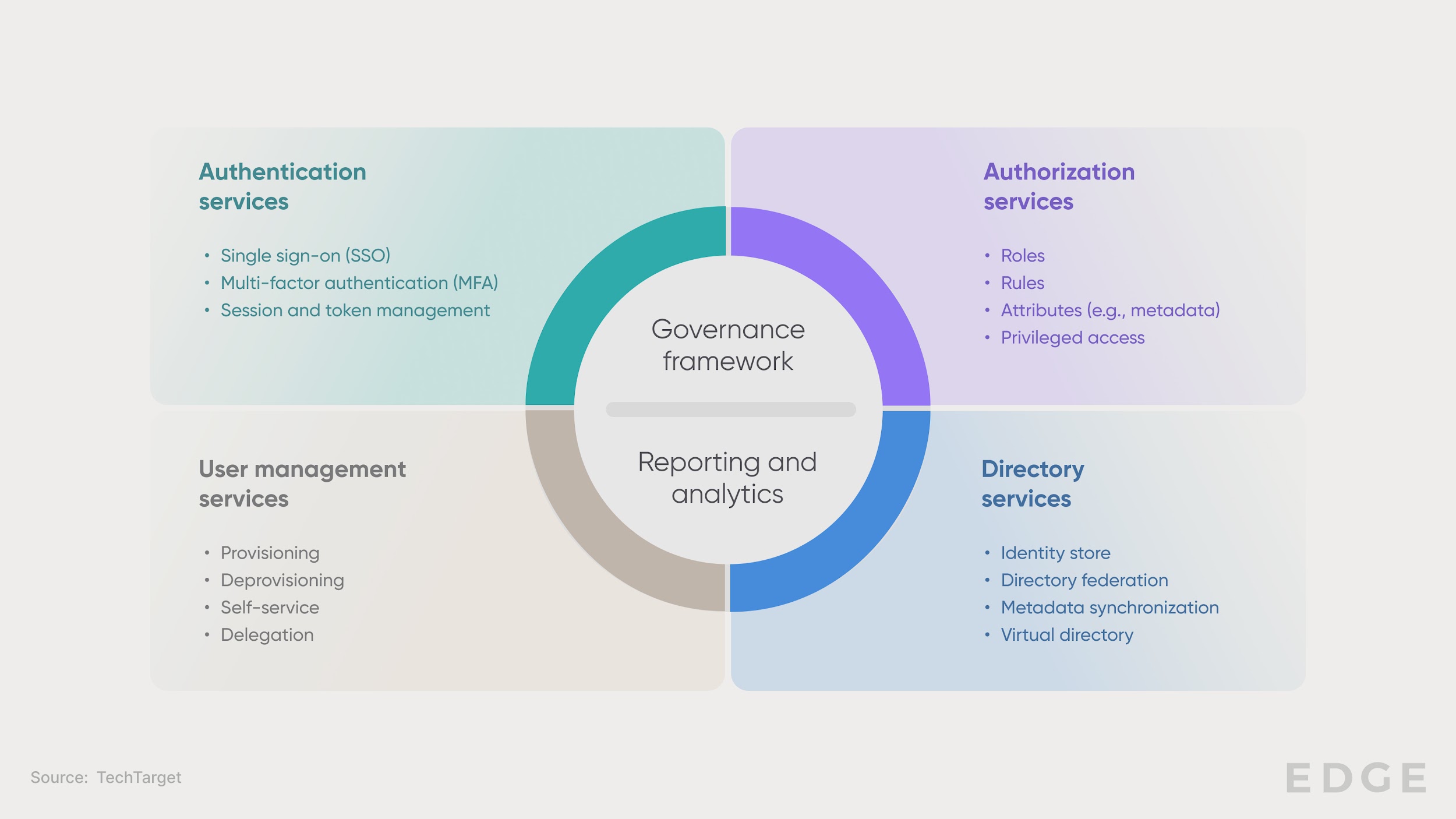
Modern tools can automate this process, enabling administrators to authorize access based on a set of rules or policies. This means that with an organization’s employee identity credentials residing in a central database, changes in access can be enforced through changing rulesets rather than access for users or applications individually. This is known as role-based access control (RBAC).

