



# AVOIDING A **BREACH** WITH AUTOMATED IDENTITY INTELLIGENCE



# TABLE OF CONTENTS

<b>Welcome to the Elephant in the Room!</b>	<b>03</b>
<b>Introduction</b>	<b>04</b>
Identities and Privilege Make the IT World Turn	<b>04</b>
Non-Human Identities	<b>05</b>
<b>Challenge</b>	<b>06</b>
The Risks Surrounding Mismatched Identities	<b>06</b>
Potential Damage from High-Risk Accounts	<b>07</b>
What an Identity-Based Attack Can Look Like	<b>08</b>
The Complex Identity Landscape	<b>09</b>
<b>Identity Intelligence</b>	<b>10</b>
Identity Intelligence and Why It's Important	<b>10</b>
Key Components of Effective Identity Intelligence	<b>11</b>
<b>Solution</b>	<b>12</b>
How SPHERE Helps	<b>12</b>
Key Features and Benefits	<b>13</b>
Why SPHERE Is Different from What You Have	<b>14</b>
Create Visibility	<b>15</b>
Establish Ownership (a.k.a. Find the Human)	<b>16</b>
Automate and Integrate for Scale	<b>16</b>
Learn More About SPHERE	<b>17</b>
<b>Glossary</b>	<b>18</b>

Introduction

Challenge

Identity Intelligence

Solution

Glossary

# WELCOME TO THE ELEPHANT IN THE ROOM!

You have in your hands a guide designed to call out the elephant in the room—a topic that’s too important to be ignored but maybe isn’t getting the attention it deserves.



## INTRODUCING THE ELEPHANT

### Avoiding Breaches with Automated Identity Intelligence

Identity is the new security perimeter when considering how to protect your company, your assets, your people, and your customers. We’re excited to bring you important insights into the technology space and elevate the importance of identity intelligence to prevent data breaches and improve overall security posture.

This guide is powered by Exact Market research and created in collaboration with SPHERE.

SPHERE Contributors:

**Rosario Mastrogiacomo**  
Chief Strategy Officer, SPHERE

**Ken Grohe**  
President, LeverageGTM, Inc.

Introduction

Challenge

Identity Intelligence

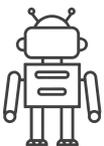
Solution

Glossary

# INTRODUCTION

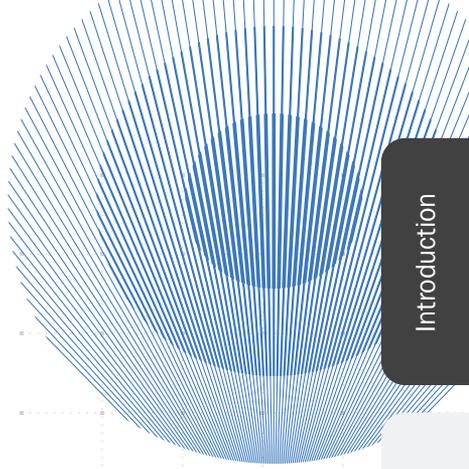
## Identities and Privilege Make the IT World Turn

Privileged access accounts and credentials are the keys that unlock digital and innovation services. If you don't live and breathe account management, it can be helpful to get a foundational understanding before learning about the potential risks that can lead to a data breach.

<b>The Who: Identity</b> An identity is a unique human or machine (i.e., non-human) account that utilizes credentials to access resources or perform tasks. Most users and entities have multiple accounts; some accounts are leveraged by multiple users.		<b>The How: Privileged Accounts</b> Accounts have credentials that provide access to and the ability to interact with various systems. Privileged accounts provide elevated access to sensitive or restricted resources.
<b>Unique Human User</b> 	<b>Example Users</b> <ul style="list-style-type: none"><li>• Domain administrators</li><li>• Server administrators</li><li>• IT experts</li><li>• Business users</li><li>• Developers, DevOps</li></ul>	<b>Example Access and Actions</b> <ul style="list-style-type: none"><li>• Root or superuser</li><li>• Admin access to manage upgrades, modify settings, perform maintenance</li><li>• Access to SaaS or web applications</li><li>• Access to cloud or software development tools and services</li></ul>
<b>Unique AI Entity</b> 	<b>Example Entities</b> <ul style="list-style-type: none"><li>• AI agents</li><li>• AI models</li><li>• Bots</li></ul>	<b>Example Access and Actions</b> <ul style="list-style-type: none"><li>• Accounts that run applications, services, and scheduled tasks</li><li>• Automated workflows using RPA or AI to mimic human actions</li><li>• Systems within DevOps toolchains</li></ul>
<b>Unique Machine Entity</b> 	<b>Example Entities</b> <ul style="list-style-type: none"><li>• Service accounts</li><li>• API keys</li><li>• Machine identities</li><li>• OAuth tokens</li><li>• Robotic process automation (RPA)</li></ul>	

