PAM PILLAR GUIDE

Privilege Is an Action, Not a Job Title



Bravura Security

October 2026

Contents

Executive Summary	**03**
Key Takeaways	**04**
Introduction	**05**
1 What Is Privileged Access Management in 2026?	**06**
2 How PAM Relates to IAM and IGA	**13**
3 Coverage, and Getting There in Weeks	**18**
4 Make Standing Privilege the Exception with Just-in-Time Access	**24**
5 Securing Non-Human Identities (NHIs) and AI Agents	**29**
How We Help	**34**
Where This Guide Fits Best	**35**
Guide FAQ	**35**
Before You Go	**36**

FIGURES

Figure 1	Privilege is an action, not a job title	07
Figure 2	Four costs you pay each week	09
Figure 3	Coverage has two dimensions	19
Figure 4	Vaulted is not managed	20
Figure 5	Standing privilege vs. just-in-time elevation	27
Figure 6	The non-human estate	31

Copyright © Bravura Security Inc. 2026. All Rights Reserved.

Executive Summary

Privileged access management (PAM) grew up around human administrators, and it still serves them well. In 2026, they are no longer the whole picture. Service accounts, workloads, pipelines and AI agents now hold privileged access, and they act at machine speed and scale. Privilege is an action, not a job title. Any identity that holds elevated access, or can easily obtain it, holds privilege.

This guide comes down to one idea. Coverage is the real benchmark for a PAM program, and most programs cannot yet prove theirs. Coverage has two dimensions. Breadth is the range of identity types you manage, human and non-human. Depth is the control you apply to each credential, from storage through rotation, session control and just-in-time elevation.

The gap between what you vault and what you truly manage is not a security abstraction. It is a running operational cost. You pay it four ways: in manual toil, in standing exposure, in audit fire drills and in lost accountability. The Verizon 2026 Data Breach Investigations Report counts credential abuse at 39% of breaches across the full progression. The exposure is real as well as costly.

The path out is practical and staged. You discover the privileged population, one segment at a time. You bring credentials under management, not just into a vault. You shrink standing access with just-in-time elevation until it is the exception. You extend the same discipline to non-human identities (NHIs). Then you govern the result with certification you can prove.

Start with what you can count. Measure breadth and depth by the evidence you can show today, segment by segment, not by the intent you hold. Each next control is a bounded piece of work, and you add it to what you already run.

> **IN ONE LINE**
>
> Coverage is the real benchmark for PAM in 2026: governing administrators alone leaves service accounts, workloads and AI agents outside your control.

Copyright © Bravura Security Inc. 2026. All Rights Reserved.

Key Takeaways

1 Privilege is an action, not a job title. Any identity that can change a system holds it, human or machine. Figure 1 · p. 7

2 Incomplete coverage is a running operational cost, paid in toil, standing exposure, audit fire drills and lost accountability. Figure 2 · p. 9

3 Certification is the proof. It shows, on a cycle, who should still hold privilege, not just who does. Chapter 2 · p. 15

4 Coverage has two dimensions: breadth, the identity types under management, and depth, the control applied to each credential. Figure 3 · p. 19

5 A vault stores a credential. Full credential management under PAM discovers it, rotates it and controls the session it opens. Figure 4 · p. 20

6 Standing privilege is access that persists whether or not it is in use. Just-in-time elevation makes it the exception. Figure 5 · p. 27

7 Non-human and AI-agent identities are a rapidly growing part of the estate. Service-account governance is where that work starts today. Figure 6 · p. 31

Copyright © Bravura Security Inc. 2026. All Rights Reserved.

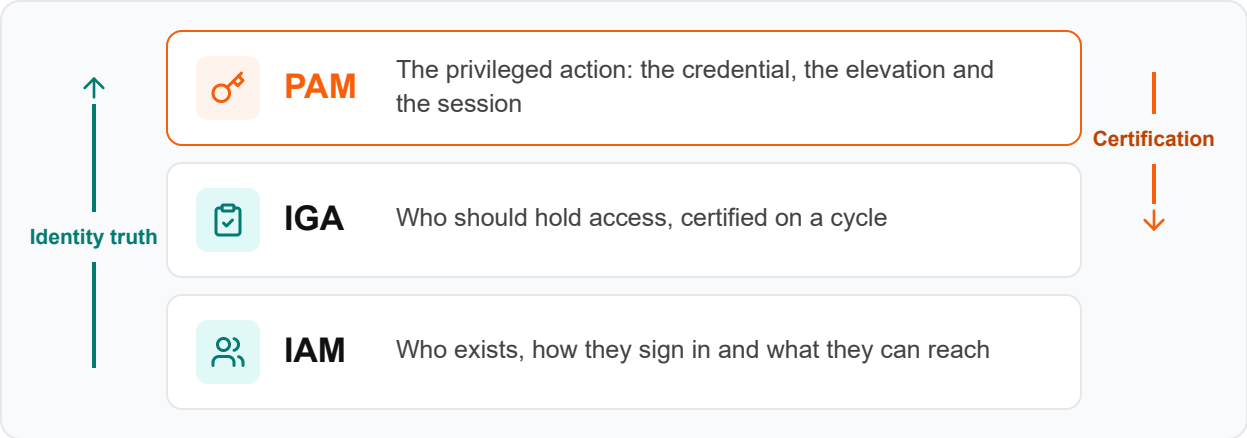
Introduction

Ask a PAM team how many privileged accounts they manage, and you will usually get a confident number. Ask how many of those are service accounts, pipelines or AI agents, and the answer gets harder. That pause is where this guide begins.

A deployment pipeline can change production. A service account can read a payroll database at 3 a.m. An AI agent can request access and act on it at machine speed. None of them has a job title. Each of them holds privilege.

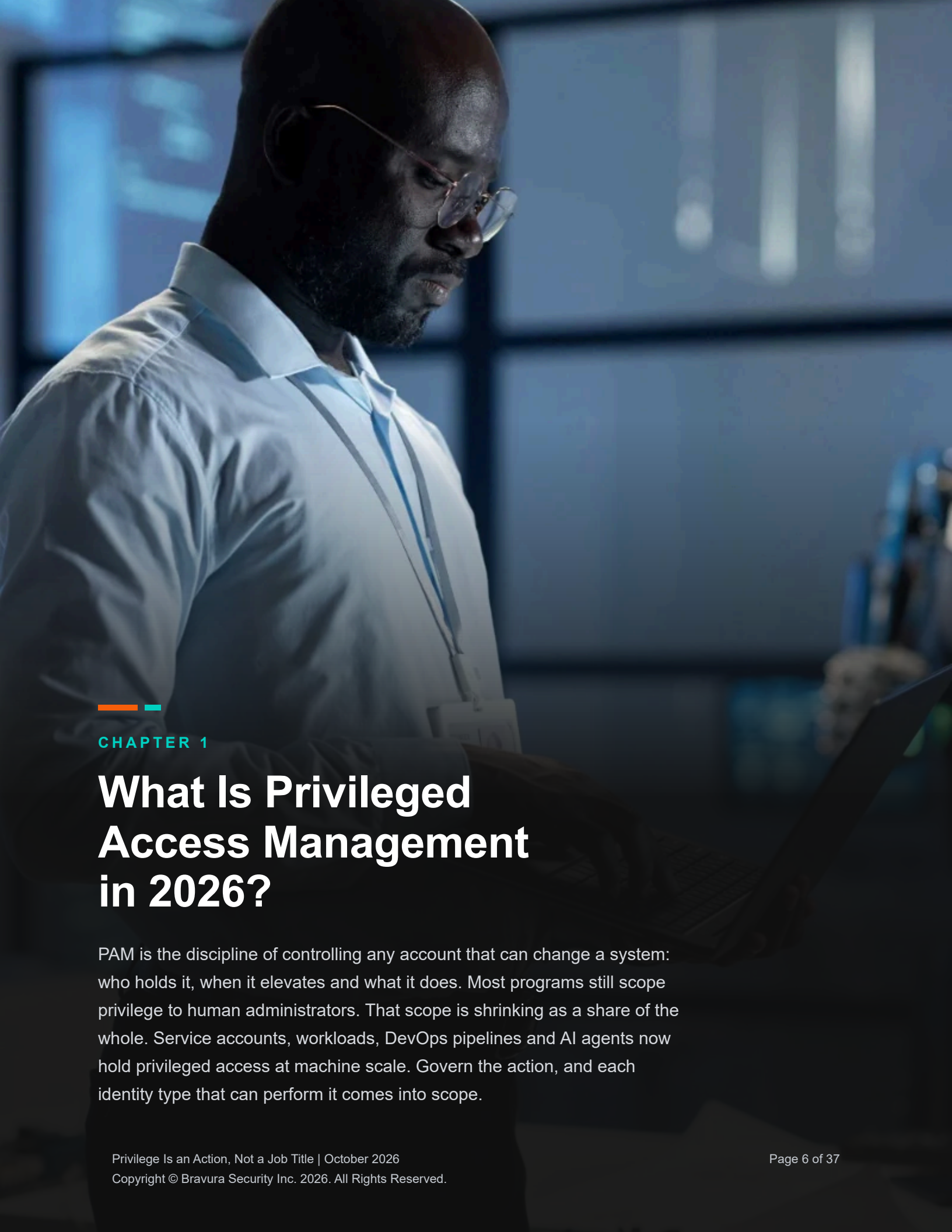
Your PAM program was built for the people on the admin list. The reality is simpler than the market makes it: privilege is an action, not a job title. Once you see privilege that way, the question changes. It is no longer how many admins you manage. It is how much of your privilege you control, and whether you can prove it.

