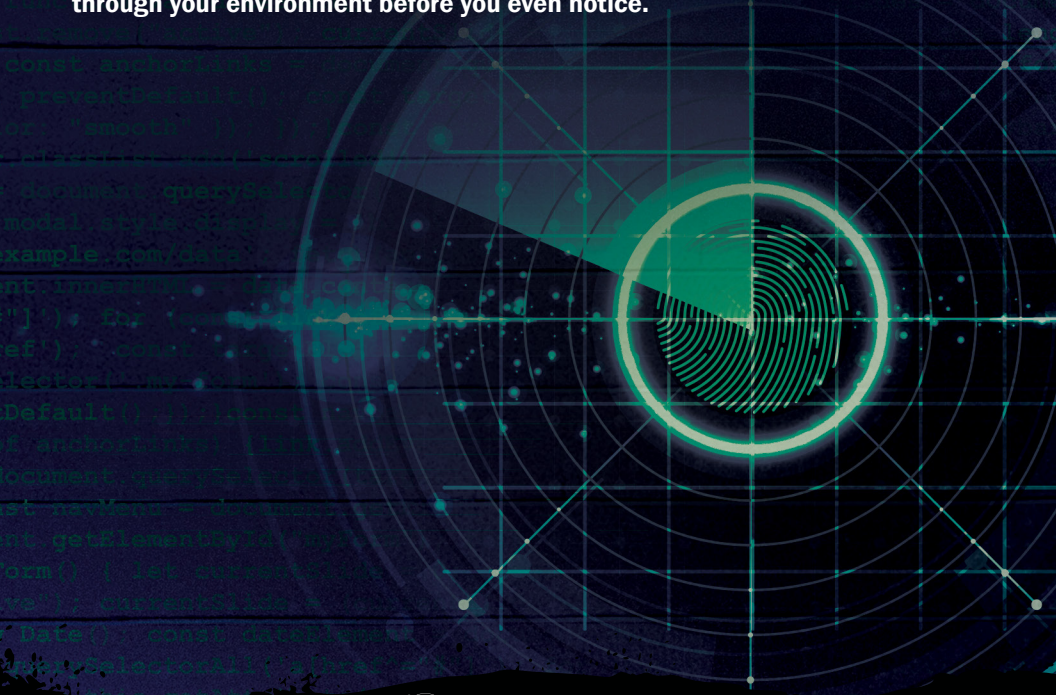
IDENTITY

IS THE NEW PERIMETER— AND ATTACKERS KNOW THIS BETTER THAN YOU

Cybercriminals don't break in anymore. They log in with valid credentials, bypass your defenses, and move laterally through your environment before you even notice.



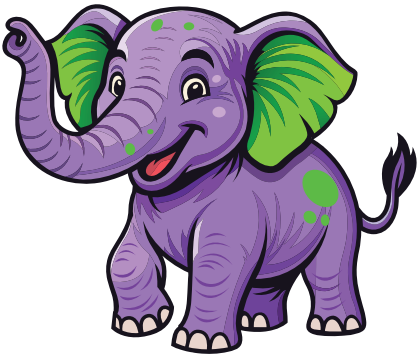
exactmarket℠

ELEPHANT IN THE ROOM EBOOK SERIES

TABLE OF CONTENTS

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 ignore but maybe isn't getting the attention it deserves.



INTRODUCING THE ELEPHANT

The Perimeter Has Changed

Identity drives almost every security decision today, yet many organizations still treat it like a secondary priority. This document calls out the reality that most teams already sense but rarely discuss directly: identity has become the most reliable way into an environment, for both legitimate users and attackers.

INTRODUCTION

Identity has become the control layer that everything else depends on.

Identity Is the New Perimeter

Security used to center around the network boundary. Firewalls, VPNs, and IDS tools handled keeping untrusted traffic outside the environment. That model works only when applications, data, and users are in a controlled environment.

That world is gone.

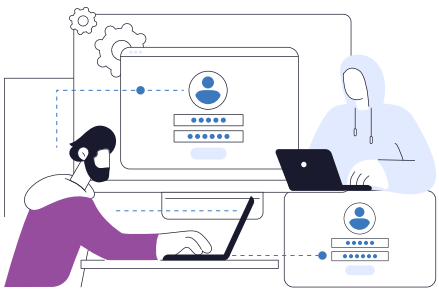
Remote work, SaaS adoption, multi-cloud setups, and distributed teams changed the landscape. The perimeter dissolved, and identity is now the most consistent access point across digital environments.

Attackers know this exceptionally well. They do not bother with the network edge if they can get a valid login.

According to the 2025 Data Breach Investigations Report (DBIR) from Verizon, credential misuse is responsible for 22% of all breaches and 88% of breaches involving web applications.[1]

The Breach Has Changed

Modern breaches rarely begin with an exploit. They start with access. Phishing kits steal credentials, infostealer malware captures session cookies, and attackers acquire valid open authorization (OAuth) refresh tokens or compromised single sign-on (SSO) sessions that bypass multi-factor authentication (MFA). This approach is quiet, appears legitimate to most systems, and does not trigger exploit-based alerts.



