SailPoint

Interactive Book

Identity security fundamentals

An interactive introduction to identity security

Start your journey now →

Introduction

Providing fast, accurate access to digital resources for those who need it is essential for organizations to secure the business and gain a competitive edge. Yet businesses are facing unprecedented security challenges with more sophisticated cyber threats and growing privacy regulations.

These are challenges that only identity security can address today. **Identity security** (also known as identity governance and identity management) protects organizations by discovering, managing, and securing technology access for a diverse set of digital identities. Identity security pays the ultimate dividend: freeing your workers to focus on innovation, collaboration, growth, and productivity while keeping your business secure.

Let's begin →

Whether you are new to identity security or just looking for a quick refresher, this eBook will review the fundamentals of identity security and discuss how identity security best protects critical assets and systems from cyberattacks and helps organizations ensure regulatory compliance.

Identity landscape

Identity security categories | Identity security foundations

Traditionally, categories associated with identity security have included:

Identity and Access Management (IAM)

Identity and Access Management (IAM) is a specialty discipline within identity security designed to automate the assignment of access and ensure only the right people have specific, fine-grained access to the appropriate data and applications at the right times and for the right reasons.

Identity Governance and Administration (IGA)

Identity Governance and Administration (IGA) extends IAM to allow organizations to improve and automate their processes to validate least-privileged access, ensuring access is appropriately reviewed and separation of duty policies are implemented and enforced, providing accountability, transparency, and risk mitigation in order to meet compliance mandates and other audit needs.

Privileged Access Management (PAM)

Priviledged Access Management (PAM) is a subset of IAM that focuses on protecting accounts of privileged users who need access to backend systems, databases, and other places, typically controlling access to administrative accounts and access rights.

Access Management (AM)

Access Management (AM) focuses on authentication and grants identities access to your applications via methods such as: Single Sign-on (SSO) or multi-factor authentication (MFA).

It's important to note that while an important part of an identity strategy, access management alone is not enough. What separates IAM from AM is the ability to provide access to not just the application but provide fine grained controls over what specific data a user can access.

For more information

- IAM vs. PAM
- What is IGA?
- Why access management alone is not enough

Identity landscape

Identity security categories | Identity security foundations

Authentication

Authentication in identity and access management is the process of verifying someone is who they say they are and is accomplished through **credentials** like passwords, one-time personal identification numbers, biometrics, and other information provided by the user. Note: Passwords that are habitually reused, shared, or easily accessible are especially vulnerable to compromise.

Authorization

Authorization in identity and access management is the process of specifying which fine-grained access rights a user has to applications, systems, data, and tools; and the actions a specific user is allowed to take within them (read, write, delete, etc.). Once defined, access is **provisioned and governed accordingly.**

Authorization must be designed to support the **principle of least privilege** in which users are granted only as much access as they require to perform their job, nothing more. This is done through judicious administration of permissions.

Strong identity security depends on how authentication and authorization are implemented. Once someone acquires authenticated credentials (whether maliciously or through error), they gain access to resources the identity is authorized to use.

An identity security program must enforce strong access policies based on the identity lifecycle, as well as integrate with advanced authentication solutions (such as MFA and adaptive authentication) as part of their larger identity security initiatives.

For more information

- What is the difference between authentication and authorization?
- Top five password management best practices

Managing access

Managing and securing identities and their access

Provisioning access throughout the identity lifecycle

Because of the value of its **digital resources**, an organization needs to know who or what currently has access to their applications, systems, and data; who is seeking access to them; and be able to track their digital activity and behavioral patterns based on their users.

These users also known as **digital identities** may be human (including employees and non-employees such as contractors, contingent workers, partners, 3rd party suppliers, etc.) or machines (robots, IoT/OT devices, APIs, microservices): basically anyone or anything accessing an organization's digital resources. Despite their differences, identities share one thing in common: they have access to your data which is a very compelling reason to control their access and their identity lifecycle.