#### 

#### **What does IAM do?**

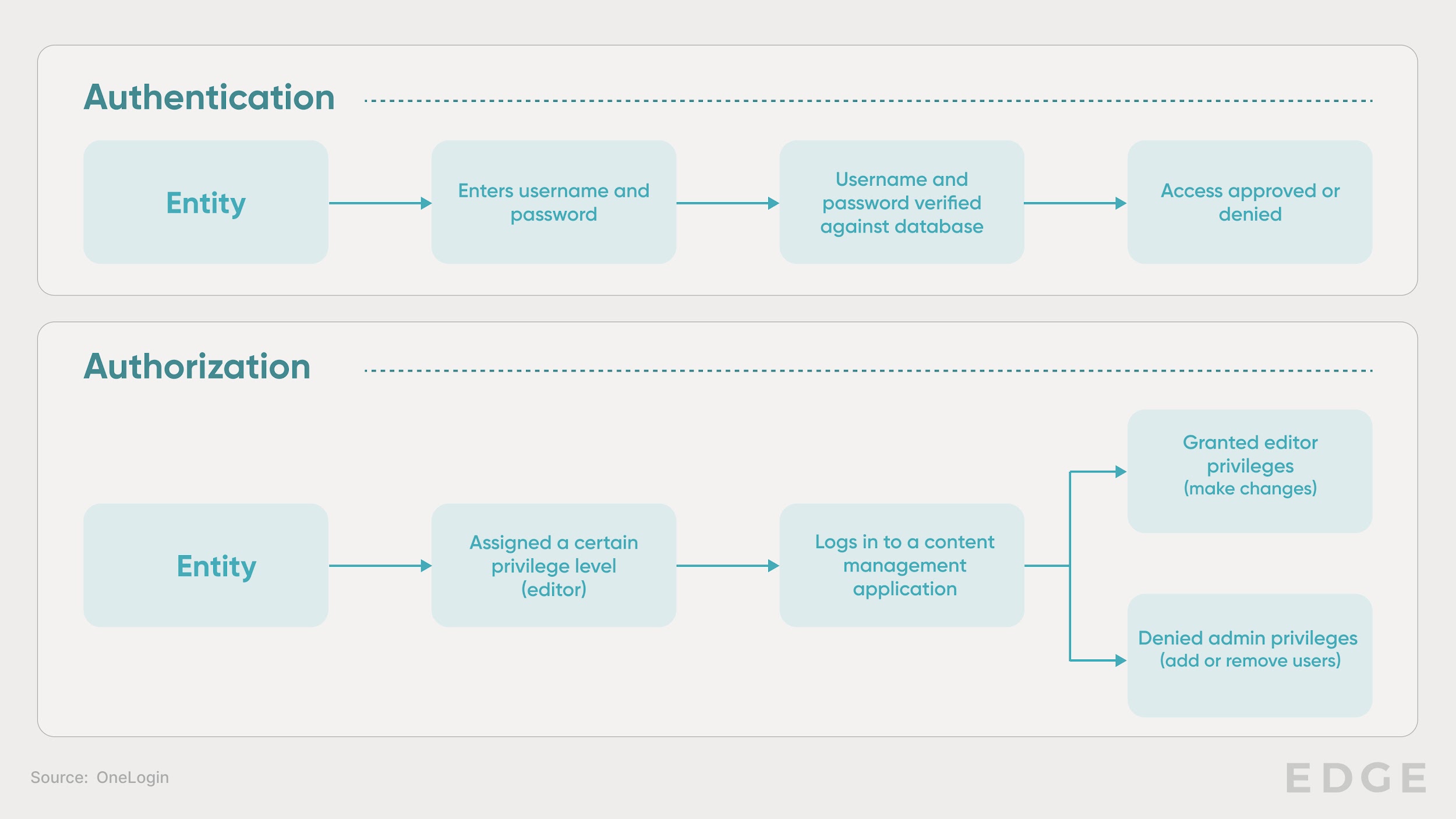


#### **Components of an IAM platform**

****

#### 

#### **Handling basic authentication and authorization in an IAM system**

****

Solutions such as multi-factor authentication (MFA) grant additional security, while governance platforms ensure easy and secure management of user credentials and streamlined authorization compared with traditional methods. Modern platforms combine some or all of this into a single interface where access, authorization, and user identities can be managed without requiring network administrators and IT teams.