A typical example of identity-first compromise

A contractor signs into a SaaS tool on a personal device. That session cookie is harvested by malware. The attacker uses the same session hours later and appears completely legitimate. No alarms. No blocked activity. No sign that anything is wrong.

The New Math of IDENTITY

The number of identities inside modern environments has grown far beyond anything traditional governance models can handle. Human users now account for only a small part of the overall identity footprint. Cloud services, automation pipelines, APIs, and machine processes create large volumes of non-human accounts.

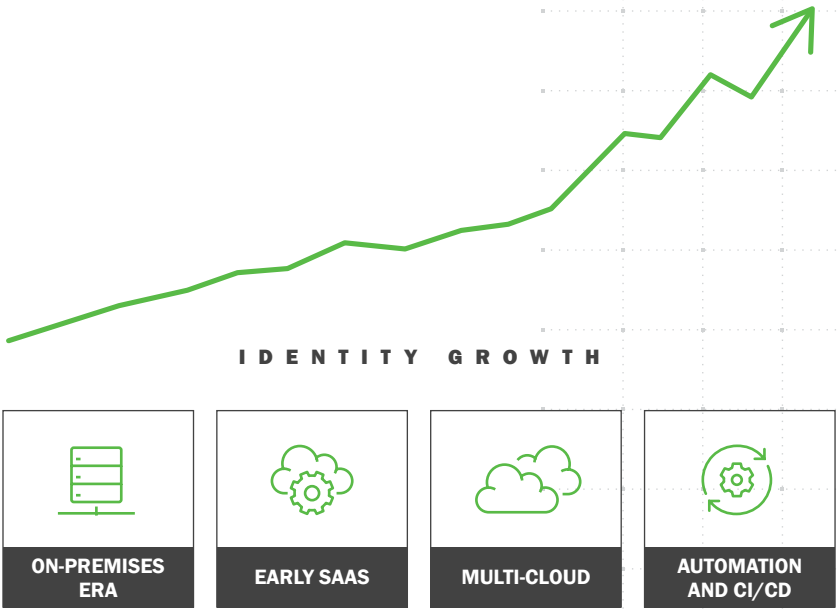
Key facts that matter:

Machine identities outnumber human accounts by ratios up to 82:1 in large enterprises.[2]

42% of machine identities have sensitive data access.[3]

Cloud and SaaS adoption accelerate identity growth faster than manual processes can keep up.

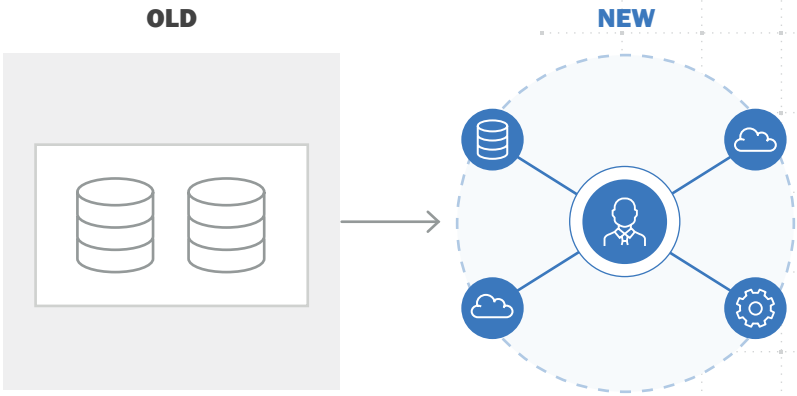
Scale is the core challenge. Not identity itself, but the sheer volume of identities that must be tracked and governed.



Why the Perimeter Moved

Older security models assumed a centralized workforce and applications running in a data center. Today, users work from anywhere, data flows through multiple cloud providers, and workloads move across various platforms. Attackers adapted quickly. Using valid credentials is simpler than exploiting software, and MFA cannot help when an attacker already has a working session token. Once an identity is inside the environment, it looks legitimate until proven otherwise, which is why identity controls now matter more than traditional network boundaries.

Identity has become the most stable control layer across modern environments. It influences who can access systems, how far they can move, and how quickly unusual activity can be detected. The sections that follow describe how identity debt forms, where it accumulates, and the steps organizations can take to rebuild identity governance in ways that support how environments run today.



THE PERIMETER DID NOT DISAPPEAR. IT SHIFTED TO IDENTITY.