A digital identity is tied to an individual user's attributes which change over time. A good example of this is Personally Identifiable Information (PII) such as name and government ID as well as information related to the **role** they play. This helps inform the kind of access the user should be authorized to have.

A strong identity security program with insight to the latest information on users must be in place to govern identity processes. It is essential to protecting organizations against cyber-attacks and ensuring they remain in compliance with privacy and security regulations.

For more information

- Digital identity: What is it?
- What is identity and access management (IAM)?
- What is identity security?
- History of identity management

Managing access

Managing and securing identities and their access

Provisioning access throughout the identity lifecycle

User **provisioning** is a process that spans the **identity lifecycle**. User provisioning is initially activated when new users are **onboarded**, their identities are created, and authorization to access multiple digital resources is defined. This results in the creation of accounts and the required access rights given to digital resources. Digital resources may be located on premises, in the cloud, or in a hybrid environment.

As user roles and business needs evolve over time, provisioning must change appropriately to ensure users continue to have access to the right resources and are using them appropriately. When users change positions, access associated with their previous position needs to be removed immediately to limit the risk of fraud and limit exposure in case of breach. Access to resources needed for their new position must also be given in a timely manner to ensure worker satisfaction and productivity. At the end of the identity lifecycle, **deprovisioning** removes a user's access rights and deletes accounts associated with the user, reducing the opportunities for attack and error.

A key component of an identity security program, identity provisioning must be fast, accurate, and thorough, leaving no unused identities, including orphaned or dormant accounts, with access in place. That level of speed and comprehensive monitoring is impossible without automated provisioning based on role, workflow, or rules created for accounts. Integration with directories, applications, and other identity security tools is also essential.

For more information

- What is user account provisioning?
- Overview of identity provisioning
- Best practices for onboarding and offboarding
- What is deprovisioning?

Strengthen security

Controls that tighten security in identity and access management

Managing risk in identity security

As organizations expand their digital transformation to achieve their goals, the number of identities generated and their points of access—complex and ever changing—continue to escalate. Provisioning access must keep pace with this growth without sacrificing security.

A strong identity security program leverages all three of the following controls:

Zero trust

Zero trust is an IT security framework that requires all identities to have their authentication and authorization verified continuously, whether the user is inside or outside the enterprise's network, prior to and while accessing data and applications.

Least privilege

Least privilege, a key principle of zero trust, ensures users across the organization only have fine-grained access within the data stores and applications they need, and only for as long as they need them, controlling the size of the attack surface. Along with micro-segmentation, least-privilege minimizes lateral movement during an attack.

PAM integration

Integration with privilege access management processes that monitor, track, and create alerts on the behavior of users authorized to access higher value resources where a breach would be catastrophic. This includes administrators who must have deeper and broader access for implementation, maintenance, and updates.

For more information

- Identity and access management security checklist
- Zero trust security guide: What is zero trust?
- Zero trust & micro-segmentation explained
- What is privileged access management?
- Identity access management (IAM) vs. privileged access management (PAM)

Strengthen security

Controls that tighten security in identity and access management

Managing risk in identity security

To protect against cyber threats and penalties from regulatory non-compliance, identity security must be consistent with an organization's **governance, risk, and compliance (GRC)** framework, including:

- Rules, policies, processes, and procedures that govern decisions made in managing identity and access;
- A continuous process for identifying, evaluating, analyzing, and minimizing the adverse effects (risks) from suboptimal identity security and governance;
- Adherence to the rules of maintaining regulatory and government compliance, including protecting sensitive data and applications critical to business continuity.

A strong identity security program will help organizations:

- Know where all sensitive files are stored;
- Promptly detect inappropriate access, policy violations, or weak controls;
- Verify that the right controls are in place for regulatory compliance;
- Easily audit access certification and remove over-privileged or unused access;
- Demonstrate consistency in managing access authorization;
- Monitor for malicious activity, and automatically take corrective action in real-time.