#### **What technologies enable modern IAM?**

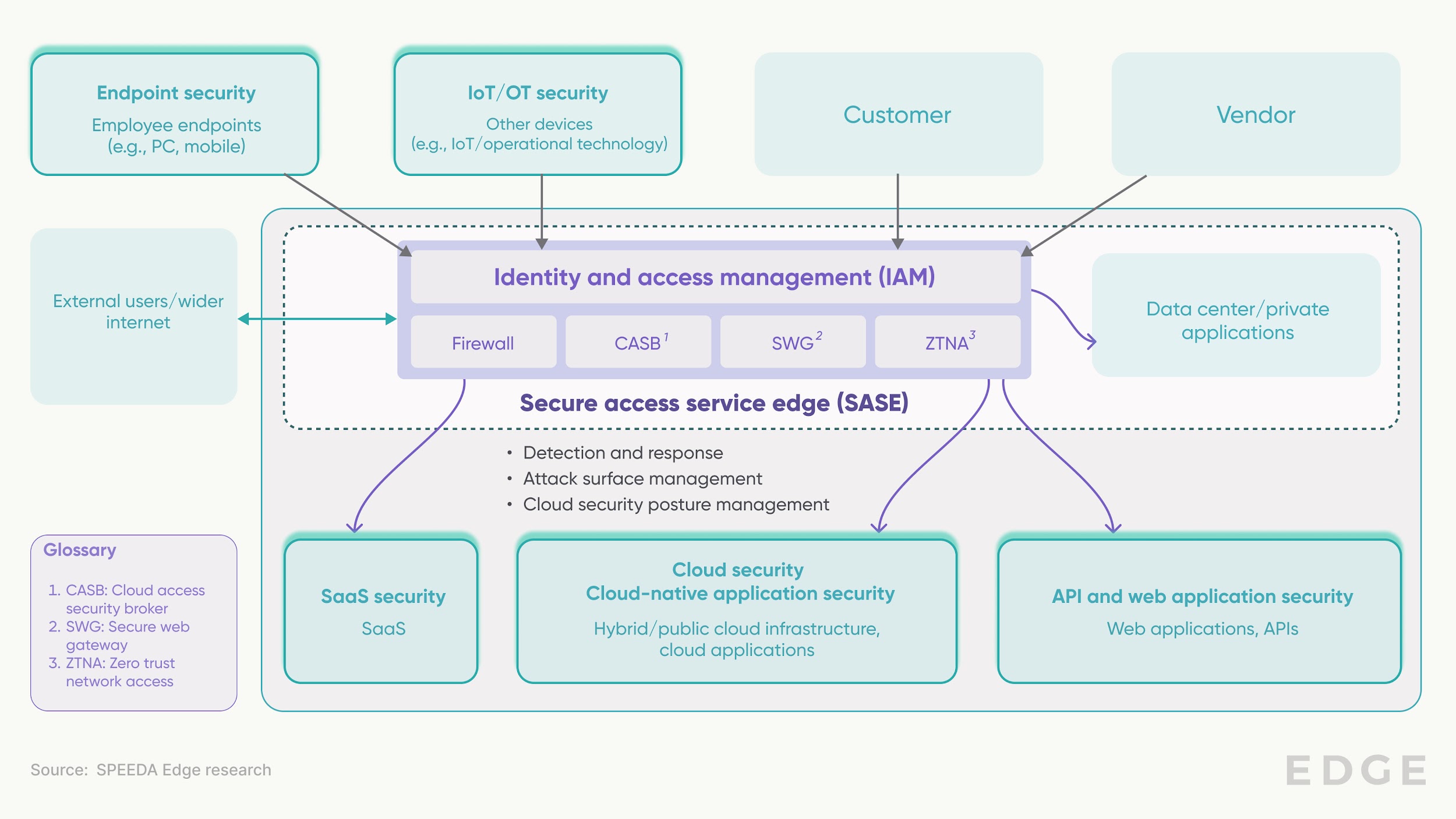
Modern tools are increasingly using AI to monitor user behavior and identify anomalies or collate various external data points to ensure each connection is secure. These systems can also adapt to the level of authentication needed, adding extra factors like biometrics depending on the assessed risk.

AI is also being used to monitor and audit identities, processes, and control policies, automating the management of user identities and policies as required by leveraging machine-learning algorithms. Biometrics add a new layer to the development of new MFA methods, moving the IAM process beyond just passwords or tokens to include the physical features of the user.