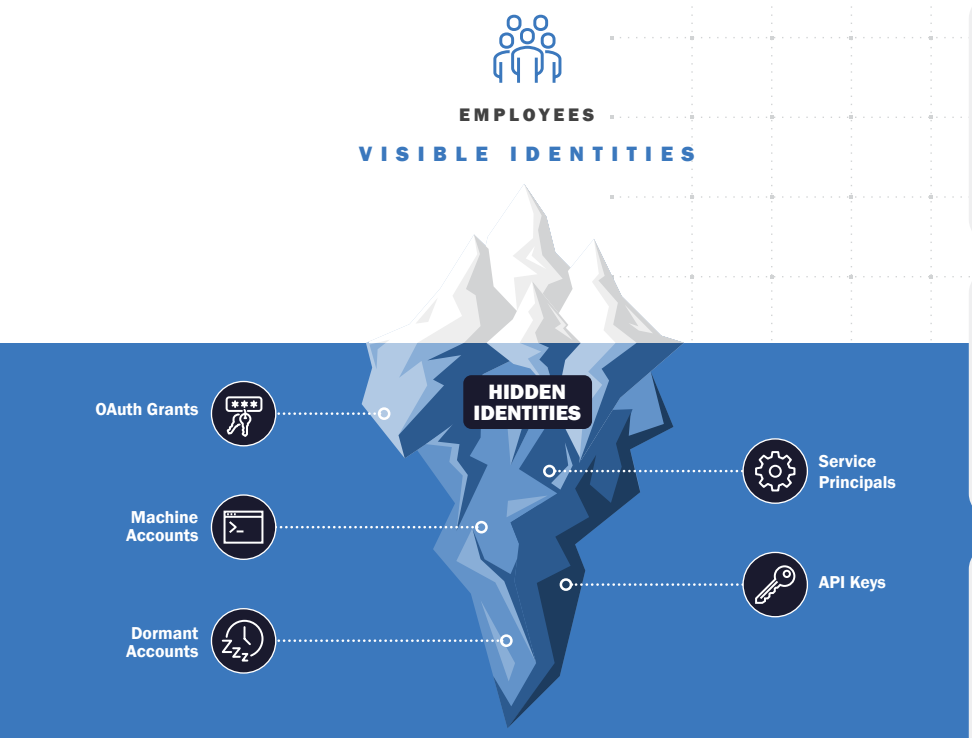
CHALLENGE

Identity Debt and Hidden Vulnerabilities

Identity debt builds quietly. Most teams do not see it forming because it grows one request, one exception, and one temporary permission at a time. As organizations expand into cloud platforms and SaaS ecosystems, the number of identities increases far faster than the mechanisms needed to govern them. The result is a landscape full of accounts that nobody fully understands and access grants that outlive their purpose.

Attackers thrive in this situation because it provides them with a larger, more flexible attack surface than most defenders realize.

IDENTITY ICEBERG



THE PROPORTION PROBLEM

HIDDEN IDENTITIES OUTNUMBER HUMANS

What Identity Debt Looks Like

Identity debt builds the same way any unmanaged system grows in complexity. It increases slowly, becomes harder to track, and expands faster than the team responsible for it can manage.

Years of accumulated access

Employees collect permissions as they move through the organization, and these permissions are rarely audited and removed. Managers assume someone else will handle the review, and IT believes business units will ask for removals. Attackers inherit everything that was never revoked.

Service principals growing without oversight

Cloud teams create service principals and automation identities to keep projects moving. These identities often have powerful roles because removing friction is more important than precision during early builds, and attackers target them because they offer consistent access with minimal monitoring.

Former employees with active accounts

Offboarding covers AD and email, but it does not consistently clean up SaaS accounts, cloud roles, or third-party access. That gap creates dormant accounts tied to people who no longer work for the organization.

Permission creep

Users accumulate access faster than they lose it. For example, temporary permissions stay permanent, project access doesn't expire, and responsibility shifts happen without a corresponding cleanup. When an attacker compromises these over-extended accounts, the blast radius increases significantly.

Mapping Identity Types

IDENTITY TYPE	DESCRIPTION	GOVERNANCE GAP
Human identities	Employees, contractors, partners	Role changes do not produce reliable access cleanup
Service accounts	Legacy system accounts, batch jobs, on-premises automation	No ownership or expiration, often shared
Service principals	Cloud-native identities—Microsoft Azure Active Directory (Azure AD), Amazon Web Services (AWS) identity and access management (IAM) roles, and Google Cloud Platform service accounts	Created by developers outside the standard review process
API keys and tokens	Non-human secrets used by scripts, pipelines, applications	Often embedded in code and rarely rotated

Most organizations focus on human identities and leave everything else unmanaged, even though non-human accounts outnumber users by large margins. Attackers understand this distribution better than defenders do, turning identity debt into an advantage for anyone trying to gain unauthorized access.

Three Categories of Hidden Risk

Zombie access (dormant accounts still active)
Dormant accounts remain enabled but unused, and because no one expects activity from them, unusual behavior often goes unnoticed. Attackers favor these identities because they produce no conflict with legitimate user behavior and rarely trigger alerts.

01

Example: An unused Okta account belonging to a former contractor still had access to GitHub. Attackers used it to access private repos and pivot into CI/CD systems.

Permission sprawl (admin rights nobody needs)
Temporary admin access becomes permanent. IT never cleans up broad roles assigned during outages or migrations. Over time, these rights drift far from the user's fundamental responsibilities. Attackers use these privileges to move quickly and quietly through the environment.

02

Example: A user granted "temporary" Azure Contributor permissions for a migration project still had them a year later, enabling an attacker to deploy privileged virtual machines (VMs).