Where PAM Sits



PAM controls the action. IGA proves who should hold it. IAM establishes who is acting.

Copyright © Bravura Security Inc. 2026. All Rights Reserved.



CHAPTER 1

What Is Privileged Access Management in 2026?

PAM is the discipline of controlling any account that can change a system: who holds it, when it elevates and what it does. Most programs still scope privilege to human administrators. That scope is shrinking as a share of the whole. Service accounts, workloads, DevOps pipelines and AI agents now hold privileged access at machine scale. Govern the action, and each identity type that can perform it comes into scope.

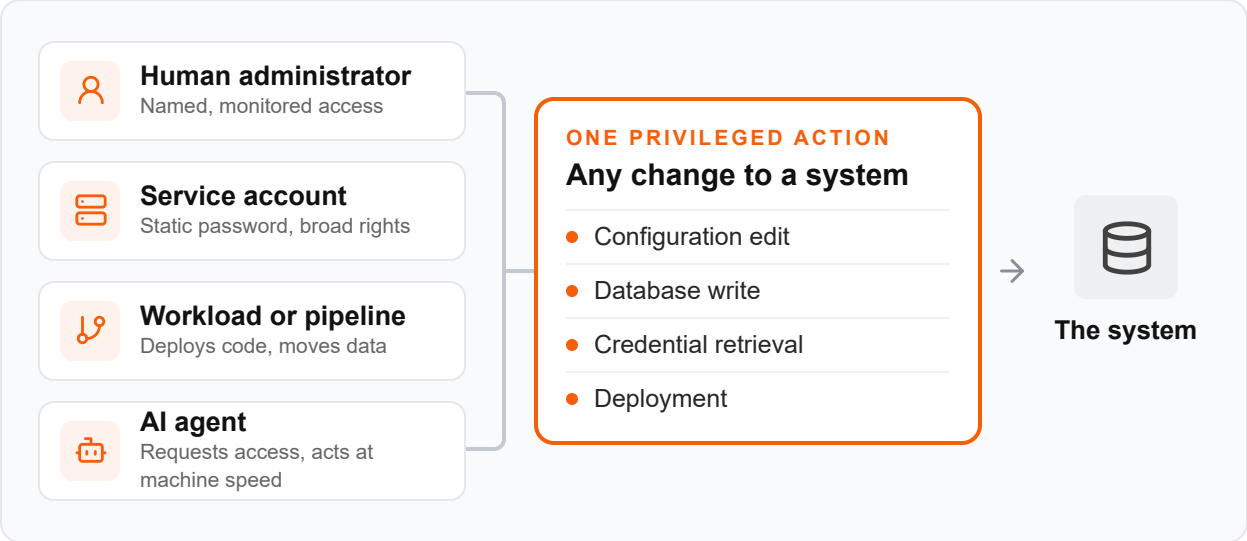
Copyright © Bravura Security Inc. 2026. All Rights Reserved.

Privilege is defined by the action, not the role

For years, a privileged account meant a named administrator with elevated rights. That model was easy to picture and easy to list. It is now the smaller part of the problem. A privileged action is any change to a system: a configuration edit, a database write, a credential retrieval, a deployment. The identity performing it can be a person, a service account, a workload or an AI agent. When you scope PAM to the action rather than the job title, coverage widens to match reality. You stop protecting a list of people and start protecting the ability to change things. For the basics, see our page on **what is privileged access management**[1].

This shift matters because risk follows the action, not the title. Any identity that can make a change can be misused to make it. A service account with a static password and broad rights carries more exposure than a named admin with monitored access. The job title on the account tells you little about the damage it can do. The action it can perform tells you far more.

FIGURE 1 **Privilege is an action, not a job title**



Govern the action, and each identity type that can perform it comes into scope.

Privilege is an action, not a job title. Any identity that can change a system holds it, human or machine.

1 bravurasecurity.com/what-is-privileged-access-management

Copyright © Bravura Security Inc. 2026. All Rights Reserved.

The four questions each privileged action raises

A useful way to frame PAM is as four questions asked of a privileged action.

- Who, or what, holds this access, and is that identity known and owned?
- When does it elevate, and does the access expire when the task ends?
- What did it do while elevated, and is that activity recorded?
- Can you prove those answers to an auditor?

A mature program answers the four for each privileged identity, human and non-human. Most programs answer them well for named administrators and poorly for everything else. The chapters that follow work through each question in turn.

What incomplete coverage costs you

When scope is incomplete, the cost is operational, not theoretical. An unknown privileged account cannot be governed, monitored or revoked, because no inventory lists it. An unowned credential has no one accountable for rotating it, so it drifts out of policy and stays valid long past its use. An audit you cannot prove fails examination and stalls the compliance work behind it. The account that needs attention is often the one no one is watching.

Executives often hear PAM framed as breach insurance, a cost you carry against a risk that may not arrive. That view undersells it. The larger cost is the one you pay week after week, whether or not an incident happens. You pay it four ways: manual toil, standing exposure, audit fire drills and lost accountability. Each is a line item in how your team spends its time.

The Toil of Managing Credentials by Hand

The most visible cost is manual credential management. When rotation is not automated and dependency-aware, someone has to do it, and the work is both tedious and risky. Rotate a shared service-account password by hand, miss one dependent service, and an application fails. After one outage like that, teams learn to stop rotating. The credential then stays static, which is the condition an auditor flags first.

The evidence that this drag is real sits in the data. The Verizon 2026 Data Breach Investigations Report measured how long organizations took to fix credential problems in third-party cloud environments. For weak passwords and permission misconfigurations, the time to resolve half of all findings reached almost eight months. That is not a queue that clears. It is a backlog that grows, because the manual work needed to clear it competes with everything else. Automated, dependency-aware rotation removes the toil and the outage risk together, so the backlog stops forming.

Copyright © Bravura Security Inc. 2026. All Rights Reserved.

FIGURE 2 **Four costs you pay each week**

~8 months to resolve half of all weak-password and permission-misconfiguration findings.

Verizon 2026 Data Breach Investigations Report

Manual toil

Hand rotation misses a dependent service, an application fails, and teams stop rotating.

WHAT REMOVES IT
Automated, dependency-aware rotation

Standing exposure

A standing credential is valid around the clock, including the hours no one is watching.

WHAT REMOVES IT
Just-in-time elevation with expiry

Audit fire drills

Each audit becomes a manual reconstruction of logs and access lists from separate systems.

WHAT REMOVES IT
Control and certification on one platform

Lost accountability

A shared account acts, and no action ties back to a person.

WHAT REMOVES IT
Individual authentication and session recording

Incomplete coverage is a running operational cost, paid in toil, standing exposure, audit fire drills and lost accountability, whether or not an incident happens.

Standing Credentials as Continuous Exposure

The second cost is exposure, and it runs around the clock. A standing credential is valid whether or not anyone is using it, including the hours no one is watching. It is a target that does not sleep. The longer it stays valid, the more copies and the more risk accumulate behind it.

Each person who once checked out the credential may still hold a copy, and each copy works until the credential rotates. Chapter 4 shows how just-in-time elevation shrinks that surface, and what the breach data says about credential abuse.

Copyright © Bravura Security Inc. 2026. All Rights Reserved.

