BeyondTrust

A PAM Maturity Model

Effectively mitigate the ever-evolving risks of privilege and identity-based attack vectors by maturing your organization's Privileged Access Management.

BeyondTrust

TABLE OF CONTENTS

Introduction

We've heard the refrain ceaselessly these past several years—"it's easier for an attacker to log in than hack in" —especially for privileged accounts.

While it remains a best practice to patch or otherwise mitigate traditional software vulnerabilities, identity attack vectors (human and machine) have become the path of least resistance in this era of dissolving perimeters, hybrid infrastructure, and remote workforces.

When we dig deeper into identity security challenges and consider the best ways to build and evolve identity-first cyber defenses, we see threat actors specifically targeting privilege and privilege pathways (ways to escalate access that may be indirect or hidden and occur through identity vulnerabilities or weaknesses, such as misconfigurations, nested entitlements, shadow permissions, etc.)—to gain persistence in an environment. This is why privileged access management (PAM) is the keystone of modern identity security.

The most innovative and advanced PAM offerings are evolving to address identity challenges stemming from gaps in existing security solutions. They also address emerging use cases defined by relatively newer acronyms, such as cloud infrastructure entitlement management (CIEM) and identity threat detection and response (ITDR).

Despite significant cybersecurity investments, newer identity security use cases often remain underdeveloped, and foundational PAM controls are still not adequately mature. What's more, when addressed at all, these use cases are often handled piecemeal by several vendors and fragmented in implementation.

Maturing your PAM strategy isn't just about managing who has access to what. It's also about establishing trust in every interaction, embedding security controls into business processes enterprise-wide, and applying least privilege and identity hardening principles everywhere. This must be coupled with continuous verification that every identity and account behaves as expected.

Without a proactive, maturity-based approach to managing and securing identities and their entitlements, organizations face higher risks of obsolescence, poor security hygiene, incomplete deployments, and solution silos. These factors increase the likelihood of data breaches and attack-induced downtime, ultimately undermining the trust of both the business and its clients.

This guide provides a clear, pragmatic roadmap for advancing your identity security strategy with a privilege-centric approach. For most organizations, this journey will take them from basic coverage to an adaptive, intelligent defense found as their environment matures. We map five journeys covering the most common identity security use cases, each guiding you through milestones proven effective in the vast majority of commercial environments.

As you read on, we will challenge you to think differently about PAM and identity security: not as an obstacle, but as a powerful enabler of resilience, agility, and trust in a world where the attack surface is always expanding, and embracing maturity is the key to minimizing risk.

Journeying to a Mature PAM Posture

The journey to maturing your PAM deployment starts with quantifying the type of deployment your organization has adopted. Most PAM journeys are not single-threaded, but rather a combination of multiple paths executed simultaneously or, for the largest enterprises, executed independently by dedicated teams.

Regardless of an organization's size, each stage of this journey represents a reduction in the overall risk surface for the business and establishes a more robust security and compliance model for protecting the organization.

Below, we describe five maturity journeys in business terms, clarifying why an organization embraces identity security in the first place. Organizations can choose one or more of these paths to mature their deployments.

The PAM Modernization Journey

PAM modernization involves embracing updated identity security guidance to address new and emerging use cases in our environments. It should not only tackle these newer use cases, but also significantly improve productivity through intelligent workflows and automation. Modern PAM should seamlessly secure access to and from anywhere, while baking in auditing and oversight controls that simplify attestation reporting, access reviews, and compliance.

PAM modernization directly addresses the well-established fact that any identity can potentially be abused and lead to a path of privileged access. These paths proliferate rapidly within hybrid and multicloud environments, with many being indirect or hidden from the purview of most security toolsets. Today, organizations need to be able to understand and address the True Privilege™ of every identity, which encompasses all possible privileges, entitlements, permissions, and potential escalation paths.

In addition, organizations need to make policy-based decisions for authentication, authorization, and access. Modern PAM embraces dynamic identity knowledge, such as location, host, vulnerabilities, etc., to enact more intelligent, context-aware access decisions. This contrasts with legacy, and still largely prevalent, approaches to standing privileges. While just-in-time (JIT) access approaches have been touted for years, only recently have PAM toolsets emerged to effectively implement this important security model enterprise-wide, without disrupting workers.