Machine identity chaos (API keys, service accounts without owners)
Machine identities grow faster than any team can document and often use static secrets and broad permissions because they support automation pipelines or CI workflows. Nobody owns them, so nobody reviews them, and attackers use these to blend in with normal operational activity.

03

Example: A CI/CD pipeline token with broad AWS IAM permissions was stolen from a developer's laptop via an infostealer.

MACHINE IDENTITIES ARE GROWING FASTER THAN HUMAN ACCOUNTS AND OFTEN WITH MORE PRIVILEGE.

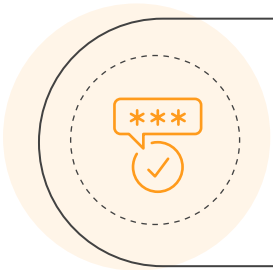
These patterns appear in nearly every environment, regardless of size or maturity. Once teams understand this, they can find where they accumulate. Organizations are often surprised by how many high-risk items sit outside formal governance boundaries.

Where the Risk Hides

A significant amount of identity debt is hidden entirely from routine review and hides in places where governance is inconsistent or nonexistent.

Over-permissioned cloud IAM policies

Cloud permissions are easy to grant at a broad level, especially during rapid deployment or troubleshooting. IT creates policies quickly and doesn't always review them, leaving access in place. Attackers can get in and move laterally without needing a secondary exploit.

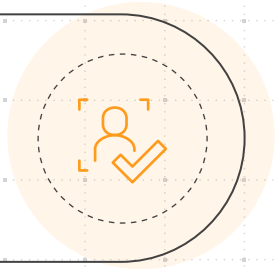


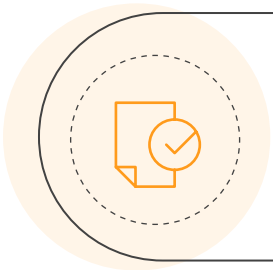
Approved and forgotten OAuth integrations

During initial setup, SaaS applications often request persistent access, and organizations grant it once and move on. The tokens stay valid long after the application is unused or the vendor relationship has ended, creating an attack path that bypasses passwords and multi-factor authentication (MFA) entirely.

Convenient standing privileges

Many teams maintain permanent administrative rights because they believe it reduces friction. This habit creates many high-value accounts that, if compromised, give the attacker immediate administrative control. Moving to a just-in-time access model requires cultural change, but it cuts a large portion of unnecessary privilege.





Offboarding gaps

Modern offboarding must remove access across dozens or hundreds of SaaS tools and cloud platforms. Legacy processes stop at AD, email, or human resources-linked systems, leaving the rest to manual cleanup. Those manual steps fail often, creating a growing inventory of active accounts tied to former employees.

Why Identity Debt Matters

Identity debt increases the impact of every breach and provides more hiding places, more privileges to exploit, and more time for attackers to work undetected. Most breaches start with valid credentials, and attackers exploit unmonitored identity structures that have been in place for years. Organizations that reduce identity debt shrink their attack surface, gain visibility, and detect and contain misuse faster.

TRANSFORMATION

Identity as a Strategic Control Plane

Identity plays a central role in modern environments. Applications, data, automation, cloud platforms, and third parties all rely on identity to determine who or what can access systems and data. As organizations move further into hybrid and remote models, identity becomes the only consistent layer across their entire operating environment—evolving from an access mechanism to a strategic control layer.

IDENTITY AS THE CONTROL PLANE

The Shift in Thinking

For years, teams treated identity as a supporting function—necessary, but largely invisible. That assumption no longer holds. In modern environments, identity determines how applications run, how data is accessed, how incidents unfold, and how organizations show resilience under regulatory scrutiny.

Many organizations still treat identity as routine IT work. In practice, it now affects performance, risk, compliance, and incident response. A compromised identity can cross cloud boundaries, bypass network controls, and access data directly. A shift in thinking reshapes identity's role across three areas: daily operations, threat detection, and regulatory accountability.

Identity Risk Directly Impacts Operations

When identity becomes the primary control point, failures translate directly into operational impact. Breaches that use valid credentials are slower to detect and more costly to contain. IBM reports the average cost of a data breach is $4.4 million per incident.[4] A significant part of this cost comes from the time it takes to confirm whether a legitimate user is behind the activity. Identity risk directly influences service uptime and response windows.

Detection Tools Struggle with Valid Access

That operational impact is compounded by a fundamental mismatch between identity-based attacks and how most security tools are designed. Most security tools look for patterns associated with exploitation, not typical logins. When an attacker uses valid credentials, the activity often looks ordinary and may even align with standard user behavior. Effective detection requires understanding identity behavior across systems, not only watching for anomalies at the edge.

Governance Is Now a Compliance Expectation

These challenges no longer affect only security teams. Regulators, including those enforcing the Digital Operational Resilience Act (DORA) and the NIS2 Directive, now expect organizations to prove reliable identity controls. DORA became enforceable in January 2025 and includes penalties up to €10 million or up to 2% of global turnover.[5] Compliance teams now treat identity as part of core risk management.