Audit and Certification as a Recurring Fire Drill

The third cost is the audit itself. When you cannot show who holds privileged access and what they did with it, each audit becomes a manual reconstruction. Teams pull logs from separate systems, assemble access lists by hand and hope the picture holds together before the deadline. The work repeats each cycle, and it grows with the estate.

This cost is easy to underestimate because it hides inside normal operations. A certification campaign that should be a scheduled report becomes a project. An auditor question that should have a one-click answer becomes a week of evidence gathering. The underlying problem is not effort. It is that control and proof were not joined. When privileged access and certification sit on one platform, the evidence assembles itself, and the fire drill becomes a report you run on a cycle.

INDUSTRY LENS **Financial services**

Examiners expect you to show who held privileged access, what they did with it and whether it should still exist. When that evidence lives in separate systems, each exam cycle becomes a reconstruction. Randomized administrator passwords, recorded privileged sessions and certification on one platform turn that reconstruction into a report. Frameworks such as PCI DSS, SOX and FFIEC guidance share one demand: control you can prove. See **how we support financial services**[2].

Shared Accounts and the Accountability Gap

The fourth cost is lost accountability. Many teams still rely on shared administrator accounts, where several people use one credential and no action ties back to a person. That saves a little setup time and costs a great deal of traceability. When something breaks or an investigation opens, you can see that the shared account acted. You cannot see who was behind it.

The fix is not to ban shared accounts. It is to put each privileged login through individual authentication, and to record the session. Each action then ties to a named person without slowing the work. That turns a shared credential from an accountability gap into a controlled, attributable path. It also removes a standing secret, because the shared password stops traveling in people's notes. Our case against **shared privileged accounts**[3] covers accountability in more depth.

The table below maps each state of incomplete coverage to the cost it carries and the control that removes it.

2 bravurasecurity.com/solutions/industry/finance
3 bravurasecurity.com/blog/the-case-against-shared-privileged-accounts

Copyright © Bravura Security Inc. 2026. All Rights Reserved.

Where you are	The operational cost	What it looks like day to day	What removes it
Undiscovered accounts	Untracked exposure and audit gaps	Findings surface in an audit, not your inventory	Discovery that feeds enrollment
Vaulted, not rotated	Static credentials and standing risk	A leaked copy still works months later	Automated, dependency-aware rotation
Manual rotation	Toil and outage risk	Teams stop rotating after one breakage	Orchestrated rotation with retry and rollback
Standing privilege	Continuous attack surface	Access persists with no reason to exist	Just-in-time elevation with expiry
No session control	Blind spots in investigations	You cannot show what an admin did	Session recording and playback
Ungoverned non-human	Fast-growing blind spot	Service accounts no one owns	Service-account discovery and rotation
No certification	Audit prep as a fire drill	Reviews assembled by hand each cycle	Certification on a cycle

Non-human identities (NHIs) change the privileged inventory

NHIs have become the larger share of privileged access in many enterprises. Service accounts run scheduled work. Workloads and pipelines authenticate to deploy code and move data. AI agents now request access and act on it at machine speed. These identities hold secrets, and those secrets are privilege. A program that inventories human administrators alone measures a shrinking fraction of its own exposure. The first job of a 2026 PAM program is to see the privileged population, then decide what to do about it.

The growth here is not gradual. Each new automation, integration and model deployment creates more NHIs that authenticate and act. Each one needs a credential, and each credential is a standing path unless something governs it. A program that counts people alone is measuring the past. Chapter 5 returns to non-human identity in depth, because that is where the coverage gap is growing.

Copyright © Bravura Security Inc. 2026. All Rights Reserved.

THE COST

Scoping PAM to named administrators leaves NHIs uncounted. That gap bills you week after week in toil, audit fire drills and standing exposure.

WHAT GOOD LOOKS LIKE

You define privilege by the action, so each identity that can change a system comes into scope. Automation then turns recurring costs into scheduled, provable operations.

CHAPTER FAQ

What is privileged access management?

PAM is the discipline of controlling any account that can change a system. It governs who holds elevated access, when that access activates and what it does. That scope spans human administrators and NHIs such as service accounts, workloads and AI agents.

What counts as a privileged account?

A privileged account is any identity that holds elevated access, or can easily obtain it, to change a system. That includes editing configuration, reading or writing protected data, retrieving a credential, or deploying code. Human administrators, service accounts, application identities, workloads, pipelines and AI agents can each qualify.

Does PAM cover non-human identities?

It must. Service accounts, workloads and AI agents hold secrets and act with privilege, so they belong inside your PAM scope. Governance starts with service accounts, where discovery and dependency-aware rotation are well established, and extends toward broader non-human and agent identity over time.

What does incomplete PAM coverage cost?

It costs operational time and creates exposure. You pay in manual credential rotation, in audits that become reconstructions, and in outages when uncontrolled rotation breaks an application. You also carry standing credentials that stay valid and raise breach risk. Most of this cost recurs whether or not an incident happens.

How long do credential problems take to fix without automation?

Longer than most teams expect. The Verizon 2026 Data Breach Investigations Report found that resolving half of all weak-password and permission-misconfiguration findings in third-party cloud environments took almost eight months. Manual work does not clear that backlog. Automated, dependency-aware management does, because it removes the toil that causes the delay.

Copyright © Bravura Security Inc. 2026. All Rights Reserved.



CHAPTER 2

How PAM Relates to IAM and IGA

PAM controls the privileged action itself: the elevation, the session and the credential. It works alongside the rest of identity security rather than repeating it. Identity governance and administration, or IGA, governs who should hold access and proves it. Identity and access management, or IAM, decides who exists and what they reach. You will often see the terms used interchangeably. What matters behind each of them is coverage.

Copyright © Bravura Security Inc. 2026. All Rights Reserved.

PAM vs. IAM vs. IGA: three disciplines, three questions

PAM, IGA and IAM answer different questions, and the difference shows up in what breaks when one is missing. PAM controls what a privileged identity can do in the moment it acts. IGA runs the joiner, mover, leaver lifecycle, certifies access, and proves who should hold it. IAM establishes identity, authenticates it and decides what it should reach. You need the three working together. The table below sets them side by side.

Discipline	Question it answers	What it governs	Exposure without it
PAM	Who or what can use elevated access, for how long, and what did they do with it?	Privileged credentials and secrets, just-in-time access, brokered and recorded sessions	Standing admin rights, unrotated and hard-coded credentials, unrecorded privileged activity
IGA	Who or what should hold access, and can you prove it?	Joiner, mover, leaver lifecycle, entitlements and roles, access requests, certification, segregation of duties (SoD)	Access creep, SoD conflicts, complex audits
IAM	Who or what is this, and what should they reach?	Human and non-human identities, authentication, SSO and federation, access decisions	Unknown or duplicate identities, weak sign-in, access decisions that ignore context

Each discipline fails in a different way, and each failure has a different cost. Weak PAM means privileged credentials sit unrotated and sessions go unrecorded, so a compromised account acts freely and invisibly. Weak IGA means joiners, movers and leavers go unmanaged and access accumulates without review, so no one can prove who should hold what. Weak IAM means unknown or duplicate identities and weak sign-in, so access decisions rest on an identity you cannot trust. A program can be strong in one discipline and exposed in another.

Where the disciplines intersect

PAM does not stand alone. It hands off to IGA for certification: controlling access in the moment is one job, and proving who should still hold it is another. PAM also depends on IAM for identity truth, because a privileged session means little if the underlying identity is wrong. These disciplines coexist. A purpose-built PAM program runs alongside your identity platform rather than replacing it.

Copyright © Bravura Security Inc. 2026. All Rights Reserved.

This is also why coverage has to be measured across disciplines, not inside one. An identity platform that handles sign-in and federation well can still leave shared admin credentials unrotated. A governance tool that runs joiner, mover, leaver lifecycle and certifies access quarterly can still miss the service account no one owns. PAM closes the specific gap the others leave: control over the privileged action, in the moment, with a record. Bringing that control onto the same platform as identity and governance makes the handoffs clean rather than manual.

Certification is the proof point

Certification proves, on a cycle, who should still hold privilege, rather than just controlling who does. That is governance, and it is where PAM and identity governance meet. Control keeps the estate safe day to day. Certification is what lets you demonstrate it to an auditor. Without it, you can show what happened but not that it should have.

Bringing privileged access and certification onto one platform, the Bravura Security Fabric, makes that proof practical rather than aspirational. Convergence is something you grow into, not a package you buy, and you reach it from a PAM program.