The Security and Governance Journey

Organizations frequently experience internal friction between Security and Governance, Risk, and Compliance (GRC) teams. An ideal state of organizational maturity is achieved when these teams align on the same goals, creating security by design and integrating compliance reporting and auditing into daily business practices.

With regard to PAM, a mature state is reached when certification reviews, session monitoring, behavioral analysis, and entitlement attestation reporting are seamless, automated, and routine across all business operations. PAM security and governance maturity implies that security controls are well-understood throughout the teams. It means GRC can establish metrics to routinely measure the effectiveness of controls and identify when events might introduce unnecessary risk. This includes improving joiner, mover, and leaver processes associated with Identity Governance and Administration (IGA), eliminating and managing shadow IT, and demonstrating tangible results from initiatives like zero trust.

Organizations leveraging cloud environments often face even more complex barriers in balancing security and governance. The cloud has always promised agility and rapid time to value, cultivating an environment where developers can build quickly and with ease. However, this also makes it easy to overlook or bypass proper security considerations. As a result, secrets sprawl across more environments, causing least privilege and access reporting to become a larger task. Cloud PAM maturity is achieved when there are clear lines of sight into what exists in the estate, and security becomes a byproduct of proper cloud development and configuration, backed by automated access reviews and simplified compliance.

The Journey for Least Privilege Defense in Depth

Defense in Depth is a longstanding security concept that focuses on constructing multi-layered protection. Least privilege is itself a fundamental security principle that can be applied to humans, machines, systems, and processes throughout an organization. Implementing multi-layered least privilege can provide a strong, proactive defense in depth against internal and external threats.

While we are far from having one tool that can apply the principle of least privilege across every practical use case, most organizations also have plenty of room to make progress from the current highly fragmented approaches to least privilege. Privileged access management capabilities are central to any least privilege strategy. The more PAM capabilities an organization has, and the better integrated they are via a single platform, the more mature and effective its least privilege approach will tend to be.

Some areas where PAM enforces least privilege include:

- Endpoints and applications
- Identities and accounts
- Sessions
- On-premises, hybrid, and cloud environments

It's important to clarify that "endpoints" here refers not just to an end user's workstation, but any asset connected to a network as a last hop. Examples include servers, workstations, mobile devices, and assets owned by the organization or entities outside the traditional corporate perimeter. Essentially, any device connected to a network or the Internet that serves as an IP destination, and does not route or bridge network traffic as its primary business function, is an endpoint.

With this in mind, defense in depth encompasses all the hardening, configuration, and agents within a standard build image. This layered approach aims to protect against malware and facilitates patch management, content filtering, vulnerability assessments, and more.

It's well-established that end users operating with administrator privileges present a higher risk for malware infection, ransomware, or other types of vulnerability exploitation, including identity attack vectors. With a least privilege defense-in-depth approach, an organization can protect against modern attack vectors from many different angles, reducing breach risk, while also minimizing the blast radius of any successful attack.

A maturity model for least privilege defense in depth includes use cases such as:

- Removing and/or managing all local administrative accounts
- Providing step-up authentication for sensitive applications
- Integrating change control into privileged requests and software installation
- Making policy-based decisions for any elevated entitlements

Ultimately, this defense-in-depth approach should define the maturity of your identity security journey by adding multi-layered least privilege to your security discipline, either natively or through PAM products such as Endpoint Privilege Management (EPM), Privileged Password Management, Cloud Infrastructure Entitlement Management (CIEM), and more. Importantly, the concept of least privilege should be implemented seamlessly into operations without introducing workflow burdens. This maturity is critical for user acceptance and adoption, ensuring complete coverage throughout an organization.

The Journey to Securing the Modern Workforce

In today's hyper-connected world, employees, contractors, auditors, and vendors can operate from nearly anywhere, at any time. Supporting this flexibility requires IT and Security teams to adapt their solutions to improve productivity, while maintaining or exceeding the level of security of their in-office environments. While we may still protect sensitive assets in data centers with firewalls and network segmentation, remote workers and cloud-based solutions bypass these traditional network-based IT and security tactics.