#### **How does IAM fit into the cybersecurity stack?**

IAM systems sit between any cloud-based service, on-premises application, or other resource and any entity (including an employee, customer, or device) attempting to access that service. IAM may be implemented as part of a broader cybersecurity stack, such as alongside secure access service edge (SASE), zero-trust security, or micro-segmentation, or as a standalone security solution, with various modular components being added as required. Once an entity is admitted into a network by an IAM system, traffic from the device is routed, monitored for threats, and protected by various instruments within the network’s cybersecurity stack.

#### **Where IAM sits within a typical next-gen cybersecurity stack**

****

*Refer to* [Next-gen Cybersecurity](https://sp-edge.com/industry/51) *for a market map on other verticals of the cybersecurity stack*

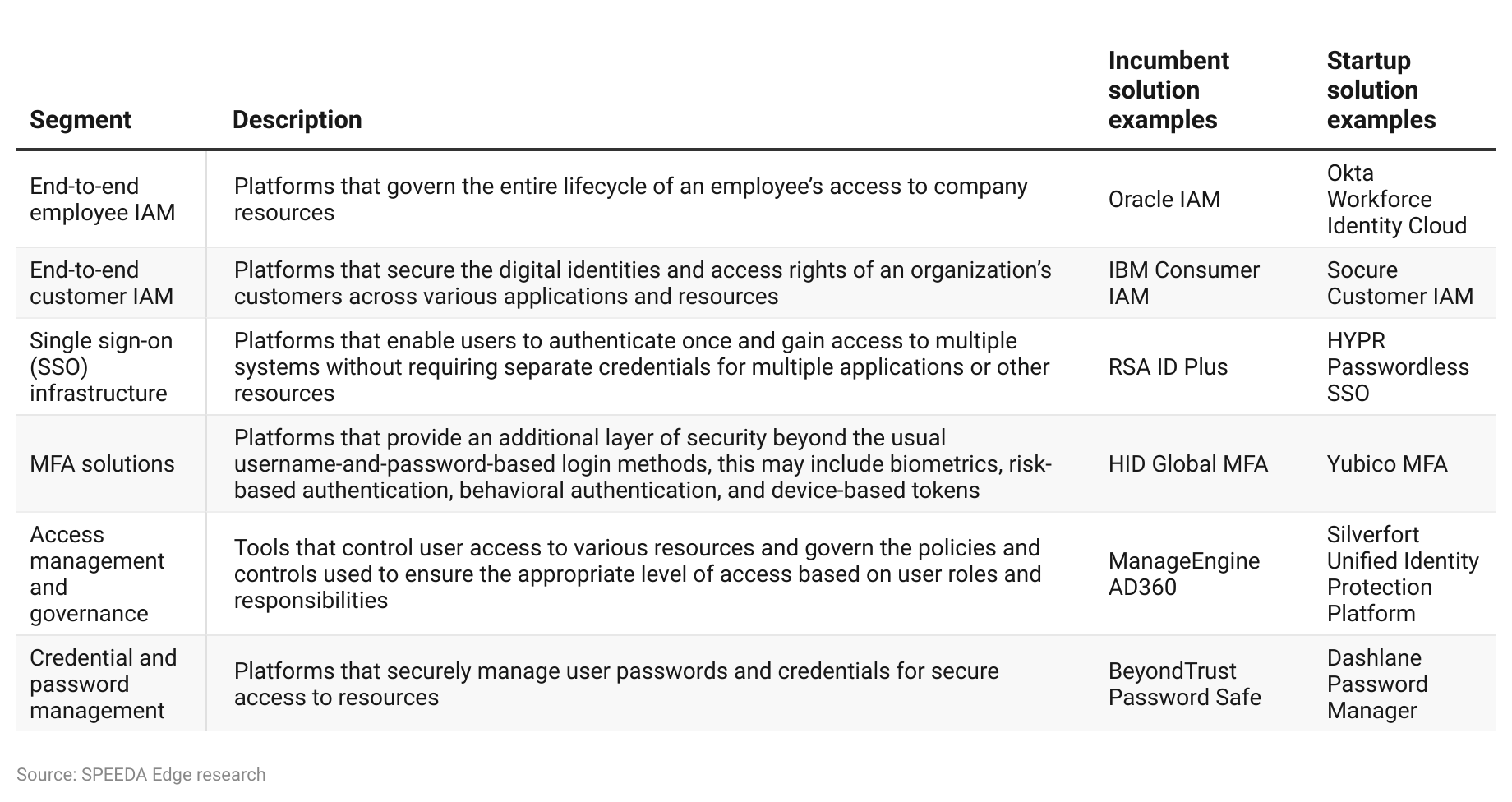
## **What does the industry landscape look like?**