PIM vs. PAM: where built-in identity tools stop

Many identity platforms include privileged features, such as role activation, conditional access and approval workflows for admin roles. These are useful. They often cover the cloud roles the platform itself governs, and they cover them well. The gap sits outside that boundary. Shared administrator accounts on servers, local admin credentials and service accounts with static passwords rarely live inside the identity platform’s reach. Network gear, legacy applications and mainframe accounts sit outside it too.

So the useful question is not which tool to choose. It is which privileged identities each one governs. Map your privileged population against both. Where the identity platform covers a role well, let it. Where a credential sits outside it, PAM takes the credential, rotates it, brokers the session and records it. Handled this way, the two coexist without overlap, and the gaps between them close. You add control where it is missing rather than replacing what already works.

Copyright © Bravura Security Inc. 2026. All Rights Reserved.

A NOTE ON PIM AND PUM

You will see two more terms alongside PAM. PIM, privileged identity management, is primarily a Microsoft Entra ID product term for managing privileged roles and their lifecycle. PUM, privileged user management, is a legacy term for shared account control that PAM has absorbed. You will often see both used interchangeably with PAM, but neither names a separate discipline. The practical test is the control behind the acronym. A role-activation feature does not rotate a shared service-account credential or record a privileged session. When a PAM requirement gets a PIM answer, ask which of the four questions from Chapter 1 it answers. Our comparison of **PAM, PIM and PUM**[4] goes deeper.

THE COST

Treating PAM, IGA and IAM as interchangeable leaves gaps between them, where an unrotated credential or an uncertified account slips through unnoticed.

WHAT GOOD LOOKS LIKE

Each discipline does its job and hands off cleanly. You can prove who exists, who should have access and what privileged identities did.

What identity should sign in to the PAM platform

The identity that enters the console is itself a privileged action, so tier it by risk. An identity platform authenticates the person. Bravura Privilege governs what that person does next. Low-risk credential retrieval can use an everyday account with multifactor authentication. Administrative work needs a separate, dedicated privileged identity, kept apart from daily email and browsing.

This closes a gap the four questions leave open. They govern the target credential. They do not say which identity should reach it. The answer follows the logic of the rest of the guide. Privilege is the action, not the account. So the login that starts privileged work deserves privileged control.

Tier the entry by what it can do. Reading a low-risk secret is not the same as opening an administrative session on a domain controller. Match the identity and the checks to the risk of the action behind them.

4 **bravurasecurity.com/blog/pam-vs-pim-vs-pum**

Copyright © Bravura Security Inc. 2026. All Rights Reserved.

For administrative access, Bravura Privilege brokers the session without disclosing the credential, authenticates each user, records activity and grants access just in time. The dedicated identity signs in, the session is attributed and recorded, and the elevated access expires with the task.

Keep a break-glass path for the times the identity platform or the PAM platform is unavailable. Store those emergency credentials under the same controls, and review their use after each event. A controlled exception is still a controlled account, not a standing back door.

CHAPTER FAQ

How do PAM and IGA work together?

PAM controls privileged access in the moment it is used. IGA certifies, on a cycle, who should still hold that access. PAM gives you control, and IGA gives you proof. Bringing both onto one platform makes certification part of the same program rather than a separate tool.

Do I need PAM if I already have IAM?

IAM establishes who exists and what they can reach. It does not rotate a shared credential, record a privileged session or grant access just in time. PAM adds that control. The two work together: IAM gives you identity truth, and PAM governs the privileged action on top of it.

What is the difference between PIM and PAM?

PIM, privileged identity management, is primarily a Microsoft Entra ID term for managing privileged roles and their lifecycle. PAM controls the privileged action itself: the elevation, the session and the credential. They overlap for privileged role lifecycle, and the terms are often used interchangeably.

Which identity should sign in to the PAM platform?

Treat the sign-in as a privileged action and tier it by risk. An everyday account with multifactor authentication can handle low-risk retrieval. Administrative work needs a separate, dedicated privileged identity. Bravura Privilege authenticates each user, records the session and grants access just in time.

Is an everyday identity platform account enough for admin access?

No. An everyday account, even with multifactor authentication, is exposed through daily email and browsing. Keep it for low-risk retrieval. Administrative work needs a separate, dedicated privileged identity, with each session brokered, recorded and granted just in time.

Copyright © Bravura Security Inc. 2026. All Rights Reserved.



CHAPTER 3

Coverage, and Getting There in Weeks

In this guide, coverage means how much of your privileged estate is under management. It has two dimensions. Breadth is which identities are under management: human and non-human, across your estate. Depth is how much control each credential is under: stored, rotated, session-controlled, dependency-aware. A vault gives you storage, not control. An unrotated vaulted credential stays an open path for anyone who once held it. Most programs fall short on both dimensions and cannot prove either.

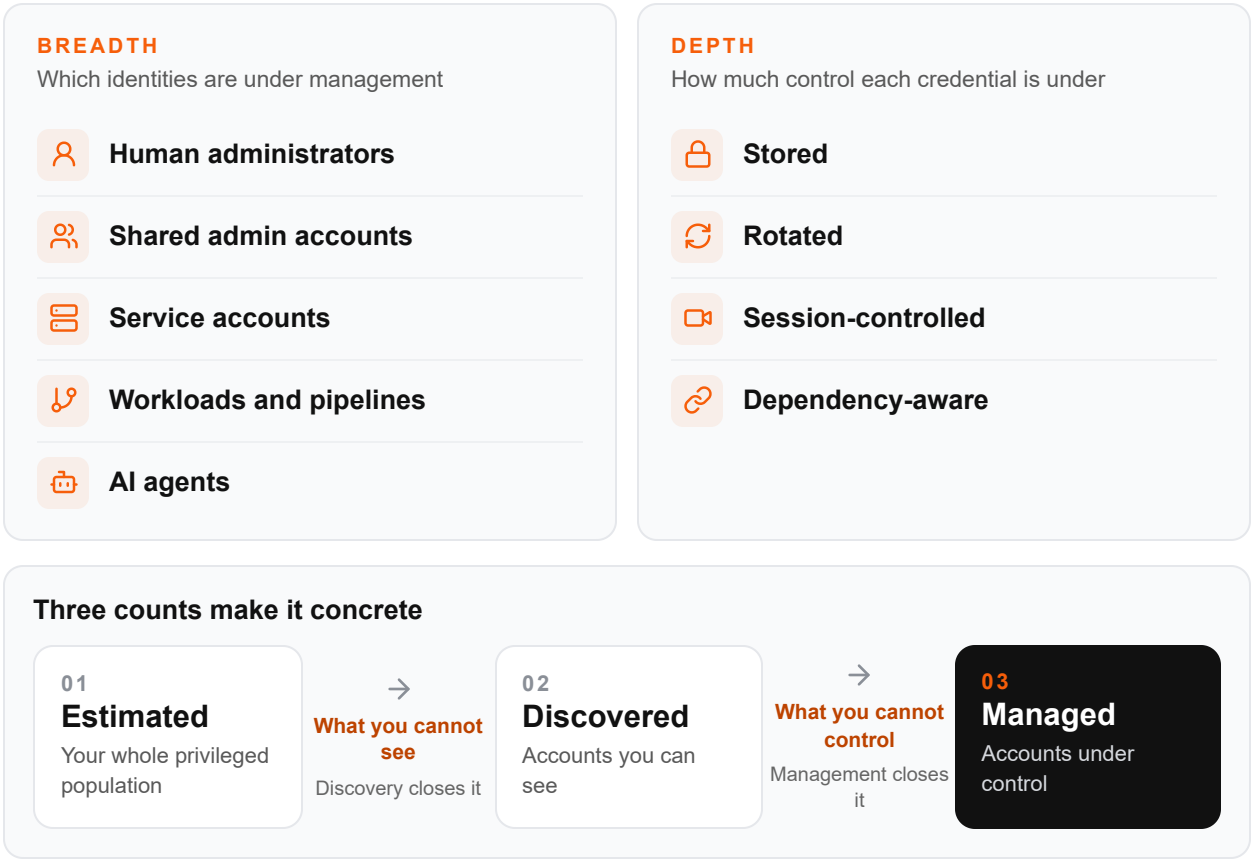
Copyright © Bravura Security Inc. 2026. All Rights Reserved.

How to measure PAM coverage: breadth and depth

Coverage is often reported as a single number, and that number hides the gap. Breadth asks which identity types you manage. A program that vaults human administrators but ignores service accounts has narrow breadth, whatever its dashboard says. Depth asks how much control each credential is under. A credential that sits in a vault but does not rotate has shallow depth. You need both. Measure them separately, and the real state of the program comes into view. Three counts make it concrete: privileged accounts estimated, discovered and managed.