Securing environments outside a traditional perimeter represents numerous challenges and pitfalls for organizations, such as unsecure networks or unknown operations in distributed or foreign geolocations. Moreover, when operating in the cloud, you no longer own the hardware and software; in most cases, you're merely licensing it from someone else.

Most cloud providers follow a shared responsibility model, meaning you, as the customer, are still responsible for securing what runs on the infrastructure—identities, apps, data, and configurations. While the cloud provider secures the infrastructure itself, it's crucial for customers to properly configure their cloud services to avoid security gaps. Simply put, securing the modern workforce needs a technology boost to vet host security, enforce the principle of least privilege (PoLP) everywhere, provide high confidence in identity authentication, and secure remote access technology without creating unnecessary attack paths.

Maturing the PAM journey for the modern workforce entails:

- Limiting or removing native operating system protocols like RDP and SSH
- Replacing legacy access technologies like virtual private networks (VPN)
- Performing session recording and monitoring for privileged activity
- Implementing zero trust architectures and just-In-time (JIT) access to eliminate standing privileges

The ultimate goal is to instill confidence in every identity that requests access and to provide oversight by monitoring all operations for appropriate activity, regardless of whether the session is privileged.

The Journey to Streamlined PAM and Vendor Consolidation

In recent years, organizations have grown more mindful of vendor sprawl. This has cast a spotlight on the goal to reduce the number of vendors in their supply chain. The benefits of vendor consolidation can include better price negotiations, less management overhead, a lower risk surface from supply chain attacks, and so on.

Even if you must move to new vendors that cover multiple use cases during this process, the costs of migration can be offset by the cost savings in licensing, training, and administrative overhead across fewer vendors.

When considering your current identity security and PAM deployments, this approach is a viable way to save costs and streamline your identity security, while also benefiting from integrations and synergies between a single vendor's products. For example, managed secrets could be auto-injected into remote sessions, or end-to-end zero trust architecture (ZTA) could be leveraged to solve secure remote access problems.

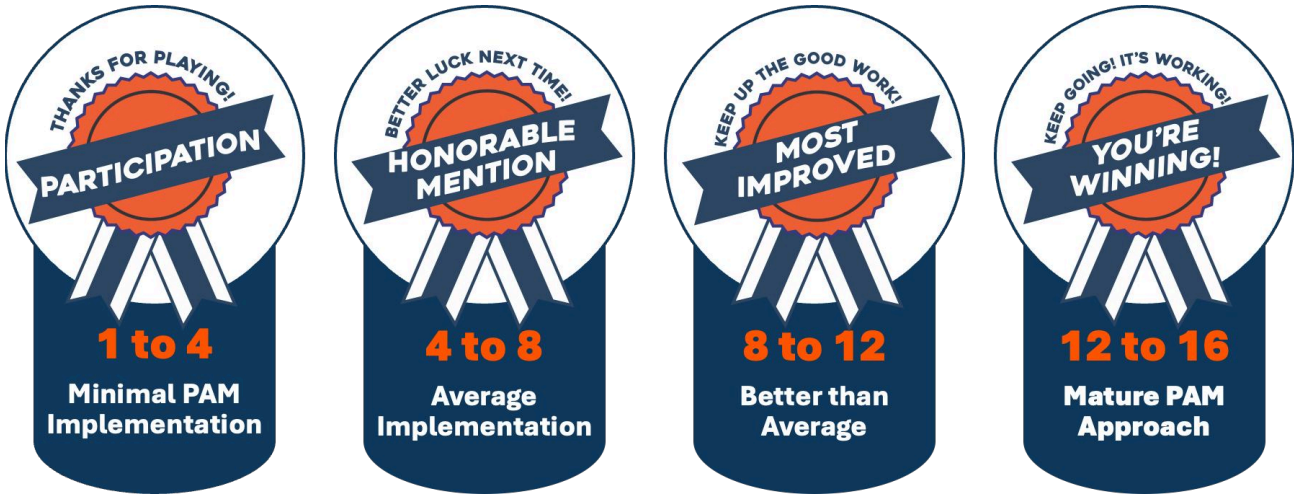
While vendor consolidation can address many security use cases, the key takeaway for your own maturity journey is efficiency. Whether that efficiency is realized via a common user interface, consolidated reporting, or simplified Role Based Access Controls (RBAC), using one vendor to manage multiple security disciplines makes sense, just like having one Identity Provider (IdP), or one vendor for multi-factor authentication (MFA).