# Non-Human Identities

Non-human identities (NHIs) represent a growing—and underestimated—base of machine entities, driven to greater numbers from accelerated cloud and AI adoption. But are NHIs creating risk? A recent CyberArk report showed that 88% of respondents incorrectly assumed that a “privileged user” applies solely to human identities.<sup>1</sup>



Introduction

Challenge

Identity Intelligence

Solution

Glossary

**42%**

**Among machine identities, 42% have privileged or sensitive access.<sup>1</sup>**

**82:1**

**There are 82 machine identities for every human identity.<sup>1</sup>**

**2X**

**Machine (and human) identities are expected to double in 2025.<sup>1</sup>**

**The truth is:** Machine identities are mostly unknown and uncontrolled within organizations and often require elevated access to platforms and data, creating new levels of potential risk.

# CHALLENGE

## The Risks Surrounding Mismanaged Identities

Your organization's collection of identities and privileged accounts should be viewed as its own threat landscape. Many in the industry consider identity to be the new security perimeter.<sup>2</sup> In fact, Gartner predicts that by 2027, 70% of organizations will combine data loss prevention and insider risk management disciplines with identity and access management (IAM) context to identify suspicious behavior more effectively.<sup>3</sup>

Mismanaged accounts create an open door for cyber attacks. To close security gaps, accounts and groups (collections of accounts created by admins to simplify permission and access management) must be discovered and profiled for risk and managed accordingly. Gaps include:



### Unmanaged or unknown accounts

Active accounts outside the purview of account management or security systems



### Overshared

Many people sharing credentials of a single account muddying ownership and increasing risk



### Non-compliance

Accounts not protected according to company policy or regulations



### Heavily nested groups

One group is a member of another group, making it difficult to trace and manage entitlements



### Over-permissioned

Users (or entities) with access to accounts that grant greater privileges than they need



### Empty or stale groups

Groups that have been inactive or empty for an extended period or are no longer needed



### Circular membership

Groups nested inside each other in a loop, making it hard to enumerate and track true membership

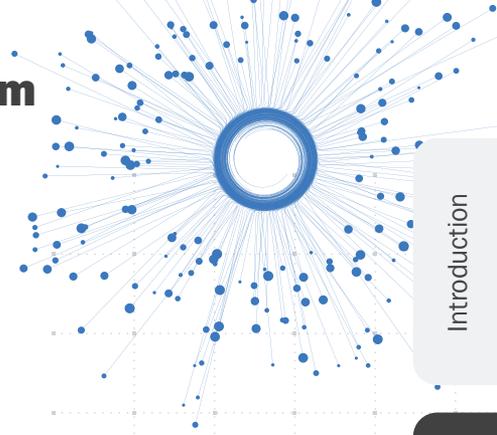


### Missing ownership

Accounts or groups that no one is responsible for, creating potential for being mismanaged, misused, forgotten, or misconfigured

# Potential Damage from High-Risk Accounts

Privileged accounts and credentials are necessary but become a high-risk liability if they fall into the wrong hands. When that happens, the damage can be extensive.



Introduction

**87%**

**A majority of organizations experienced at least two successful identity-centric breaches in the past 12 months.<sup>1</sup>**

Challenge

**USD 4.88M**

**The average cost of a data breach in 2024—10% higher than the previous year.<sup>4</sup>**

Identity Intelligence

**30%**

**Identity-based attacks make up nearly one in every three intrusions.<sup>5</sup>**

Solution

**292 DAYS**

**Breaches as a result stolen or compromised credentials take the longest to identify and contain of any attack vector.<sup>4</sup>**

Glossary

# What an Identity-Based Attack Can Look Like

The challenge with identity-based attacks is that from most vantage points, they appear as legitimate access and activity. The likely attack vector is phishing, but there are many paths to credential theft and ultimately data loss.