The distance between those three counts is the story. The gap between estimated and discovered is what you cannot see. The gap between discovered and managed is what you cannot control. Both are exposure, and they are different problems. Discovery closes the first. Management closes the second. A program that reports one number tends to be reporting the smallest one, and hiding the two gaps behind it.

FIGURE 3 Coverage has two dimensions



Coverage has two dimensions: breadth, the identity types under management, and depth, the control applied to each credential. Discovery closes the first gap; management closes the second.

Copyright © Bravura Security Inc. 2026. All Rights Reserved.

Password vault vs. privileged access management

A vault stores a credential. Credential management under PAM discovers the account, rotates the credential, controls the session it opens and understands what depends on it. The distinction matters because a stored credential can still be a standing path. Someone who once checked it out may hold a copy. If it does not rotate, that copy still works. The table below shows the difference between a vaulted credential and a managed one.

Many programs reach the vaulting stage and stop, because vaulting feels like completion. Credentials are in one place, behind strong authentication, and the dashboard turns green. A vault, paired with a connection manager, can even launch a session with a stored credential. The problem is that a vault answers just the storage question. It does not rotate the credential, so a leaked copy stays valid. It does not record and replay the session, so you cannot review what happened after checkout. It does not track dependencies, so rotation risks breaking an application. Vaulting is real progress. It is a start, not the finish.

FIGURE 4 **Vaulted is not managed**

CONTROL	Vaulted only Stores the credential.	Under management Discovers, rotates and controls the session it opens.
Credential storage	✓ Yes	✓ Yes
Automatic rotation	✗ No	✓ Yes
Session recording and playback	✗ No	✓ Yes
Dependency-aware password changes	✗ No	✓ Yes
API-based credential retrieval at runtime	⚠ Possible but fragile	✓ Supported
Access revoked when role or privilege changes	⚠ Manual	✓ Policy-driven

A vault stores a credential. Full credential management under PAM discovers it, rotates it and controls the session it opens.

Copyright © Bravura Security Inc. 2026. All Rights Reserved.

Service account password rotation without outages

Rotation sounds simple until a password is in use somewhere you did not map. Consider a Windows service account. Rotate its password, and each dependent service that uses it needs the new value: Service Control Manager entries, IIS application pools, scheduled tasks. Dependency-aware management notifies those dependents automatically, with retry and rollback if one fails. Rotation without that awareness breaks applications. That is why teams stop rotating. Passwords then stay static for months, and the breach surface grows with them.

A team rotates a shared service-account password, a dependent service misses the new value, and an application fails at the worst time. After one outage, the team leaves that account alone. Dependency-aware rotation removes the fear by handling propagation, retry and rollback as one orchestrated step. The credential rotates on schedule and the applications keep running.

There is a second approach, and it solves the same problem from the other end. Rather than push a new password to each dependent, the application retrieves the current secret from the vault through an API each time it needs it. Because it reads the vault each time, a rotation cannot leave it stranded. That makes API-based retrieval an alternative to dependency-aware password changes, and different enough to plan for on its own. It suits automation and service-to-service calls well.

Rotation is technically possible with a vault alone, but fragile there. If the real password changes on the target outside the vault, the application retrieves a stale value and fails. The approach holds up when the vault manages the credential and stays the source of truth. Mature programs use both approaches, matched to each workload.

PAM implementation timeline: coverage at scale

Privileged accounts do not come under management at the same moment. A rollout protects some accounts first, then more, until the estate is covered. Time to coverage at scale is how long it takes to bring your privileged estate under management. It is not how fast the first few accounts are protected. An example makes the difference clear. A vendor can vault your first 50 admin accounts in a week. Covering the last few hundred service accounts, with their tangled dependencies, is the work that sets the real timeline. A phased rollout puts the first accounts under management in weeks, then works outward until coverage is complete.

The last 20% stalls because it holds the hardest identities. Shared service accounts carry tangled dependencies. Legacy systems, mainframe and network gear sit beyond the reach of a proxy-based tool. Time to first account rewards the easy start. Time to coverage at scale rewards the architecture that reaches the legacy and non-human parts of the estate. When you compare programs, ask how long full coverage took, not how fast the first vault filled.

Copyright © Bravura Security Inc. 2026. All Rights Reserved.

INDUSTRY LENS **Manufacturing**

Multi-site manufacturers often run legacy applications and mainframes alongside modern cloud systems. Shared service accounts on those legacy systems tend to go unrotated, because an outage at a plant costs more than the risk feels worth. Dependency-aware rotation and direct connection to legacy targets are what let coverage reach that part of the estate. Explore our approach to **identity security for manufacturing**[5].

Privileged account discovery: turn coverage into a number

Coverage is easier to act on when it is a number, and you can get one with a simple method. Estimate your privileged population, compare it against what is discovered and managed and name the segment that is vaulted but not managed. That segment is a depth gap in your coverage. Chapter 1 named what that gap costs, and Chapter 4 shows how to close the standing-access part of it.

Count by evidence, not intent. A program that plans to rotate credentials has not closed the gap until rotation runs and produces logs. Measuring what you can prove tells you two things at once: where you are today, and what the single next control is.

Count each segment separately: human administrators, shared accounts, service accounts and other NHIs. Human administrators on core servers may be managed and rotated while service accounts sit at discovered. A single program-level number averages those together and hides the weakest segment. The least-covered, highest-risk segment is usually the most useful next project, and it lets you report real progress while naming where the next investment goes.

THE COST

A single coverage percentage hides two gaps, the accounts you cannot see and the ones you can see but do not control, and both are exposure you are already carrying.

WHAT GOOD LOOKS LIKE

You measure breadth and depth separately, so you can name your privileged population, your managed share and the vaulted-but-not-managed segment in real numbers.

5 bravurasecurity.com/solutions/industry/manufacturing

Copyright © Bravura Security Inc. 2026. All Rights Reserved.

CHAPTER FAQ

Is a password vault enough?

A vault stores credentials, which is a start, not a finish. Management adds rotation, session control and dependency awareness. An unrotated vaulted credential stays an open path for anyone who once held it. Vaulting gives you breadth of storage; management gives you depth of control.

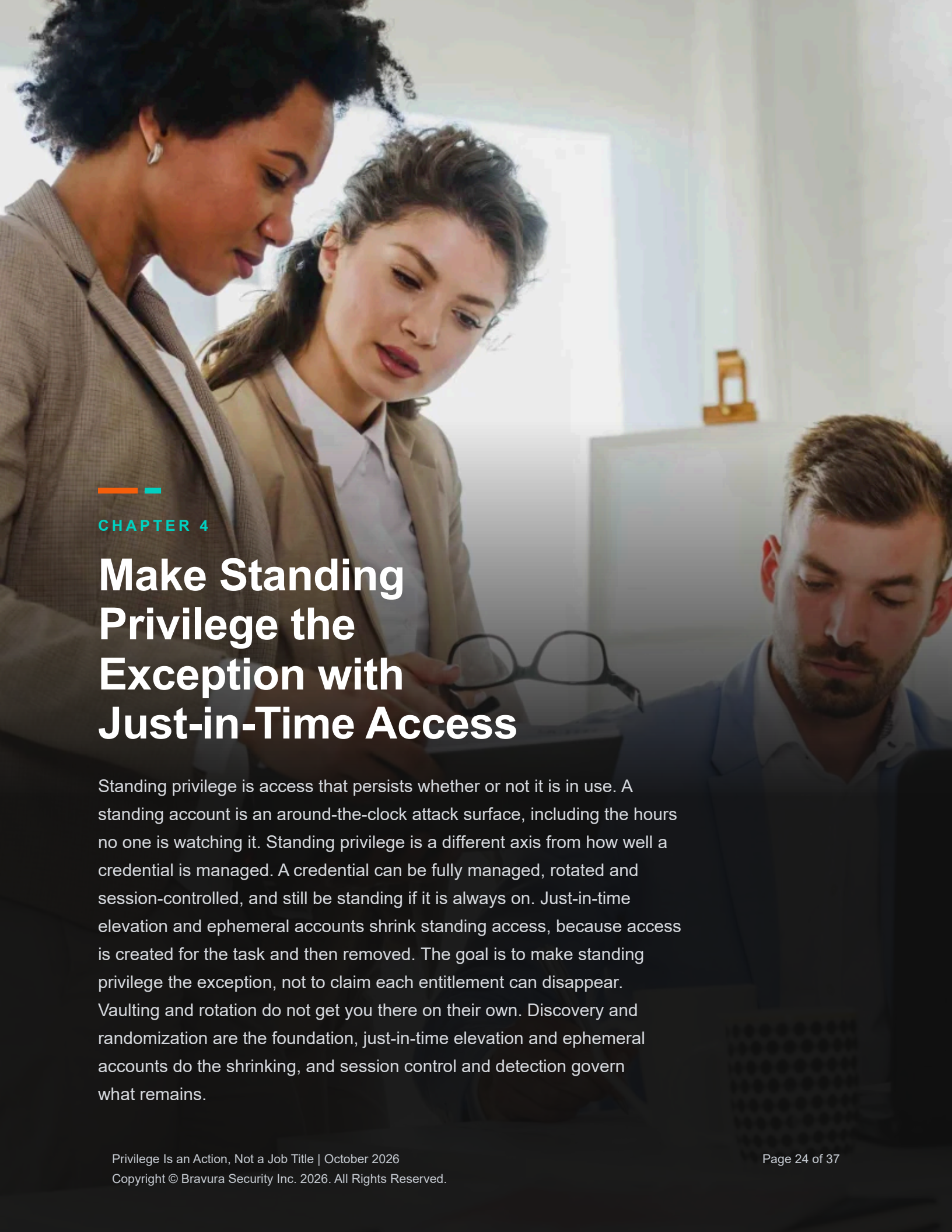
How long does PAM implementation take?