PAM Maturity Test

Now that we understand the potential routes for your privileged access management (PAM) journey, it's time for a quick test to assess your organization's overall PAM maturity.

This PAM Maturity Questionnaire is comprised of sixteen questions, broken into four categories representing the most common business reasons organizations embrace privileged access management. For each question, award yourself one point if your organization can truthfully meet the objective.

Category	Question	Point(s) (yes is 1, no is zero)
Mitigate risk, or reduce the impact, blast radius, or recovery time of a potential breach?	Are you eliminating standing privileges through just-in-time (JIT) access?	
	Can you provide real-time visibility into privileged or suspicious activity through logs or a SIEM integration?	
	Does your implementation restrict lateral movement by enforcing least privilege everywhere?	
	Does your PAM implementation include AI-driven anomaly detection and automated remediation?	
Reduce overall operational costs?	Does your PAM implementation have a single interface for all users?	
	Can you automate common or frequent privileged access tasks and workflows?	
	Does your PAM implementation integrate with IGA or change control?	
	Are you sole-sourced (one vendor) for your PAM solutions?	
Better alignment with compliance objectives?	Does your PAM solution provide session recording / monitoring?	
	Does your PAM solution have built-in compliance frameworks (NIST CSF, etc.) and reporting for vertical markets (PCI, etc.)?	
	Does your PAM implementation support business continuity requirements?	
Protect the business and reduce the overall risk surface?	Does your PAM solution support cloud, multicloud, and SaaS initiatives through cloud-native security controls?	
	Can you enable and control secure remote work and clientless third-party access without a VPN?	
	Does your PAM implementation facilitate DevOps through automated privileged access workflows?	
	Can your PAM solution automatically scale and contract licensing to meet business demands and seasonal activities?	
	Does your PAM implementation increase operational efficiency (JML, mouse clicks, etc.), while improving security?	
Total		



For these scores consider:

- **Minimal to no PAM Implementation, 0 to 4:** Your organization has minimal to no PAM or identity security coverage, indicating high risks and significant vulnerability to modern identity attack vectors.
- **Average Implementation, 5 to 8:** You have a traditional PAM implementation, likely focusing on one journey that is relatively mature, with minimal effort or coverage for other PAM/ identity security use cases.
- **Better than Average, 9 to 12:** Your organization has implemented multiple PAM maturity journeys. While good, there's still significant room for improvement with more complete coverage, additional use cases, and further effort to achieve best-in-class deployment.
- **Mature PAM Approach, 13-16:** Your organization is engaged in multiple journeys with many of them achieving foundational and modern PAM controls. Organizations that score in this range are generally considered best-in-class, but can still benefit from newer features and continuous refinement to further minimize risk, while supporting productivity.

Maturing your PAM Approach

But what does the "ideal state" of a mature PAM approach for you look like? Privileged access management maturity refers to an organization's ability to consistently manage and improve its security posture over privilege and access escalation pathways over time. It reflects how well an organization identifies, manages, protects, detects, responds to, and recovers from privilege- and identity-related attack vectors. A mature PAM program moves beyond ad hoc or reactive measures and is guided proactively by formal policies, risk assessments, continuous monitoring, and strategic alignment with business goals.

Maturity models provide structured frameworks for assessing various levels of maturity. These stages range from inchoate or absent approaches, where practices are informal and inconsistent, to advanced, where PAM is fully integrated and continuously improved to address a broader swath of critical identity security use cases. High maturity levels not only indicate the presence of technical defenses, but also a culture of identity threat awareness, governance, and resilience.

The model presented later in this document is not absolute. It's designed to provide guidance and should be reviewed and customized by teams to meet their unique business objectives. Each stage of PAM maturity is benchmarked by measures of adoption, use cases, features, and overall coverage within an organization.

If you can't demonstrate adoption, coverage, and use cases, then it's technically impossible to move to the next level in the maturity model. For example, only removing administrative rights in the sales department—but not for developers or for remote workers—doesn't qualify for moving higher in the maturity model.