IAM solutions can be divided into several categories, including the base subdivisions of “identity” and “access.” “Identity” management comprises the databases that contain user information as well as the supporting tools such as user analytics and audit and identity lifecycle management platforms. On the other hand, “access” management products typically include systems, such as MFA, which involve token-based authentication, behavioral authentication, and risk-based authentication. Capabilities such as single sign-on (SSO) are also found within this category.

Vendors within the IAM industry are divided into segments based on what products they offer. These include specific authentication technologies, identity management tools, or end-to-end identity management solutions incorporating all these elements, which focus on managing either employee or customer identities. Password and credential managers are also offered by players.

#### 

#### **Types of IAM platforms**



#### **We exclude the following areas when selecting companies for this industry:**

1. Platforms that **protect enterprise data and infrastructure in the cloud** from internal and external threats (covered under [Next-gen Cybersecurity](https://sp-edge.com/industry/51))
2. Platforms that offer tools to **ensure compliance with privacy regulations** and carry out data governance and other data security tasks associated with such compliance (covered under [Digital Privacy Tools](https://sp-edge.com/industry/34))
3. Platforms that use facial recognition technology to monitor **physical access** to offices, retail stores and residences (covered under [Facial Recognition](https://sp-edge.com/industry/16))
4. Platforms that **leverage blockchain technology to provide security and identity management solutions** for enterprises (covered under [Enterprise Blockchain Solutions](https://sp-edge.com/industry/121))