A phased rollout puts your first privileged accounts under management in weeks. The longer work is coverage at scale: dependency-aware rotation of service accounts and discovery that feeds enrollment. Time to first account is quick. Time to full coverage is the number worth planning around.

What is privileged account discovery?

Discovery finds the privileged accounts across your estate, human and non-human, including the ones no inventory lists. It is the first step in coverage, because you cannot manage what you cannot see. Strong discovery feeds enrollment automatically, so found accounts move into management rather than onto a spreadsheet.

Copyright © Bravura Security Inc. 2026. All Rights Reserved.



CHAPTER 4

Make Standing Privilege the Exception with Just-in-Time Access

Standing privilege is access that persists whether or not it is in use. A standing account is an around-the-clock attack surface, including the hours no one is watching it. Standing privilege is a different axis from how well a credential is managed. A credential can be fully managed, rotated and session-controlled, and still be standing if it is always on. Just-in-time elevation and ephemeral accounts shrink standing access, because access is created for the task and then removed. The goal is to make standing privilege the exception, not to claim each entitlement can disappear. Vaulting and rotation do not get you there on their own. Discovery and randomization are the foundation, just-in-time elevation and ephemeral accounts do the shrinking, and session control and detection govern what remains.

Copyright © Bravura Security Inc. 2026. All Rights Reserved.

Why standing privilege is a problem

Standing privilege is a problem because idle access is still live access. A credential that is always valid is always reachable, by the person who holds it and by anyone who takes it. Managing the credential well raises the cost of misuse. It does not close the standing window, because the access is still there when no one is using it.

This is why non-standing access became a goal in its own right. If access exists only while a task runs, there is almost nothing standing to misuse or inherit. The next sections show how to get there, and what to do about the access that must remain.

INDUSTRY LENS **Higher education**

Campus IT is distributed by design. Departments, research groups and central IT each run their own systems, many of them homegrown, and people change roles from term to term. That churn is how standing privilege accumulates: access granted for one project outlives it. Just-in-time elevation fits this pattern, because access expires with the task instead of waiting for someone to notice. On campus, federated and departmental accounts often double as admin logins. Require a separate privileged identity for elevated work, not the everyday federated account. Explore **identity security for higher education**[6].

The path to zero standing privilege

Some steps on this path are shared with most PAM programs. Discovery and automatic randomization are foundation work that a credible PAM program needs. They matter here, but they are table stakes. Two mechanisms do the specific job of shrinking standing access. Just-in-time elevation grants access for a task and expires it when the task ends. Ephemeral accounts exist only for the session and are removed after it. Session control and recording belong to a mature program too, but they govern and record the access that happens. They do not, on their own, reduce standing privilege. NIST SP 800-207, Zero Trust Architecture, calls for granting access to individual resources on a per-session basis. Just-in-time elevation applies that principle to privilege.

It helps to see these as one sequence. Discovery finds the privileged accounts. Randomization neutralizes their static passwords. Just-in-time elevation then grants access only when it is needed, and ephemeral accounts leave nothing behind. Skip the first two, and just-in-time has nothing solid to stand on. Bravura Privilege supports just-in-time access through several methods: time-bound elevation of an existing account, on-demand creation and removal of a temporary account, and just-in-time group membership. You pick the least-privilege option that suits each situation. Independent analyst research supports this flexibility as a strength.

6 bravurasecurity.com/solutions/industry/education

Copyright © Bravura Security Inc. 2026. All Rights Reserved.

Two controls, not one: shrink and detect

Just-in-time access reduces the chance of abuse. It does not remove it, because some access must persist, and any valid credential can be misused while it is live. A complete program pairs two controls. The first shrinks the standing window, through just-in-time elevation and ephemeral accounts. The second watches what remains, through monitoring for anomalies in activity carried out under a valid credential. Detection is a partner control in our approach, so you can pair just-in-time access with the analytics tool you already trust. The principle holds whatever the tool: shrink the window, then watch what is left.

A realistic word on the ideal state. Some standing privilege is hard to remove, because many enterprise applications still rely on persistent entitlements to function. The aim is not a number that reads zero on a slide. It is to make standing access the exception, to grant it just in time where you can, and to record and review whatever must remain. A program that treats total elimination as the sole pass mark will struggle to move off the starting line.

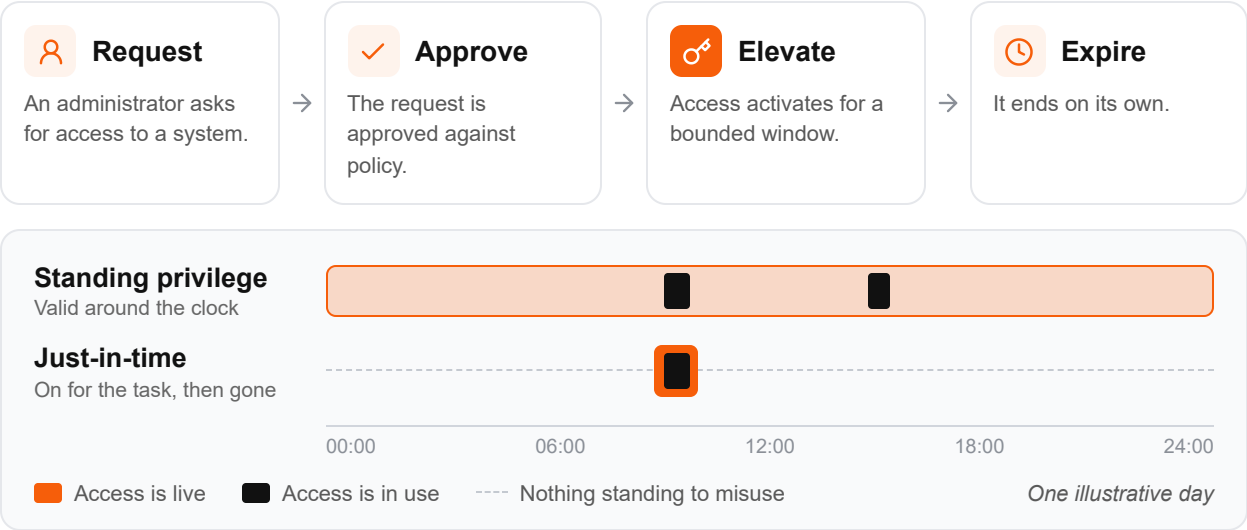
What just-in-time changes for the admin’s day

Zero standing privilege holds up when people use it day to day. The daily pattern becomes request, approve, elevate, expire. An administrator asks for access to a system. The request is approved against policy, access activates for a bounded window, and it ends on its own. Done well, just-in-time access adds little friction and removes a standing target. Done poorly, people route around it, and the standing accounts creep back. Experience determines adoption, and adoption determines whether the control is real.

This is why PAM programs should prioritize solving the operational constraints to adoption. A just-in-time system that is slow or confusing trains people to keep a standing account “just in case,” which defeats the point. A system that approves routine requests in seconds and gets out of the way earns the trust that keeps standing access rare. The goal is not to make elevation hard. It is to make time-bounded, recorded elevation easier than keeping a standing credential around.