Finally, when reviewing the maturity model, consider this legend:

- **Level:** A simple way to define each category in the maturity model by number, 1 to 5.
- **Percentage:** The percentage of defined use cases for each level accomplished by the organization. For simplicity, these are broken down into 25 percent increments in the model, and each level should have one or more defined milestones.
- **Coverage:** A value for coverage is intentionally absent from the model. This is user-definable and represents the percentage threshold for deployment coverage that must be complete to mark a level finished and proceed to the next one.
- **Title:** An abstract term, covered below, to describe each level in the maturity model. These include:
    - Absent: Minimal or no technology, policy, or procedures are in place or enforced for the journey.
    - Ad hoc: Policies and procedures may be in place, but enforcement is loosely governed, and coverage extends only to select assets, users, and environments.
    - Standardized: Policies and procedures are implemented and enforced for specific assets, workflows, and users. Exceptions and coverage can vary widely throughout the organization.
    - Managed: Policies and procedures are widely adopted, almost always enforced, and tested for compliance, minimizing the overall identity security risk surface. Technical debt from legacy deployments may be present, but only for specific use cases.
    - Advanced: Coverage, policies, and procedures are fully adopted across the enterprise for the specified journey. Modern, best-in-class approaches are embraced, and technical debt from legacy deployments has been eliminated.

The Maturity Model for Privileged Access Management

Now, let's look at the actual maturity model. You'll notice a correlation between your assessment score and your organization's business use cases and journeys. For instance, a low score likely indicates you've embraced only one journey, potentially reflecting an ad-hoc or standardized environment. Conversely, a high score suggests your organization covers multiple journeys, though some key milestones for maturing PAM and identity security might still be lacking.

With that in mind, please review the table below and consider if you are fulfilling each use case within your organization. And remember, this model isn't absolute. You might disagree with certain entries due to specific business reasons, and that's perfectly fine. You're encouraged to customize them based on your unique business objectives.

For example, if you're standardizing on Google Chromebooks as your endpoint operating system, many items in this journey become moot. However, the applications accessed remotely may still require password management or a passwordless approach for access.

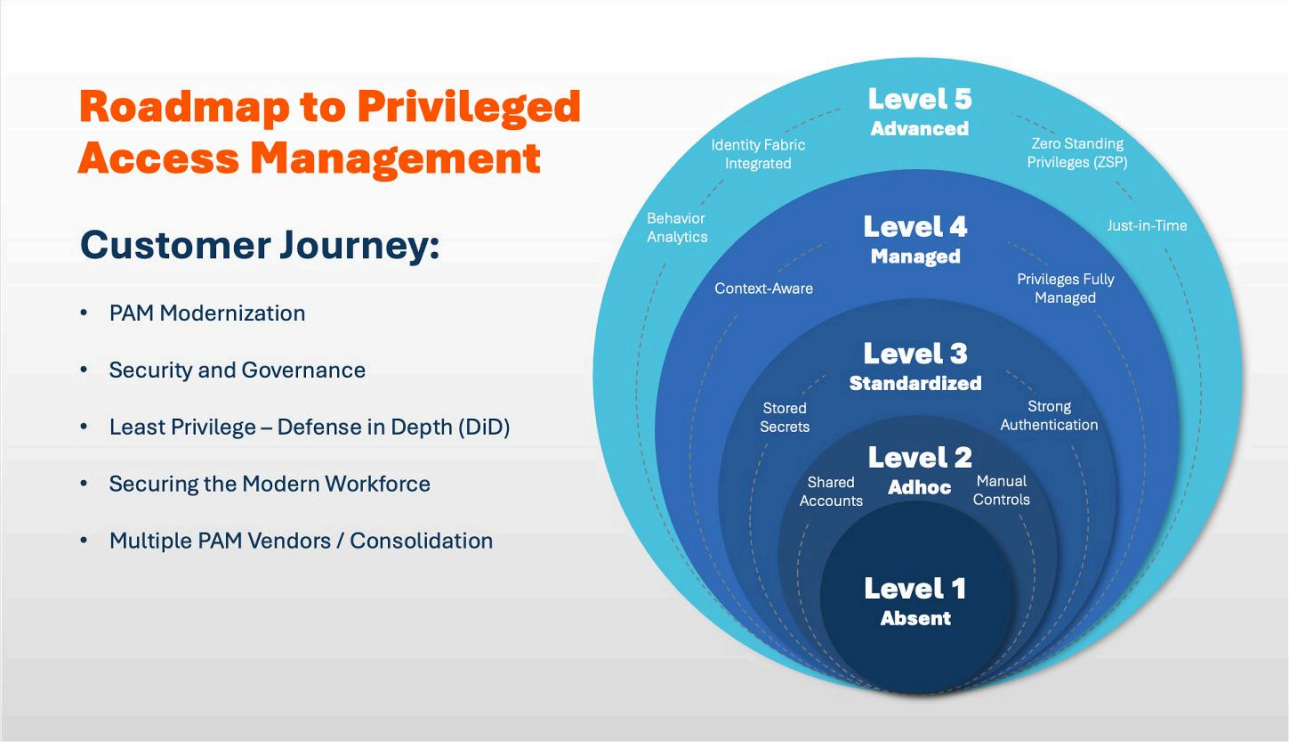
Please note that the individual entries for coverage and maturity in the table below should be adjusted to meet your own business requirements **and do not follow a linear horizontal progression.** Each cell below represents recommended milestones that can stand on their own.