UP TO €10 MILLION IN FINES

REGULATION PRESSURE POINTS

REGULATIONS:

- DORA
- NIS2

REQUIRED CONTROLS:

- Access accuracy
- Privilege governance
- Traceability
- Proof of deprovisioning

From Reactive to Continuous

This shift in how organizations think about identity also changes how identity work must be done. What once were sporadic tasks, such as annual access reviews, quarterly certification cycles, and occasional cleanup projects, are no longer enough. Cloud usage changes weekly, SaaS tools get added constantly, and automation creates new accounts without human oversight. Organizations that continue to rely on periodic identity work risk falling behind the current state of their environment.

OLD APPROACH	MODERN APPROACH
Annual access reviews	Continuous evaluation of access and behavior
IT owns all identity decisions	Security, risk, and compliance share ownership
Trust but verify (once a year)	Never trust, always verify (continuously)
Standing administrative access	Just-in-time and just-enough access

Why Identity Controls Matter Now

Attackers increasingly prefer identity-based pathways because they are efficient and reliable. Stolen credentials are widely available. OAuth tokens can bypass multi-factor authentication (MFA). Session cookies behave like legitimate users. Once inside, attackers use identity relationships rather than exploits to move through the environment.

Ransomware Groups Buy Credentials, Not Exploits

Reports show a clear trend: ransomware operations increasingly begin with purchased access rather than zero-day vulnerabilities.[6] The 2025 DBIR highlights that credential misuse accounts for a significant share of breaches, particularly in web applications.[7] Valid identities require no exploitation and typically trigger fewer alerts.

Cloud Breaches Are Often Identity Failures, Not Software Failures

Cloud environments rely heavily on a permission structure. Over-permissioned IAM roles, stale service principals, and inherited privileges create pathways that attackers can exploit without compromising infrastructure. Many cloud incidents are traced back to unrestricted roles or misaligned access.[8]

Lateral Movement Follows Identity Paths

Once an attacker gains a foothold, they expand access through identity relationships. They assume roles, use shared secrets, or move between cloud services through excessive permissions. Network segmentation is effective only when identity structures are correctly aligned. If privileges span environments, attackers can follow those paths with very little resistance.

IDENTITY CONTROLS DETERMINE HOW FAR AN ATTACKER CAN MOVE AND HOW QUICKLY YOU CAN STOP THEM.

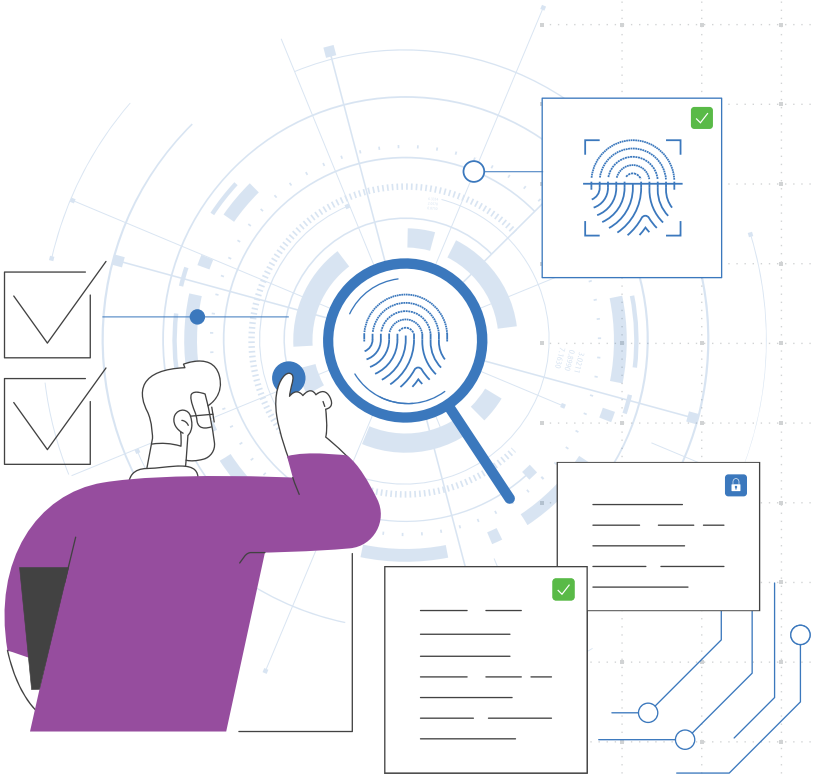
Identity as a High Leverage Control Plane

Identity has emerged as a consistent control point across cloud platforms, SaaS tools, on-premises systems, and automation pipelines. It empowers organizations to enforce least privilege, reduce excessive access, and automate provisioning and deprovisioning without relying on separate processes in every environment.

When identity is accurate and governed continuously, security teams gain clearer visibility, detection becomes faster, and audit requirements become easier to manage. This creates a more predictable operational model and reduces the noise caused by outdated or misaligned access.

As environments become more distributed and interconnected, identity offers stability in places where tools and systems do not. It now directly influences security posture, operational reliability, and compliance readiness. Organizations that treat identity as a strategic control layer gain a clearer understanding of who has access, how far that access reaches, and where risk is accumulating.