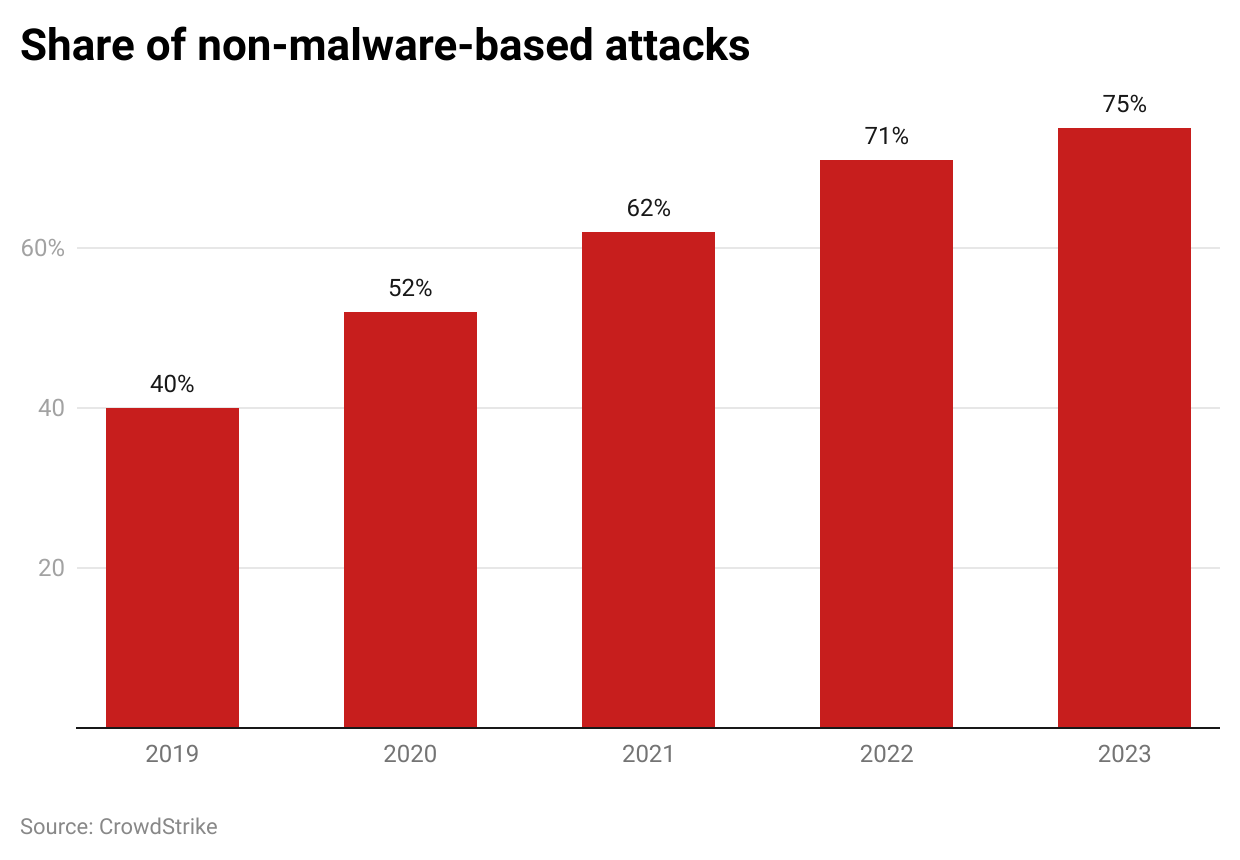
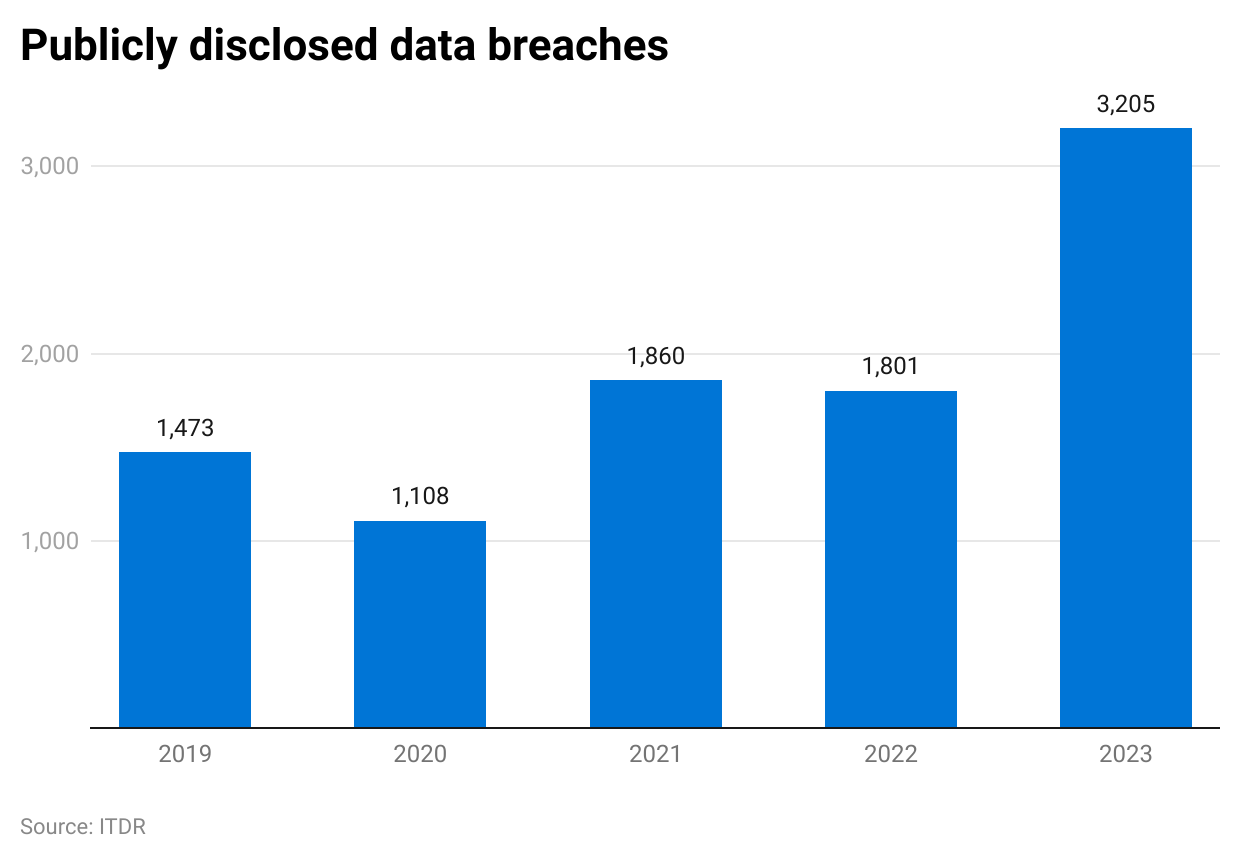
These IAM solutions are generally delivered via a B2B model, plugging into an organization’s infrastructure to securely connect employees and customers to cloud applications, information, and other resources. Pricing across the segment is mostly on a subscription basis, with customers paying per user, per month.