Journey	Level 1 - 0% Coverage % Absent	Level 2 - 25% Coverage % Ad hoc	Level 3 - 50% Coverage % Standardized	Level 4 - 75% Coverage % Managed	Level 5 - 100% Coverage % Advanced
PAM Modernization	No visibility into privileges or entitlements, and no concept of True Privilege. Limited controls to verify who is using which account and when. No shared account password management. Lack of accountability for access and activity. Rampant standing privileges.	Manual controls and processes for privileged access. Audit trail isn't reliable and may have missing or inconsistent information.	Automated discovery, inventory, and onboarding. Limited password management with workflow approval and automated rotation. Privileged account usage reporting and certifications. Some standing access is eliminated.	Passwordless session access and management. Context-aware privileged access using RBAC, ABAC, and MFA. Minimized standing privileges through full enablement of a JIT model.	Holistic, cross-domain visibility and understanding of identities, entitlements, and access escalation pathways, including knowing the True Privilege of every identity. Identity fabric (IAM, IDP, IGA, SSO) integrated. Advanced coverage (Cloud, SaaS, Apps). User behavior analytics. Identity hygiene analysis using AI.

Journey	Level 1 - 0% Coverage % Absent	Level 2 - 25% Coverage % Ad hoc	Level 3 - 50% Coverage % Standardized	Level 4 - 75% Coverage % Managed	Level 5 - 100% Coverage % Advanced
Security and Governance	Unknown and unmanaged privileged access. Faults in joiner, mover, and leaver process. Potential for default, re-used, clear text, or guessable secrets.	Manual access reviews for privileged activity. Privileged accounts are shared across multiple identities. Implementation of secrets management best practices (rotation / dynamic generation, complexity, etc.) is manual and faulty.	Privileged secrets are stored but not managed or automatically rotated. Workflows for privileges or entitlements are inconsistent, but gated. Compliance enforcement for secrets complexity, age, etc. is enforced and reviewed manually.	Privileged identities are identified and managed, and access is gated using standardized workflows. Dormant and shadow IT accounts are identified and mitigated. Secrets management for machine identities follows documented procedures.	All access is just-in-time. Zero standing privileges (ZSP) achieved. All privileged access follows internal policies, and deviations can be identified in real time.
Least Privilege Defense in Depth	Unmanaged users have direct administrative privileges, entitlements, or access to local, remote, or cloud assets.	Users have admin accounts that can be used for ad hoc access with no verification. Identities have administrative accounts with standing privileges. Identities have direct access to local admin accounts that may or may not be directory services managed.	Local admin privileges are managed via directory services. Limited allowlist and blocklist access per application, based on privileged policies. System admin account passwords are centrally managed and retrievable.	Policy-based access to applications requires privileges. Workflows for privileged escalation are enforced and can provide attestation reporting. All local privileged accounts are managed, rotated, and centrally retrievable.	Context-aware access policy (user risk, asset risk, ITSM validation, MFA). IAM integration with separation of duties by policy or role. Policies are definable by identity, role, namespace, asset, etc. and are dynamic.
Securing the Modern Workforce	Internet-exposed remote access protocols (SSH, RDP, etc.) present. VPN access is allowed into multiple private networks.	Remote access via VPN or remote proxy has some segmentation. User behavior and sessions are unmonitored. Unmonitored remote authentication and lateral movement.	Devices delegated for remote access are segmented and a bastion host is provided for remote access. Strong authentication is enabled. Remote authentication is directory services integrated.	A workflow is implemented with managed accounts to access internal resources per role. Activity and sessions are monitored for inappropriate behavior and lateral movement. Remote access follows a model of least privilege.	Just-in-time access is provisioned to users only when appropriate or needed. Activity and sessions are recorded, archived, and monitored for inappropriate activity. Network tunneling is permitted per application, port, and protocol, using advanced remote access technology.