This realization marks the end of incremental improvement and the beginning of a different approach. Rebuilding identity governance for modern environments requires more than new tools or tighter reviews; it requires a reset aligned with how identity functions today.

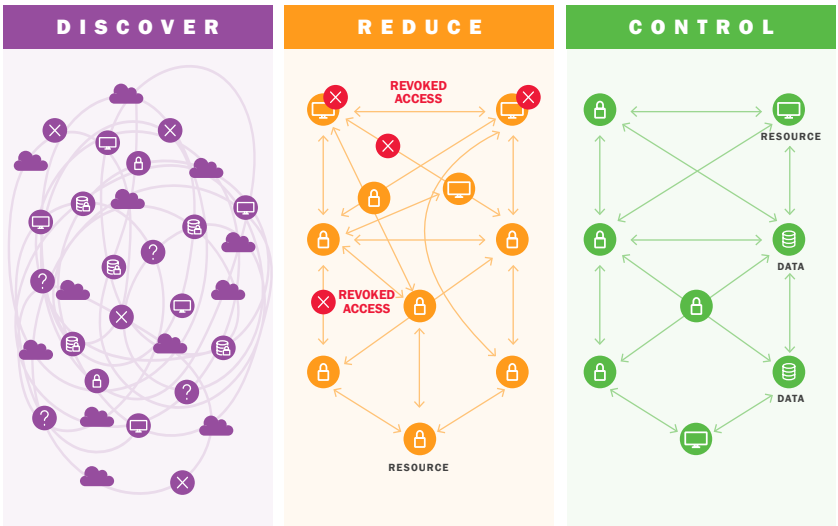


SOLUTION

The Identity Reset Playbook

Identity debt does not disappear through cleanup projects or one-time reviews. It grows faster than human processes can keep up with, particularly in cloud and SaaS environments where new accounts and tokens appear daily. Addressing this problem requires a structured approach that can be repeated, measured, and adapted as environments evolve.

This playbook focuses on three stages that work together: Discover, Reduce, and Control. Each stage serves a distinct purpose and builds momentum for the next. The goal is a measurable reduction of identity risk, not perfection.



IDENTITY ACCESS PLAYBOOK

PHASE 1

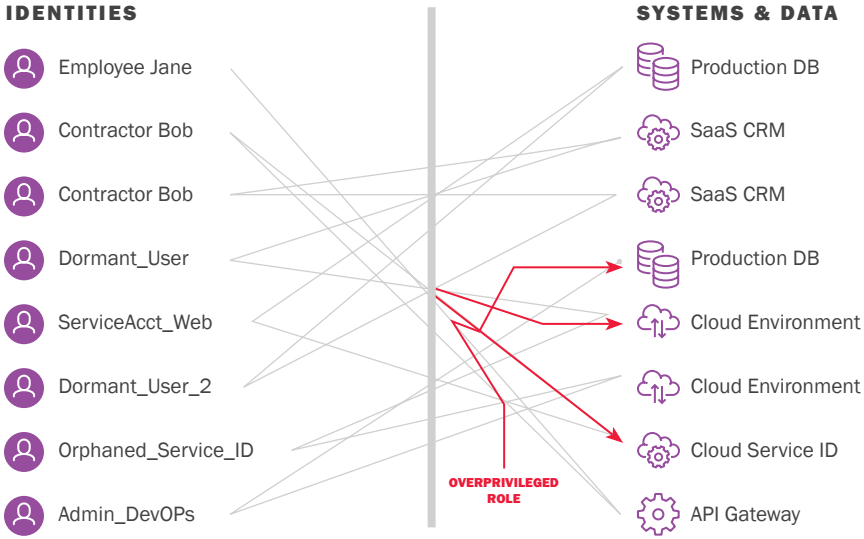
Discover (Map Reality)

Many organizations still base decisions on estimates rather than verified inventory. The discovery phase removes that assumption and replaces it with facts. The goal is complete visibility into every identity, access path, and privilege across the environment.

Begin with a complete inventory that includes human accounts, service principals, API keys, workload identities, and OAuth integrations. This requires connecting cloud IAM roles, on-premises directories, SaaS platforms, and partner systems. Once the inventory is established, map the access each identity has, including what systems it can reach, what data it can view, and what level of privilege it holds.

Discovery also reveals identity debt. Dormant accounts, unowned service principals, standing administrative access, and stale OAuth grants often surface at this stage. Cloud environments may reveal hidden role assumptions or forgotten trust relationships. This is the stage where the scale of the problem becomes visible, and where the first meaningful opportunities for reduction become clear.