## HUMAN-TARGETED ATTACKS

- **Phishing:** Fraudulent emails or texts that trick recipients into providing credentials or installing malware
- **Social engineering:** Manipulation through impersonation to collect sensitive information

## MALWARE ATTACKS

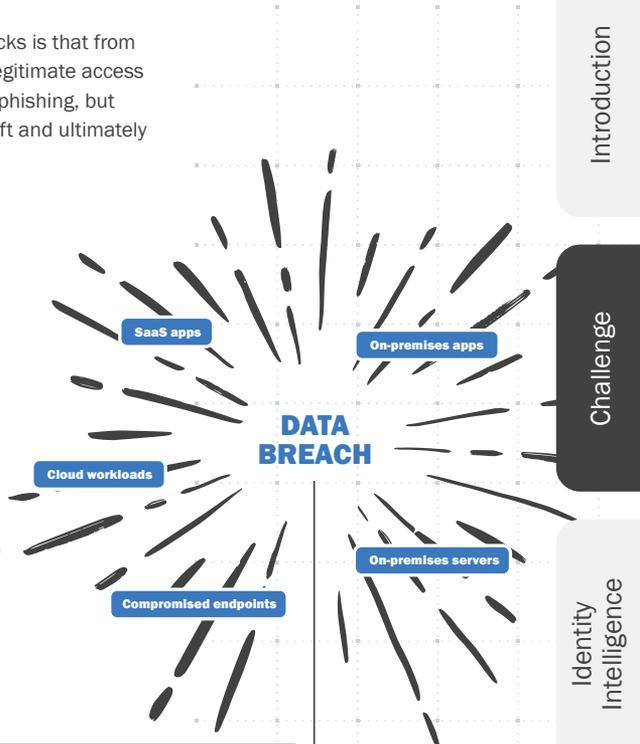
- **Keylogging:** Software that secretly tracks keystrokes to record usernames, passwords, and more

## AUTOMATED ATTACKS

- **Credential stuffing:** Automated testing of stolen username and password combinations across different platforms

## ACCOUNT TAKEOVER AND LATERAL MOVEMENT

- Remote access to other systems
- Internal spear phishing
- Leverage system tools (“living off the land”)



# The Complex Identity Landscape

When it comes to the landscape of identities, accounts, and other credentials, organizations struggle with volume, velocity, and variety.

## VOLUME

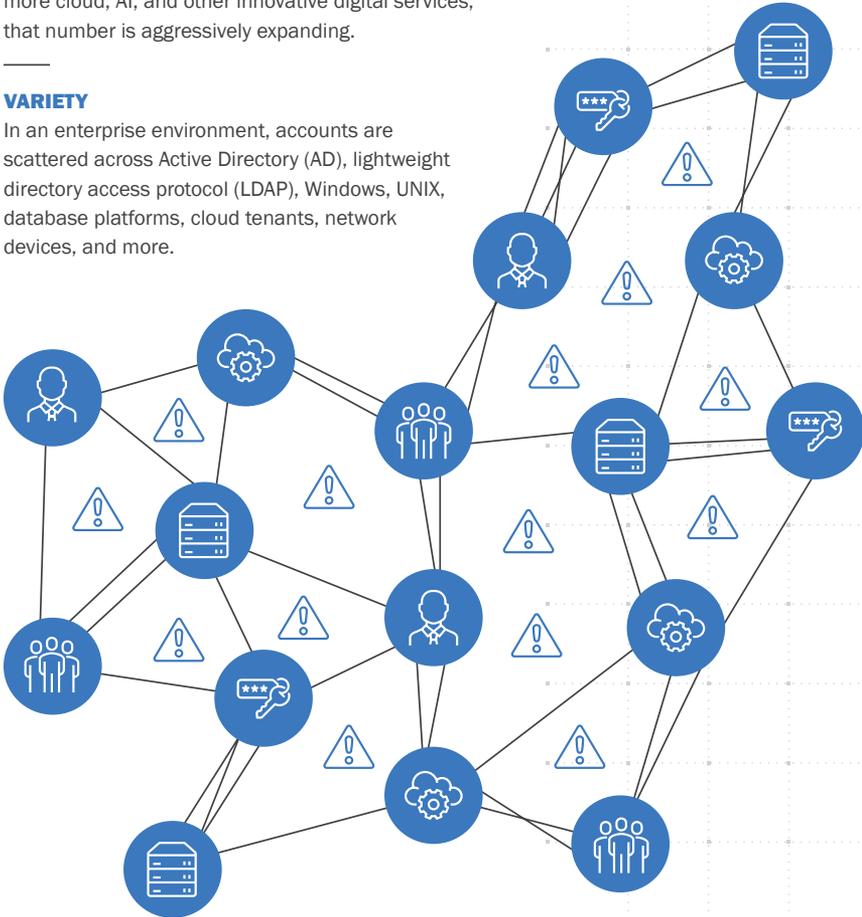
Companies often have two to three times more privileged user accounts than individual employees.<sup>6</sup>