Copyright © Bravura Security Inc. 2026. All Rights Reserved.

FIGURE 5 **Standing privilege vs. just-in-time elevation**



Standing privilege is access that persists whether or not it is in use. Just-in-time elevation makes it the exception: request, approve, elevate, expire.

From a coverage number to a remediation story

Chapter 3 turned coverage into a number and named the segment that is vaulted but not managed. Part of that segment is also standing: access that stays on whether or not it is used. Chapter 1 put a cost against the gap. This is where you close the standing part of it. Start with the always-on access your coverage count found. Randomize those credentials so no old copy stays valid. Move routine elevation to just in time, so access expires with the task. Record and review whatever must stay standing. Then count again. The first result is your before, and the smaller standing segment is your after.

The breach data shows why this matters. The **Verizon 2026 Data Breach Investigations Report** counts credential abuse at any point in the breach progression. On that measure it still sits on top, at 39% of the breaches studied. As a first entry point it fell to 13%, behind vulnerability exploitation. The report still calls credential abuse “a legitimate mitigation target chokepoint.” Removing standing credentials removes part of that surface.

Copyright © Bravura Security Inc. 2026. All Rights Reserved.

THE COST

Standing privilege is an around-the-clock attack surface, and misuse under a valid credential looks normal, so it is hard to catch before it happens.

WHAT GOOD LOOKS LIKE

Just-in-time elevation and ephemeral accounts mean access exists only for the task. Standing access becomes the exception, so few paths remain to inherit.

CHAPTER FAQ

What is zero standing privilege?

Zero standing privilege is a model where standing elevated access is the exception, not the default. Access is granted just in time for a task and expires when the task ends. Where an application still needs a persistent entitlement, that access is recorded and reviewed. Session control records what happens while access is live.

How do you remove standing privileges?

Start with discovery and automatic randomization, which are foundation work. Then add the two steps that shrink standing access. Just-in-time elevation grants access for a bounded window and expires it. Session control governs and records the elevated session. Where an entitlement must persist, record and review it. Vaulting alone does not remove standing access.

Is just-in-time access the same as zero standing privilege?

They are closely linked but not identical. Just-in-time elevation is the mechanism: access granted for a task, then removed. Zero standing privilege is the resulting state, where standing elevated rights are the exception. You reach that state by applying the mechanism, together with discovery, randomization and session control.

Copyright © Bravura Security Inc. 2026. All Rights Reserved.



CHAPTER 5

Securing Non-Human Identities (NHIs) and AI Agents

Machine identities hold a large share of the privilege in a modern estate. Service accounts, DevOps pipelines, APIs and AI agents authenticate, hold secrets, and act at machine speed and scale. Most programs govern the human share. Governing non-human privilege uses the same discipline as human privilege: discover the identity, control the credential, scope the elevation and record the action. The fundamentals come first, and service accounts are where that work is proven today.

Copyright © Bravura Security Inc. 2026. All Rights Reserved.

AI agent security starts with the fundamentals

Much of what makes AI feel dangerous is unmanaged privilege that was already dangerous. Take an unrotated service account, a shared admin credential or an entitlement no one certifies. These are the same exposure whether a person or an agent reaches for them. An AI agent does not invent a new attack surface so much as reach an existing one faster and at greater volume. Master the fundamentals and you remove most of that exposure. You also build the discipline the harder, AI-specific problems will demand.

The fundamentals are not yet universal, and that is the deeper issue. Discovery, zero standing privilege, just-in-time access, role-based access, certification and continuous authorization are familiar words and uncommon practice. Many organizations are still doing basic vaulting while shopping in a hurry for something to secure AI. Our own work on non-human and agent identity is the next step, not a substitute for the basics we already serve well. Your program is better served treating it the same way.

Why non-human identity, and why now

Your teams are already asking how to secure AI agents and machine identities. Start with the NHIs you can govern today. Service accounts are often the largest segment, and discovery and dependency-aware rotation bring them under control now. Apply the same controls as you add agents and workloads.

The timing matters for your program. Each automation and model you deploy adds NHIs that hold secrets and act. If your PAM program governs people alone, that gap widens with each deployment. Starting with service accounts is not a partial answer. It is the part of the non-human estate that is both large today and ready to govern. That is where effort pays back most reliably right now.

Service account management: the proven core

Service accounts are NHIs that already sit inside strong governance. We discover them across the estate, including the ones no inventory lists. We rotate their credentials with awareness of what depends on them, notifying dependent services and rolling back on failure. That dependency orchestration is the hard, documented work that makes non-human rotation safe rather than disruptive. A service account that holds broad access around the clock is standing privilege, and leaving it unrotated compounds the risk. Bringing service accounts under management closes a real part of the gap Chapter 3 described.

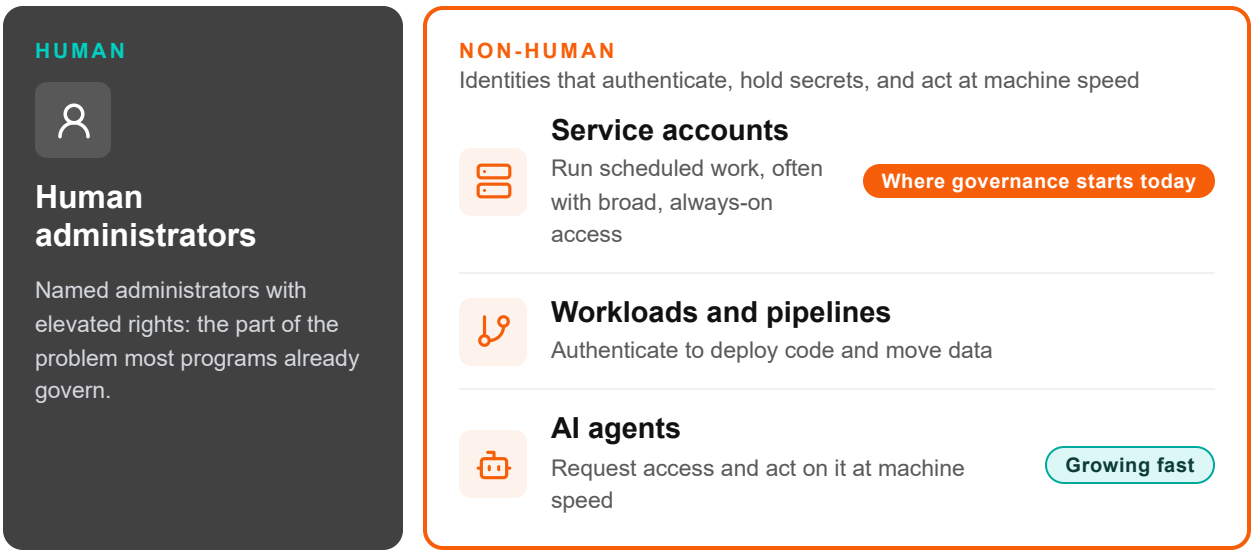
The reason service accounts are the right starting point is that they combine high risk with high readiness. They are numerous, they often hold broad standing access, and they are frequently shared and rarely rotated. They are also well understood, so discovery and

Copyright © Bravura Security Inc. 2026. All Rights Reserved.

dependency-aware rotation apply to them directly. You do not need a new, specialized technology to govern a Windows service account and its dependencies. You apply the same controls you use for human privilege, run at machine scale, with the specifics tuned to each case.

Secrets management extends to the code that uses them. Bots, scripts and pipelines retrieve secrets through a governed API instead of embedding plaintext credentials in code or config. Where code cannot change, a command-line utility injects the current password into config files or command-line arguments at runtime, so legacy applications you cannot rewrite still rotate on schedule.

FIGURE 6 **The non-human estate**



Non-human and AI-agent identities are a rapidly growing part of the estate. Service-account governance is where that work starts today.

One identity model for people, NHIs and agents

Bravura Identity and Bravura Privilege share one identity model across people, NHIs and agents. You design a control once and it spans governance and execution. Each non-human account pairs with a dedicated profile that names a responsible human owner. When that owner changes roles or leaves, the NHIs they own reassign automatically, so no account is orphaned.

Bravura Identity governs the lifecycle: onboarding through request forms, ownership, certification and retirement. Bravura Privilege controls the credentials those identities hold. Because both run on the same model, there is no stitching between the tool that knows who owns an NHI and the tool that rotates its secret.