IDENTITY MAP



IDENTITY SPRAWL

VISUALIZING ACCESS COMPLEXITY

PHASE 2

Reduce (Fix the Biggest Risks)

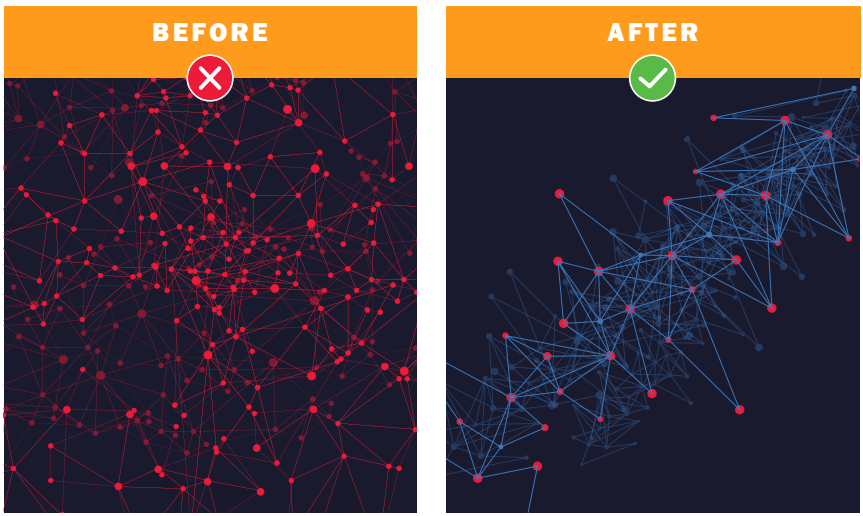
Once the environment is mapped, the next step is to reduce the highest risk exposure. Not every issue needs immediate remediation. Focus on the risks that move the needle first, then what materially reduces the identity attack surface.

Begin by removing dormant accounts and stale permissions. Any identity unused within a defined period should be challenged or removed. Next, address permissions that carry the greatest impact. High-privilege cloud roles, broad administrative access, and legacy superuser accounts should be replaced with narrower, purpose-built access.

During this phase, broken joiner and leaver processes become apparent, and it provides the right moment to correct them. When onboarding and offboarding work cleanly, future cleanup efforts shrink, compliance gaps close, and audit friction decreases.

Privilege right-sizing completes the reduction phase. This requires aligning access to what the user or system actively needs, not what has accumulated over time. Even modest reductions in privilege can limit lateral movement during an attack.

PRIVILEGE HEATMAP



EXCESSIVE PRIVILEGE & SPRAWL

RIGHT-SIZED & CONTROLLED ACCESS

IMPACT OF PRIVILEGE RIGHT-SIZING

PHASE 3
Control (Build Continuous Validation)

Reduction is only effective when it is followed by control. This phase turns identity governance into a continuous process, keeping the environment accurate as identity changes are monitored and corrected in real time.

Replace permanent administrative access with just-in-time elevation that expires automatically.

Automate lifecycle events by tying identity creation and removal to HR systems and role changes.

Feed identity telemetry into security operations so analysts can respond to unusual access events quickly, rather than relying solely on network alerts.

Continuous validation replaces annual review cycles with ongoing certification. Access reviews trigger automatically based on risk, privilege changes, or inactivity. Managers can review high-value permissions more often without being overwhelmed.

Over time, this creates an environment where access stays aligned with real responsibilities instead of drifting.

This control phase creates predictable, repeatable identity operations. Teams know exactly how access changes happen. Security knows when risk appears. Compliance knows where evidence lives. Identity becomes a managed flow rather than a backlog of unknowns.

Key Actions to Anchor the Playbook

Several actions reduce identity risk immediately while supporting longer-term improvements.

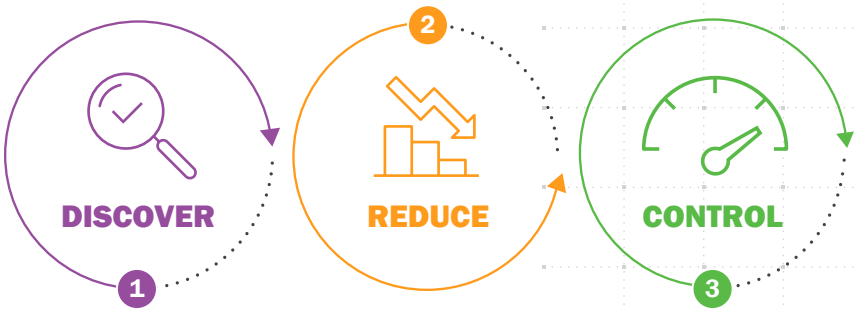
- **Start by inventorying everything, including machine identities.**
- **Remove stale accounts and unused access.**
- **Apply least privilege by default, not the exception.**
- **Automate offboarding and access expiration wherever possible.**
- **Integrate identity activity into security operations and treat it as part of incident detection.**
- **Track metrics that show progress, such as reduction in dormant accounts or fewer standing administrative roles.**

These actions are straightforward but lower risk immediately and support broader transformation by eliminating noise, tightening controls, and reducing exceptions.

Identity Isn't a One-Time Project

Identity security is a moving target because environments evolve faster than governance frameworks. The identity reset playbook is designed to keep the system stable as scale increases and new tools appear. When identity work becomes routine, organizations spend less time fixing problems and more time preventing them.

Identity debt will always exist in some form because environments continue to grow and change. The goal is not to eliminate debt entirely, but to maintain a structure where identity changes are visible, reviewed, and aligned with how the business operates. This creates a more resilient environment and a durable foundation for security and compliance.