## VELOCITY

With the growth of non-human identities as well as more cloud, AI, and other innovative digital services, that number is aggressively expanding.

## VARIETY

In an enterprise environment, accounts are scattered across Active Directory (AD), lightweight directory access protocol (LDAP), Windows, UNIX, database platforms, cloud tenants, network devices, and more.



Introduction

Challenge

Identity Intelligence

Solution

Glossary

# IDENTITY INTELLIGENCE

## Identity Intelligence and Why It's Important

When done well, identity intelligence encompasses the processes, rules, and policies needed to accurately manage access to digital assets. It is a critical component to ensuring that your digital domain remains secure so you can reduce the risk of identity-based cyber attacks.



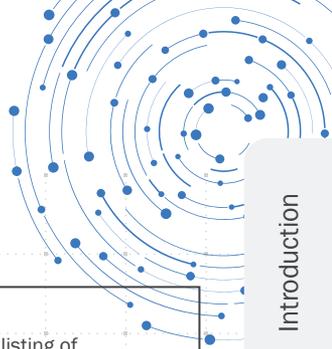
Introduction

Challenge

Identity Intelligence

Solution

Glossary



# Key Components of Effective Identity Intelligence

To establish effective identity intelligence, you need several programmatic elements in place for ongoing, operationalized success.

	<p><b>Identity discovery and ownership</b></p> <p>An essential step is having a comprehensive listing of all digital identities and assets, and more importantly, determining which human owns the account.</p>
	<p><b>Tailored asset access</b></p> <p>Different roles within a digital framework require different levels of access. This precision in defining asset types is crucial for mitigating risk.</p>
	<p><b>Access accountability</b></p> <p>Ensuring that only authorized personnel have access to specific areas is fundamental.</p>
	<p><b>Addressed protocol deviations</b></p> <p>It's critical to rectify any breaches in protocol swiftly to uphold data protection standards.</p>
	<p><b>Regular credential renewal</b></p> <p>Maintaining security involves periodic updates to authentication credentials, much like changing the locks for enhanced safety.</p>