# 

# **Driving factors**

## **1. Data breaches due to identity theft are on the rise**

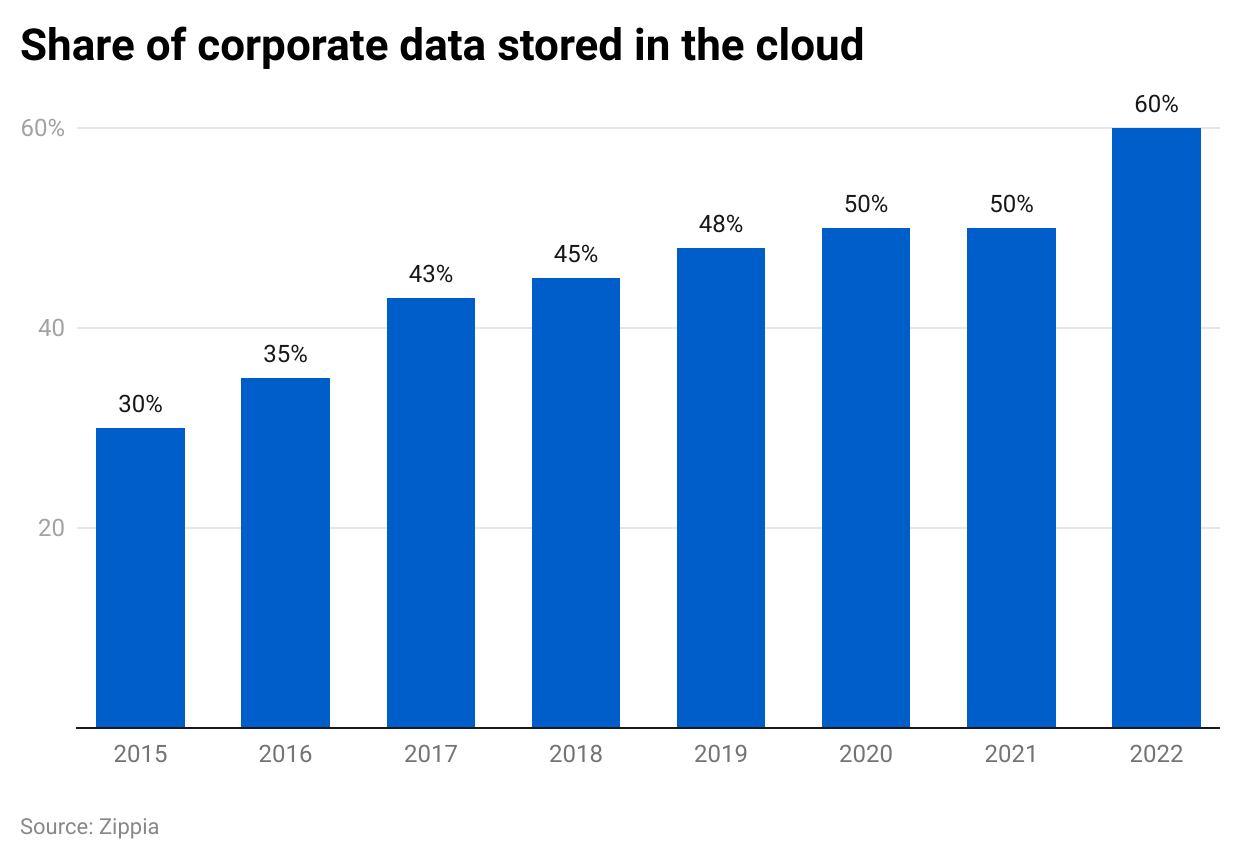
Over the last several years, there has been a general increase in cyberattacks. According to a report by the Identity Theft Resource Center (ITRC), a record 3,205 publicly disclosed personal data breaches were recorded in 2023, up 72% compared with the previous high of 1,860 in 2021, with the reported number of breach victims exceeding 350 million. A separate report by CrowdStrike states that 75% of cyberattacks in 2023 were conducted using malware-free methods, the most popular among these being phishing, social engineering, and access broker attacks—all methods leveraging identity/credential theft or manipulation.