GLOSSARY

TERM	DEFINITION
access path	A route an identity can take to reach systems, data, or resources. Attack paths often form when privileges accumulate over time or when non-human identities have broad permissions.
attack path	A sequence of identities, privileges, and access relationships that allows an attacker to move from initial foothold to a high-value target.
authentication	The process of verifying that an identity is who it claims to be.
authorization	The process of determining what an authenticated identity is allowed to access or do.
credential	Any password, key, token, or authentication material used to prove identity. Stolen credentials are often the starting point for modern breaches.
identity debt	The accumulation of outdated, misaligned, or unnecessary identities and privileges created over time as organizations grow and change. Identity debt increases risk by expanding the number of access paths an attacker can exploit.
identity governance	The policies, processes, and oversight used to determine who has access to what and to ensure permissions stay aligned with business needs.
identity lifecycle	The full progression of an identity from creation to modification to eventual removal. Weak lifecycle controls are a major source of identity debt.
just-in-time access	A method of granting elevated access only when needed and automatically removing it after the task is complete. Reduces long-lived privileges.
lateral movement	An attacker technique where access is used to move between systems after initial compromise, often by exploiting overly broad privileges or inherited permissions.
least privilege	A principle of granting only the minimum access required for a user or identity to perform its job. Helps reduce the attack surface and blast radius.

TERM	DEFINITION
machine identity	A non-human identity used by applications, scripts, services, automation tools, or cloud workloads to authenticate and access resources. Machine identities often outnumber human accounts.
multi-factor authentication (MFA)	An authentication process that requires two or more verification methods. MFA reduces some risks but does not prevent token theft or replay of active sessions.
network perimeter	The traditional boundary used to protect internal systems from external threats. Cloud and hybrid environments reduce boundary effectiveness, shifting security control to identity.
non-human identity	Any identity not tied to an individual person. Includes service principals, application accounts, automation identities, and API-driven system identities.
open authorization (OAuth) token	A token used to authorize access to web applications or APIs. Stolen OAuth tokens allow attackers to authenticate without MFA.
privileged access	Access rights that allow a user or identity to perform administrative, configuration, or sensitive operations. A common target for attackers.
service principal	A type of non-human identity, especially in Azure and Entra ID, used by applications and automation to authenticate and access cloud resources.
session token	A temporary authentication artifact created after login. Attackers frequently exploit stolen session tokens because they act as valid authentication and bypass MFA.
standing privileges	Long-lived administrative or elevated permissions that remain active regardless of whether they are needed. A major contributor to identity risk.
zero trust	A security model that assumes no identity or system is trusted by default. Access is continuously verified based on context, behavior, and risk.

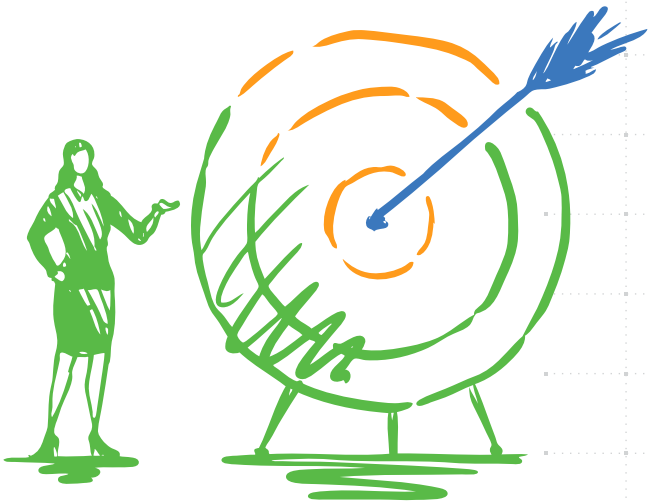
CITATIONS

SOURCES

1. Verizon, 2025 Data Breach Investigations Report, 2025
2. CyberArk, 2025 Identity Security Threat Landscape, 2025
3. Ibid.
4. IBM, Cost of a Data Breach Report 2025, 2025
5. Infosecurity Europe, EU's Digital Operational Resilience Act Officially Enforced, Jan 2025
6. Corvus Insurance by Travelers, Q3 '25 Travelers Cyber Threat Report: Ransomware Rises Again, Nov 20, 2025
7. Verizon, 2025 Data Breach Investigations Report, 2025
8. CyberArk, 2025 Identity Security Threat Landscape, 2025

ABOUT

exactmarket™



Founded in 2007, Exact Market is a woman-owned, WBENC-certified business focused on unifying marketing and technology around a shared vision to help enterprises innovate with confidence.

We bring together strategy, creativity, and data to help our clients stand out and stand for something. Our team of strategists, writers, designers, and technologists understands that the future of storytelling and software shares the same foundation: clarity, authenticity, and human connection.

We don't just help you talk about innovation.

WE HELP YOU LIVE IT.

Find out more @ www.exactmarket.com

exactmarket

ELEPHANT IN THE ROOM EBOOK SERIES