Introduction

Challenge

Identity Intelligence

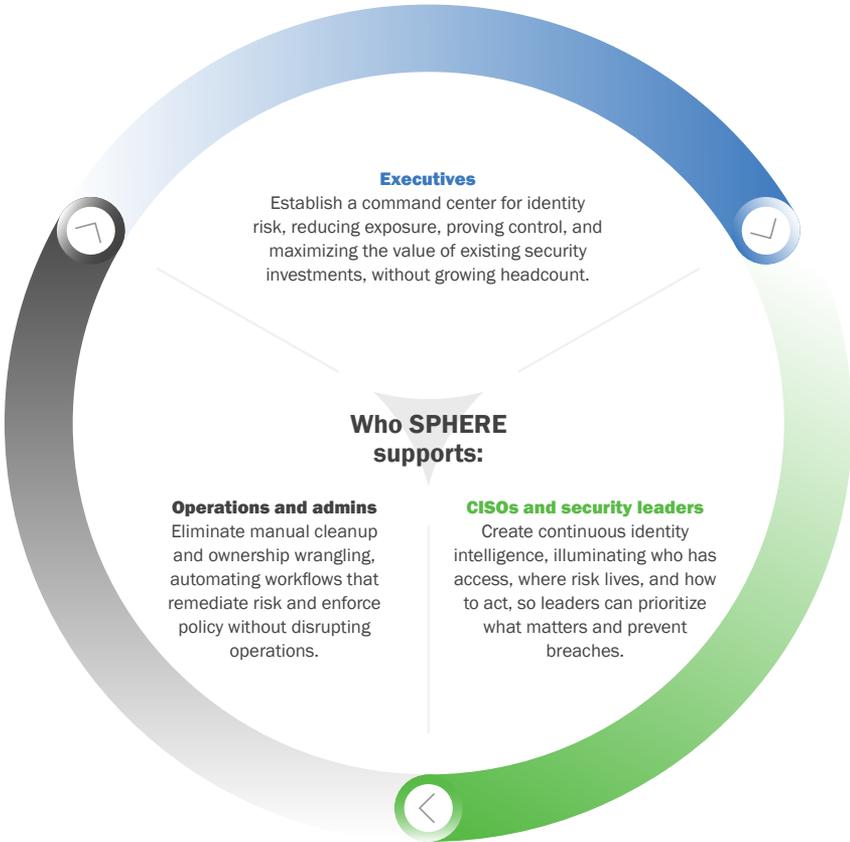
Solution

Glossary

# SOLUTION

## How SPHERE Helps

SPHERE delivers identity intelligence, acting as the command center for every identity, entitlement, and access decision, to power continuous risk reduction and breach prevention across the enterprise.



Introduction

Challenge

Identity Intelligence

Solution

Glossary

# Key Features and Benefits

SPHERE offers an end-to-end platform that enables quick recovery from cyber events and prevents future breaches. The features and benefits that contribute to identity intelligence include:



## Privileged access discovery and remediation

Surface unmanaged or noncompliant accounts and onboard them to a privileged access management (PAM) solution with automation.



## AD risk cleanup

Flatten nested groups, remove stale objects, and lock down excessive access.



## Service account intelligence

Find, classify, and control non-human accounts (before attackers do).



## Ownership resolution at scale

Map identities to legitimate human owners so security teams can act fast.



## Post-breach clarity

Rapidly investigate and remediate access following identity-related incidents.



## Audit and assurance

Deliver real-time reporting to prove control to auditors and cyber insurers.

Introduction

Challenge

Identity Intelligence

Solution

Glossary

# Why SPHERE Is Different from What You Have

By this point, you may be thinking, “We already have tools that solve for this.” The reality is that account management systems have blind spots, and many tools can identify issues but don’t enable resolution. SPHERE doesn’t replace what you have—it automates, augments, and amplifies it.

Here’s how SPHERE is different from what you have today.

**“Access reviews tell us what’s wrong, but don’t help us fix it.”**

Static reviews can’t keep up with growth or risk and fall short when it comes to prescriptive resolutions. SPHERE turns findings into action with policy-driven workflows, continuous monitoring, and remediation.

**“Our identity systems give us the visibility and control we need.”**

Most identity programs stall due to blind spots in account inventory, unclear ownership, and gaps in protection status. SPHERE helps you eliminate blind spots in privileged access, accelerate onboarding into PAM systems, such as CyberArk, and reduce breach exposure without relying on spreadsheets or manual remediation.

**“We have people to take care of this already.”**

The volume and complexity of accounts makes it impossible to manage and secure at scale. Manual processes break under the weight of nested groups, service accounts, and constant change. SPHERE makes management automated and sustainable, freeing team resources to work on higher-value tasks.

**“Our security tools take care of our needs.”**

Most security tools manage access. SPHERE fixes the intelligence gaps they leave behind, uncovering blind spots, surfacing risk, and triggering the right action at scale.