Journey	Level 1 - 0% Coverage % Absent	Level 2 - 25% Coverage % Ad hoc	Level 3 - 50% Coverage % Standardized	Level 4 - 75% Coverage % Managed	Level 5 - 100% Coverage % Advanced
Multiple Vendors / Consolidation	Partial coverage or no PAM strategy present within the organization.	Select systems under PAM management. Escalation pathways not protected or monitored.	At least one PAM discipline has proper coverage. Integration use cases for PAM haven't been realized.	Multiple integrated PAM solutions. Integration into identify fabric. Identity security prioritized.	Security best practices like zero trust are required. PAM platform, journey, and integration optimized for the business. Vendor consolidation for best-of-breed technologies and optimized cost-savings.

This table can be visualized in the following chart to simplify goals and expectations within an organization.



"Start, Stop, and Continue" for Leveraging a PAM Maturity Model

"Start, Stop, and Continue" is a deceptively simple, yet powerful, feedback framework businesses use to refine practices, clarify priorities, and drive continuous improvement. When applied to cybersecurity, it provides a practical, introspective toolkit that enables teams to identify actions to initiate ("Start"), behaviors and workflows to eliminate ("Stop"), and practices worthy of maintaining or expanding ("Continue").

✪ "Start" encourages innovation and new efficiencies, fostering adaptability and agility with best practices to solve legacy and newer challenges.

✘ "Stop" shines an uncomfortable, albeit essential, spotlight on ineffective or harmful practices and is designed to remove obsolete practices and bad habits.

✓ "Continue" validates successful strategies, anchoring teams to proven strengths and boosting morale.

Combined, these three lenses offer concise, actionable clarity, helping leaders sift through complexity and hone their operational focus. When this is directly applied to our maturity model and journey, we can make some distinct recommendations every organization should embrace.

Journey	Start	Stop	Continue
PAM Modernization	✪ Passwordless privileged access ✪ Just-in-time (JIT) access ✪ Zero trust architectures for access workflows ✪ Demonstrable regulatory compliance ✪ Preemptive identity security ✪ Prioritizing OT, clinical, and non-human identities (NHI) for privileged access management	✘ Checking out passwords and secrets with copy and paste ✘ Using client/agent-based VPN access for contractors, vendors, and employees ✘ Using secondary accounts for local privileged activity, regardless of role ✘ On-premises software installations for PAM (when possible, air-gapped)	✓ Prioritizing solving the problem around potential escalation pathways ✓ Including identity security in your future business plans based on risk scoring ✓ Embracing AI for identity security and threat detection

Journey	Start	Stop	Continue
Security and Governance	✪ Embracing compliance as a form of validation and assurance ✪ Mapping compliance requirements as the minimum required control ✪ Building compliance dashboards ✪ Alerting on non-compliance for any controls	✘ Treating compliance as a burden and afterthought ✘ Segmenting each compliance initiative as a separate process ✘ Treating cloud and on-premises security as different initiatives using disparate technologies	✓ Adopting security best practices for each environment, by discipline ✓ Leveraging platform solutions that support advanced integrations to achieve security and governance requirements ✓ Unifying on-premises and cloud-based identity security controls and technology
Least Privilege Defense in Depth	✪ Enforcing the principle of least privilege across all accounts and access ✪ Removing excessive privileges and entitlements for all non-human identities ✪ Managing all privileged accounts, including all types of secrets and owners ✪ Implementing and automating machine identity security with least privilege principles and secrets injection	✘ Giving end users administrative rights ✘ Giving non-human identities excessive privileges for application-to-application integrations ✘ Provisioning standing privileges and shared accounts (if possible) ✘ Enabling interactive logins for service accounts	✓ Discovering and identifying both human and non-human identities for all projects ✓ Replacing EOL assets with supported solutions and supporting EOL equipment when deprecation is not an option through advanced security controls (isolation, lockdown, etc.) ✓ Eliminating static credentials, whenever and wherever possible