Copyright © Bravura Security Inc. 2026. All Rights Reserved.

What agentic access changes

Agents break the oldest assumption in identity security: that a valid credential plus an authorized action equals a safe outcome. An agent can hold valid credentials and take authorized actions at machine speed, across systems, in ways no person would.

AI agents add speed, volume and delegation. An agent authenticates, holds secrets and can act on behalf of a chain of other identities. That raises the same questions PAM has asked from the start, now at a new scale. You still need to know which identity is acting, what it can do and whether you can prove what it did.

Delegation is the part that is genuinely new. When an agent acts for a chain of identities, the question of who is responsible gets harder. The audit trail has to capture the chain, not just the last actor. The market does not have a settled answer yet. Start now with the service-account work that is ready.

Provable control holds this together. Identity history, including profiles, attributes, roles and group memberships, is retained indefinitely by default, and stable identifiers track an identity even as its accounts are renamed. Privileged sessions are recorded, with detailed audit trails, risk scoring, and integration with your SIEM and SOAR platforms. When an auditor asks what an identity did, human or machine, you can show them.

Machine identity management beyond the cloud

Coverage is the benchmark, so it matters where your coverage runs deepest. Our non-human strength is the estate that sits outside the service mesh: Windows service accounts and their dependencies, legacy applications, mainframe and network gear. Discovery and dependency-aware rotation are established capabilities there, and that estate is what a workload-identity rollout most often leaves behind.

That estate is large, it is high-risk, and tools built only for cloud-native workloads tend to underserve it. Governing it well is the practical place to start, because most of the standing non-human risk lives there today. Run it alongside your cloud-native tooling, and the long-lived accounts that tooling does not reach stay governed.

The next section shows how the Bravura Security Fabric does this work across the identity types you run. It covers discovery and dependency-aware rotation for service accounts today, least privilege through policy and just-in-time control where it applies, and the audit trail that proves it.

Copyright © Bravura Security Inc. 2026. All Rights Reserved.

THE COST

A program that governs human privilege alone leaves a fast-growing non-human estate, service accounts and agents, holding standing secrets no one controls.

WHAT GOOD LOOKS LIKE

You apply the same four controls to service accounts today, and apply them to each new agent as it arrives. The largest non-human risk is under control now.

CHAPTER FAQ

What is machine identity management?

Machine identity management governs the NHIs in your estate: service accounts, workloads, pipelines and agents. It discovers them, controls the credentials and secrets they hold, scopes what they can do, and records their actions. Service accounts, with dependency-aware rotation, are where this work is most established today.

How do you secure AI agent access?

Apply the same discipline you apply to human privilege: discover the agent identity, control the secret it holds, scope its elevation and record what it does. How to govern delegation is still an open question for the market.

Are service accounts privileged accounts?

Yes. A service account authenticates and often holds broad, always-on access to systems and data, which makes it privileged. That standing access is a risk on its own, and leaving it unrotated compounds it. Bringing service accounts under discovery and dependency-aware rotation is a core part of PAM coverage, not an optional add-on.

Copyright © Bravura Security Inc. 2026. All Rights Reserved.

How We Help

We built **one platform for identity, privileged access and password management**[7]: the Bravura Security Fabric. For privileged access, that means Bravura Privilege, our **privileged access management software**[8], runs alongside the identity and password governance you already operate, rather than as a separate stack. Three qualities give you that coverage.

Hybrid coverage. We discover and manage privileged access across your estate: Windows service accounts and their dependencies, legacy applications, mainframe, network gear and cloud. Privileged access, identity lifecycle and governance run on one platform. Independent analyst research supports that unified design as a key point of difference, along with our breadth of integrations for older and cloud-based systems. Discovery finds more than accounts: it also maps entitlements, service dependencies, scheduled jobs and SSH trust relationships. The platform carries 140+ connectors.

Governance enforcement. We apply policy-driven elevation, broker access without disclosing the underlying credential and certify who should still hold access. Certification is part of the privileged access offering on one platform, the Bravura Security Fabric. Convergence becomes something you grow into, not a second product you assemble.

Operational resilience. We rotate credentials automatically, orchestrate dependencies with retry and rollback, and let automated processes pull secrets through an API. Independent analyst research also supports session management as a strength. We record screen activity and keystrokes, let reviewers watch sessions live or replay them later, and can end a session if monitoring drops. Bravura Security Fabric 12.10 adds session correlation logging for audit trail continuity, as documented in the **release notes**[9]. These are the controls that hold up when a program is under examination, not just on a slide.

Convergence means one identity model, one policy engine and one audit trail across identity, governance and privileged access. It does not mean one vendor for every control. We build depth where privilege risk concentrates and integrate where a specialist is stronger. Endpoint privilege management is the clearest example: we deliver it through a partner, so your endpoints get a specialist's depth alongside the controls in this guide. That focus gives you deeper coverage where risk concentrates. We have served over 1,200 organizations since 1992, and the platform is built for estates that are hybrid and long-lived.

7 bravurasecurity.com/products/bravura-security-fabric
8 bravurasecurity.com/products/bravura-privilege
9 docs.bravurasecurity.com/en/368628-12-10-0

Copyright © Bravura Security Inc. 2026. All Rights Reserved.

Where This Guide Fits Best

This guide is built for estates with privileged access to govern and an inventory to build against: hybrid, long-lived environments where accounts, dependencies and legacy systems accumulate. If you are still building a central directory or account inventory, start with discovery. It is the foundation for everything after it. If your estate is mostly cloud-native, breadth of coverage remains the benchmark, and the dependency guidance applies wherever long-lived accounts remain.

Guide FAQ

Where should we start?

Start with discovery, because you cannot manage what you cannot see. Count three numbers: accounts estimated, discovered and managed. Then bring the least-covered, highest-risk segment under rotation first. Chapter 3 shows the method.

What comes after vaulting privileged accounts?

Vaulting is the start. After it comes automatic, dependency-aware rotation, then session control, then just-in-time elevation so routine access stops standing, then certification that proves who should still hold privilege. Each step adds control and proof, and you add each one to what you already run.

How do we report coverage to leadership and auditors?

Report breadth and depth separately, by segment. Breadth is which identity types are under management. Depth is how much control each credential is under. Show the gap between discovered and managed as a number, and show it shrinking release by release.

How does PAM fit with the identity platform we already run?

It runs alongside it. Your identity platform establishes who exists and what they can reach. PAM takes the credentials that sit outside its reach, rotates them, brokers the session and records it. Map your privileged population against both, and add control only where it is missing.

Copyright © Bravura Security Inc. 2026. All Rights Reserved.

What should we ask a vendor before we buy?

Ask how long coverage at scale took for a comparable estate, not how fast the first vault filled. Ask whether rotation is dependency-aware, whether discovery feeds enrollment automatically, and how far the connectors reach into legacy, mainframe and network gear. Ask to see the three counts from a live deployment.

What changes for our administrators day to day?

The pattern becomes request, approve, elevate, expire. An administrator asks for access, policy approves it, access activates for a bounded window, and it ends on its own. Done well, it adds little friction and removes a standing target. Done poorly, people route around it, so adoption is the measure.

How does this relate to PAM maturity?

Coverage is the clearest measure of PAM maturity. The further your breadth and depth reach across human and non-human identities, and the more of it you can prove, the more mature your program. Measure each segment separately, and the least-covered, highest-risk segment tells you where to invest next. See where your program sits on our **identity and privileged access maturity model**[10].

Before You Go

You may be thinking one of three things, and each is fair. The first: “we already vaulted our privileged accounts.” Vaulting is real progress, and it is a start. The question is whether those credentials rotate and whether their sessions are controlled, because a stored credential can still be a standing path.

The second: “our identity platform already covers this.” An identity platform establishes who exists and what they reach. It does not usually rotate a shared credential, record a privileged session or grant access just in time. A purpose-built PAM program runs alongside it and adds that control.

The third: “we rely on help desk resets and manual reviews.” That is a starting point, not a failure. It does not call for a rip-and-replace. Add the next control to what you already run, starting with discovery and automatic rotation.

10 bravurasecurity.com/identity-and-privileged-access-maturity-model

Copyright © Bravura Security Inc. 2026. All Rights Reserved.

Bravura Security

See coverage on your own estate.

Book a demo[11] at bravurasecurity.com/request-demo.

11 bravurasecurity.com/request-demo

Copyright © Bravura Security Inc. 2026. All Rights Reserved.