Introduction

Challenge

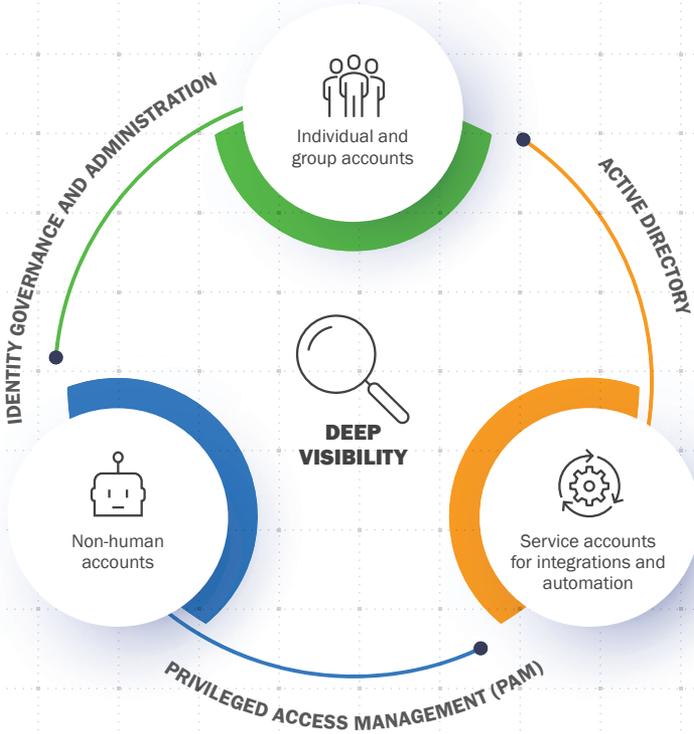
Identity Intelligence

Solution

Glossary

# Create Visibility

SPHERE intelligent discovery allows you to tag and inventory all accounts within days, providing visibility into system access and exposure. Unmanaged and noncompliant accounts are surfaced so they can be onboarded with automation. SPHERE goes beyond basic discovery to surface blind spots, map ownership, and drive remediation at scale—providing the context needed to reduce real risk.



Introduction

Challenge

Identity Intelligence

Solution

Glossary

# Establish Ownership (a.k.a. Find the Human)

When no one owns an account, remediation stalls. And without human approval, security teams can't act without risking disruption. Ownership is the only reliable way to answer the questions that matter:

<b>Who owns the risk?</b>	<b>Is the access still justified?</b>	<b>If something goes wrong, who's accountable?</b>
---------------------------	---------------------------------------	--

Without clear, validated ownership, you're not managing risk, you're hoping for the best. Every dormant account, every untracked service identity, every out-of-date entitlement is a potential breach point. This is acute in environments with high turnover, distributed workforces, or extensive third-party integrations.

Traditional tools focus on what an account can do, not who stands behind it.

SPHERE doesn't just inventory accounts or check entitlements, it continuously discovers, validates, and recertifies human ownership—the who—of every user, service, and non-human identity in the environment, unlocking remediation and accountability.

	<b>ACCOUNTABILITY</b>	<b>CONTINUOUS VALIDATION</b>	<b>ACTIVE REMEDIATION</b>
	It's not enough to conduct annual access review "fire drills"—you can't enforce policies or detect abuse if you don't know who is responsible.	Ownership isn't static. Mergers, acquisitions, reorgs, and attrition mean you need a system to regularly confirm and recertify account owners.	Elusive identity and ownership gaps can hide for years, neglecting dormant accounts, untracked service identities, and obsolete entitlements.
<b>WITH SPHERE...</b>	<b>...all accounts, especially privileged accounts, have real human owners.</b>	<b>... access reviews are ongoing and actionable.</b>	<b>... gaps are surfaced and resolved before they become a breach.</b>

## Automate and Integrate for Scale

While most enterprises invest in PAM and identity governance and administration (IGA), these systems depend on clean, complete identity data to function—and that's exactly what's missing. By feeding intelligence into IGA, PAM, and audit workflows, SPHERE makes the entire identity stack smarter and more effective.

Acting as the nucleus of the identity stack, SPHERE connects and informs IAM, IGA, and PAM systems, surfacing blind spots, aligning access with policy, and triggering automated remediation. This drives real-time risk reduction and delivers true identity hygiene and intelligence at scale.



Introduction

Challenge

Identity Intelligence

Solution

Glossary

# Learn More About SPHERE

SPHERE is the global leader in Identity Hygiene. We are dedicated to reshaping modern identity programs by embedding this foundational fabric, enabling organizations to quickly reduce risks. We work through an identity lens that protects an organization's accounts, data, and infrastructure. Our solutions deliver immediate time-to-value by leveraging automation to discover, remediate and secure identities, now and forever.

Driven by our core values of passion, empathy, and authenticity, our vision drives us to continually innovate, helping our clients to sleep better knowing their attack surface is drastically reduced, thwarting the plans of bad actors every single day.

We're ready to help you address your identity hygiene and security challenges. For more information, please visit [sphereco.com](https://sphereco.com).