A 2024 CyberArk survey found that one in five organizations believed a vulnerable IAM system is the most likely cause of an identity-related attack, with 64% saying they have or will prioritize identity threat detection and response (ITDR) in the next year. With 99% of cybersecurity leaders also expecting to face at least one identity-related compromise and a data breach costing an average of USD 4.45 million according to IBM, organizations that depend on complex IT systems and value the protection of their data and that of customers must invest in more secure identity protection and access management methods.

## **2. Enterprise IT infrastructure is becoming increasingly complex, making end-to-end security a challenge**

The share of corporate data stored in the cloud compared to traditional data centers doubled from 30% in 2015 to 60% in 2022. With greater connectivity between enterprise devices in IT and operational technology (OT), and as enterprises increasingly opt for cloud infrastructure and rely more on APIs and web applications, it’s getting harder for organizations to consistently monitor and protect these numerous avenues of attack.



Organizations that use hybrid cloud setups have more complex configurations, as they would need to integrate cybersecurity systems across their traditional and cloud infrastructure.

Meanwhile, over 80% of organizations say they experienced an identity-related breach due to a third-party identity or software supply chain issue. This means that with the dozens of services each employee uses for their day-to-day tasks in the modern enterprise, along with hybrid working that requires remote access to these tools, security teams must focus on providing secure and smooth access to each of these resources without compromising and interrupting workflows.

Modern IAM solutions, such as those from [Okta](https://sp-edge.com/companies/24243) or [PingIdentity](https://sp-edge.com/companies/29475), are seen as a catch-all solution to these issues, allowing centralized access provisioning and management of user identities as well as advanced MFA.

## **3. Regulatory pressures indirectly push identity security**

Though most existing regulations on the protection of personal information do not have specific clauses regarding standards of IAM and related security measures, regulations like the GDPR and HIPAA stipulate that organizations must take reasonable steps to ensure private data remains secure. IAM is therefore fast becoming an important part of an organization’s compliance framework.

This is also becoming popular across segments that value the security of data and the privacy of customer records, driven by potential business losses and regulatory requirements. In 2023, 725 health data breaches were reported under HIPAA, with over 133 million records exposed. This trend will likely drive organizations bound by laws such as HIPAA and the EU GDPR to implement IAM systems.

The effect of modern IAM solutions on compliance is twofold. Firstly, it secures the log-in details of consumers using advanced measures such as MFA, ensuring attackers will not easily be able to access customer accounts and the personal information stored within. Secondly, it ensures employees and other entities within the organization with access to sensitive information will be securely connected to necessary resources and only have access to the information required to complete their tasks, reducing the risk of intrusions and data breaches.

# **Risks to growth**

## **1. User perceptions that IAM requires extra work hinder adoption**

Setting up a unified IAM system from scratch or even converting a basic system requires a lot of effort. It needs multiple integrations between the IAM system and existing applications and infrastructure, data migration, and even employee/customer buy-in to undertake the possible extra steps required by MFA and access governance systems.

IAM is also far from static—constantly evolving and requiring IT and security teams to audit user identities and permission levels. In cases where additional maintenance or any security-related steps are required, certain organizations or individuals may find the added level of security not worth the investment of time, money, or effort. For example, 61% of organizations only apply privileged access protocols to “human” identities, disregarding machine identities, which could potentially make an entire ecosystem of IoT/OT devices in a company’s corporate network vulnerable.

Though in reality, migrating to a unified, centralized IAM system may save time in day-to-day tasks across an organization, security teams will have to justify the implementation of such security systems against the initial setup, management, and maintenance required to keep it operational.

## **2. Lack of skilled workforce is a challenge across the cybersecurity vertical**

Across the cybersecurity industry, the implementation and operation of advanced security measures are being held back by the lack of skilled workforce. In 2023, 68% of organizations reported staffing as the number one factor holding back their security efforts, with over 56% reporting they would require at least five additional full-time employees. This difficulty extends to IAM as well, as it may require additional resources to manage systems and implement policies and processes.

*Last updated: June 2024*

©2024 Uzabase, Inc. All Rights Reserved. The information contained herein: (1) is proprietary to Uzabase Inc. and/or its content providers; (2) may not be copied or distributed; and (3) is not warranted to be accurate, complete or timely. Neither Uzabase Inc. nor its content providers are responsible for any damages or losses arising from any use of this information.