For more information

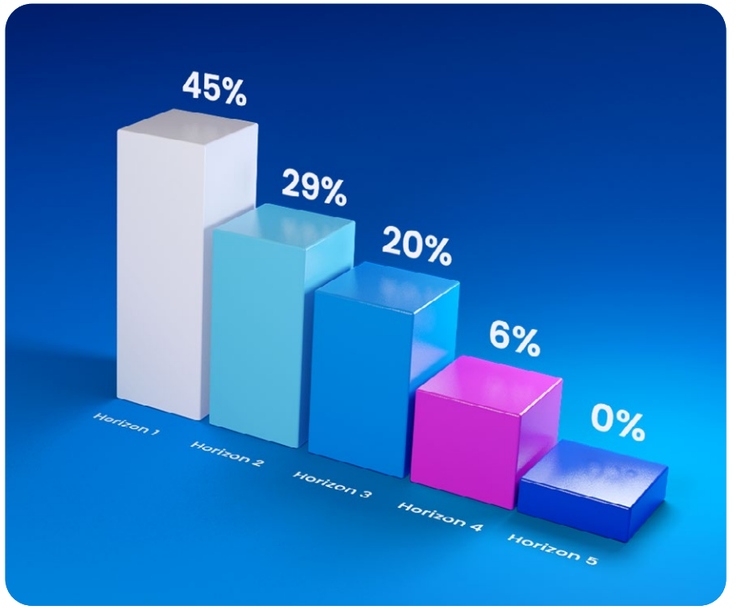
- What is governance risk and compliance (GRC)?
- What is identity governance and administration (IGA)?
- Discover how to mitigate risk with identity securtiy

Assess your maturity

Creating a mature identity security program has a strategic impact on almost every threat vector in your business, protecting all business applications, infrastructure, and critical data in every department across the organization.

Case in point: To increase flexibility and boost competitiveness, organizations have eagerly embraced growing and diverse populations of consultants, partners, vendors, and other contingent labor, as well as non-human technologies like service accounts, bots, and smart devices. But in leveraging these third parties, all with very different access profiles, levels of control, and stakeholders responsible for them, organizations may not have the right identity security program in place to manage the new operational challenges and expanded attack surface that can dramatically increase their cyber risk exposure.

In fact, most organizations are still at the beginning stage of their identity journey with immature capabilities and technology that is fragmented. They still rely on manual processes and are not yet leveraging artificial intelligence and machine learning (AI/ML) technologies that can address today's level of threat and compliance. Additionally, opportunities for integrated identity security processes and tools may not have been fully explored.



A mature, future-looking identity security program has value beyond protecting the organization's resources. It serves as a critical control point for risk management and resilience that support an organization's broader innovation strategy and collaboration with external ecosystems.

For more information

- 7 best practices for identity security
- Horizons of identity security
- How mature Is your identity security strategy?

Now that you have reviewed the basics of identity security, download the Use Cases and Best Practices eBook to dig deeper into how a strong identity security program helps you:

- Mitigate risk from cyberattacks and malicious insiders
- Comply with government and industry regulations
- Improve IT efficiencies and save costs using automation and insights
- Quickly come up to speed on the latest technologies enabling best practices in identity security

SailPoint

About SailPoint

SailPoint is the leading provider of identity security for the modern enterprise. Enterprise security starts and ends with identities and their access, yet the ability to manage and secure identities today has moved well beyond human capacity. Using a foundation of artificial intelligence and machine learning, the SailPoint Identity Security Platform delivers the right level of access to the right identities and resources at the right time—matching the scale, velocity, and environmental needs of today's cloud-oriented enterprise. Our intelligent, autonomous, and integrated solutions put identity security at the core of digital business operations, enabling even the most complex organizations across the globe to build a security foundation capable of defending against today's most pressing threats.

sailpoint.com

IB2284-2306