## DOCUMENT SOURCES

1. CyberArk, [2025 Identity Security Landscape](#), Apr 2025
2. Gartner, [The Top 8 Security and Risk Trends We're Watching](#), Nov 2021
3. Gartner, [Gartner Unveils Top Eight Cybersecurity Predictions for 2024](#), Mar 2024
4. IBM, [Cost of a Data Breach Report 2024](#), Jul 2024
5. IBM, [IBM X-Force 2025 Threat Intelligence Index](#), Apr 2025
6. U.S. Department of Health and Human Services, [Privileged User Compromise](#), Aug 2024

# GLOSSARY

## Account management concepts

- **Circular nesting:** In Active Directory security, refers to a scenario in which two groups or more become members of each other's group through nested memberships, which grant the privileges and permissions of each group to which an entity belongs.
  - **Entity:** Anything with a distinct identity within a system or environment (e.g., users, groups, devices, processes, etc.).
  - **Identity:** A unique human or machine (i.e., non-human entity) that utilizes credentials to access resources or perform tasks.
  - **Group:** A named collection of entities that can be assigned security permissions and access controls.
  - **Privileged user:** A user that has been authorized to access system functions and resources that other users cannot.
  - **Privileged account:** A user account with elevated authorizations.
  - **Stale account:** A user or service account that remains active despite prolonged disuse (e.g., for former employees whose user accounts have not been deactivated).
  - **User:** An individual, organization, device, or process authorized to access an information system or resource.
- 

## Non-human identities

- **AI agent:** Autonomous non-human entity that makes decisions and takes action on behalf of a person or organization.
  - **API key:** A passcode that serves as a unique identifier to authorize access to an application programming interface's services and data.
  - **Bot:** A software application that performs automated tasks over the Internet or on local networks or individual devices.
  - **Machine identity:** A subset of non-human identity that refers to the unique identifying attributes of workloads and physical and virtual machines used for authorization.
  - **Non-human identity:** Any identity that does not refer directly to an individual human user (e.g., applications, services, or processes).
  - **OAuth token:** An Open Authorization code used by an application to make an API request on behalf of a user.
  - **Robotic process automation (RPA):** Refers to the use of bots to automate repetitious digital tasks that are otherwise performed by humans.
  - **Service account:** A type of non-human privileged account that is used to run applications, services, or processes.
-

# GLOSSARY

## Identity-related security concepts

- **High-risk account:** An account used by an individual whose work or public status entails access to or influence over sensitive information.
- **Identity and access management (IAM):** The practice of verifying user identities and controlling permissions to restrict access to digital resources.
- **Identity hygiene:** The practice of maintaining well-regulated access to digital resources.
- **Identity governance and administration (IGA):** The practice of managing the identity lifecycle, from onboarding and deactivating users to demonstrating compliance with security regulations.
- **Just-in-time (JIT) access:** A security strategy that allows user access to sensitive resources only when needed and for only as much time as necessary, with access automatically revoked afterward.
- **Privileged access management (PAM):** A subset of IAM that focuses on elevated access controls to deter privilege misuse.
- **Vaulting:** The practice of storing secrets such as usernames, passwords, and encryption keys in a secure software vault to prevent unauthorized access.
- **Zero standing privilege / least privilege:** The security principle that access privileges should be restricted to the minimum number and duration necessary to accomplish specific tasks.

---

## Identity-related cyber threats

- **Account takeover (ATO):** Refers to the unauthorized access and misuse of a digital account and associated resources by a third party.
- **Credential stuffing:** A type of brute-force automated attack that uses stolen or compromised usernames and passwords to gain unauthorized access to accounts.
- **Internal spear phishing:** Also known as lateral phishing, refers to the use of stolen credentials to impersonate a trusted user and attempt to trick other internal users into sharing sensitive information.
- **Keylogging:** The act of covertly recording keystrokes on a device via a logging program for malicious purposes.
- **Lateral movement:** A technique used by cybercriminals to exploit unauthorized access by moving through other systems in a network in search of sensitive information or additional privileges.
- **Phishing:** A common type of social engineering attack that attempts to manipulate a user into disclosing sensitive information or performing other actions by impersonating a trusted entity.
- **Social engineering:** The act of tricking individuals into performing adverse actions by impersonating a legitimate entity.