Journey	Start	Stop	Continue
Securing the Modern Workforce	✪ Using bastion host technology to proxy all remote access ✪ Providing session management, including session recording and behavioral monitoring, for remote sessions ✪ Embracing security initiatives like zero trust ✪ Removing legacy VPN technologies ✪ Embracing ephemeral credentials and (when possible) using credential injection when systems are accessed remotely	✘ Enabling RDP, SSH, HTTP, etc. for external usage ✘ Allowing broad VPN access to private networks ✘ Providing broad administrative credentials to the service desk, contractors, vendors, etc. ✘ Manually creating privileged accounts with remote access ✘ Allowing vendors to use their own remote access solutions	✓ Identifying remote access use cases and how they can be secured using modern best practices ✓ Consolidating remote access technology for contractors, vendors, and employees ✓ Auditing all remote access, regardless of role and function
Multiple Vendors/ Consolidation	✪ Licensing best-of-breed PAM solutions from a sole provider based on a platform ✪ Embracing advanced use cases that support modern security best practices ✪ Ensuring PAM solutions can manage and mitigate the risks for every privileged account in the organization ✪ Training users that PAM is the responsibility of all employees	✘ Licensing solutions from multiple PAM vendors ✘ Limiting PAM deployments to only select assets and accounts ✘ Installing software only (installers) PAM solutions, due to overhead costs and maintenance	✓ Focusing on identity security to mitigate and reduce risk ✓ Managing privileged accounts as a high-risk resource within the organization ✓ Improving joiner, mover, and leaver processes ✓ Partnering with strategic vendors and partners to provide the best solution for your organization

Knowing Where You Are and Mapping Where You Want to Go

Maturing your organization's PAM and identity security emphasizes the critical need for proactive digital identity protection from both human and non-human threats.

To defend against the sheer volume—and ever-increasing sophistication—of identity-related cyberattacks, individuals and organizations must move beyond reactive security measures toward dynamic authentication, privileged assessments, and continuous regulatory compliance—regardless of where employees, contractors, and vendors operate.

Ultimately, we're each in charge of our own identity risk posture. By implementing identity security best practices, maturing our PAM deployments, and understanding our legal obligations for security and data privacy, we can minimize cyber risks for ourselves and our organizations.

Take Your Next Step Toward PAM Maturity with a No-Cost Identity Security Risk Assessment

Maturing your Identity Security, including PAM, begins with understanding your current maturity levels and risk posture. Take advantage of BeyondTrust's Identity Security Risk Assessment offer at no cost. See and understand identity-based risks, including True Privilege, within 24 hours.

- Achieve a unified view of identities and privileges across domains and connected systems, and understand your entire identity attack surface.
- Uncover unseen pathways and identity-based vulnerabilities attackers could exploit to gain privileged access.
- Apply prescriptive recommendations to improve your security hygiene.

Get started now.

Learn More

- Buyer's Guide for Complete Privileged Access Management (PAM)
- Paths to Privilege™ Explained
- The Guide to Identity Security Defense-in-Depth
- A Guide to Endpoint Privilege Management

About BeyondTrust

BeyondTrust is the global identity security leader protecting Paths to Privilege™. Our identity-centric approach goes beyond securing privileges and access, empowering organizations with the most effective solution to manage the entire identity attack surface and neutralize threats, whether from external attacks or insiders.

BeyondTrust is leading the charge in transforming identity security to prevent breaches and limit the blast radius of attacks, while creating a superior customer experience and operational efficiencies. We are trusted by 20,000 customers, including 75 of the Fortune 100, and our global ecosystem of partners.

Learn more at **www.beyondtrust.com.**