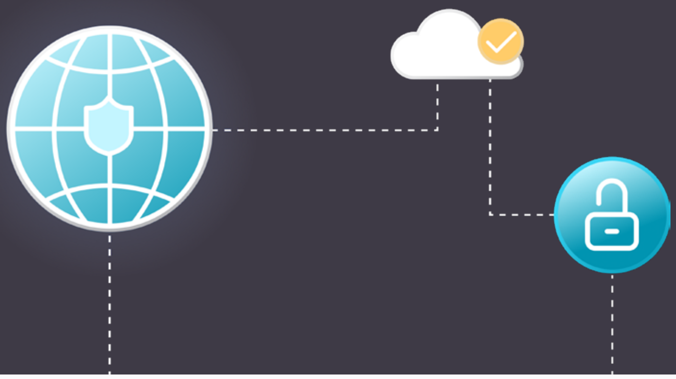
ConductorOne

Best Practices for Privileged Access Management (PAM) for the Cloud



Privileged access management (PAM) is an authorization mechanism for managing user identities that possess special "privileged" capabilities. If these accounts are compromised, they could grant unauthorized access to highly sensitive systems or data, necessitating extra safeguards beyond those applied to regular users.

Implementing PAM within your organization helps to ensure that restricted resources are kept private, supporting IGA (Identify Governance and Administration) requirements. This article explores several best practices that will allow you to successfully utilize PAM to enforce access controls and secure your environments. You'll also explore the differences between cloud and on-premise PAM.

Best Practices for PAM for the Cloud

Moving to the cloud increases the risks associated with account theft. For example, compromising an administrator's AWS or Azure account could give an attacker access to your entire cloud infrastructure. Adopting a PAM approach nullifies this threat by keeping your most critical resources out of reach until the user is able to reauthenticate themselves.

Implement a Least Privilege Model

The principle of least privilege (POLP) states that identities should be assigned the minimum set of privileges they require to carry out their role. For example, developers who don't directly interact with production environments don't need to be assigned any permissions for those resources.

Respecting POLP is an important factor when implementing PAM. Managing privileged access starts with restricting it to the smallest possible set of individuals. PAM must incorporate tooling, processes, and education to ensure that overprivileged accounts can be prevented and identified.

Implement Just-in-Time (JIT) Access for Privileged Accounts

Even accounts that unavoidably require access to privileged resources won't necessarily use those permissions on a regular basis. However, conventional authorization architectures such as RBAC result in accounts being permanently granted permissions. This means the theft of credentials or security tokens will inevitably create a risk of sensitive asset exposure.

Just-in-time (JIT) access is a seminal component of PAM that provides an effective defense against this threat. JIT refers to deferring permission grants for sensitive resources until a user account attempts access. The user will acquire a temporary authorization each time they request the resource.

JIT is supported by many cloud identity solutions. Once enabled, accounts are still able to access sensitive resources, but must first reauthenticate by calling a dedicated API. After verifying the access attempt—which could entail use of an MFA challenge and analysis of any suspicious activity, for example—the API issues a short-lived access token that the user can present to retrieve the target resource.

Enforce Strong Authentication and Access Controls

To a large extent, PAM is built on well-established security principles such as the use of strong and unique passwords, multifactor authentication (MFA), and correct network isolation of applications and infrastructure components.

These measures may seem simple, but they still play a crucial role in PAM. Relaxations in security policies and habits can occur over time, causing accounts to be breached by trivial means, such as password reuse on an unrelated website. Mandating that all identities with access to sensitive resources enable MFA is an easy but effective way to improve protection.

Similarly, critical apps and infrastructure should be placed behind strengthened perimeters that are capable of resisting unauthorized access. Firewalls, physical network separation, service meshes, and the use of network policies in cloud-native settings such as Kubernetes will prevent apps and devices from communicating with unauthorized peers.

Implement Privileged Session Monitoring and Recording

PAM isn't just about the physical means of preventing unauthorized access to sensitive resources. It's also important to implement systems that allow you to accurately monitor and record which resources are being accessed and by whom. This information can be crucial when you need to investigate a breach or demonstrate compliance during a regulatory audit.

Enable session recording controls to ensure you can analyze the interactions that individual users have made. Audit logs, event streams, and metrics that collate activity statistics keep you informed and allow anomalies to be detected in real time. If a user repeatedly tries to access a privileged resource, then it could signal that the account has been compromised and is being misused.

Regularly Review and Update Privileged Access Policies

Privileged access policies should not be static; they need to be continually reviewed and revised as your identities, apps, and infrastructure components change. As staff rotate between roles and deploy new systems, your policies can become outdated or redundant. This results in a security threat as previously secured accounts gradually become overprivileged.

To combat this, permissions and roles should be updated whenever changes occur. As this still depends on administrators remembering to follow the correct process, it's also useful to implement automated scheduled reviews that detect identities with unused privileges. Pruning any access rights that aren't actually required helps reduce your attack surface.

Try to make your access policies more precise over time and keep them aligned with changes to your organization's routines. This will help you adhere to the principle of least privilege. For example, if one individual previously created and approved payments, but this process now requires different people at each stage, then you would need to modify your PAM access controls accordingly. In this example, you'd create separate roles for "creating" and "approving" payments.

Monitor Anomalies to Detect Suspicious Access Activities

Suspicious access attempts should be triaged and thwarted at the time they occur. Implementing real-time anomaly monitoring allows you to spot and respond to new threats as they happen, facilitating a proactive defense model.

If you only know about incidents *after* they happen, your security teams can only react to access attempts. This is akin to closing the stable door after the horse—in this case, your data—has already bolted. Anomaly detection mechanisms combine behavioral analysis with heuristics such as login location, device, resource identity, and historical activity data to flag problematic events for approval and allow you to stop the door from being opened.

Use Encryption and Configure Data Protection Measures

Encryption is a security best practice for all identities, but it's especially important for privileged accounts and resources. Records should be encrypted everywhere they're encountered, both at rest in a database and during transit through your networks.

Data should also be subject to effective data loss prevention (DLP) controls that prevent resources from being inadvertently distributed outside the organization. Unintentional unsafe data sharing is a continual threat; DLP prevents this by allowing transfers of privileged resources to be detected and blocked in real time.

DLP strategies are usually formed from four components: understanding what data you have and where it resides, protecting that data, preventing it from being lost, and governing how it is accessed, retained, and stored. PAM solutions empower you to meet DLP commitments, especially those that fall within the protect, prevent, and govern spheres. Data will be less susceptible to loss if it's subject to strict privileged access requirements.

Regularly Conduct Vulnerability Assessments and Penetration Testing

The security of PAM systems needs to be assessed on a regular cadence. Vulnerabilities can arise as a result of changes, new infrastructure, and updates to your technology. These must be promptly identified and remediated to prevent a breach of your PAM protections.

You can stay ahead of vulnerabilities by conducting penetration tests of your access control systems. These could reveal previously unknown attack vectors that cause proper authorization procedures to be bypassed. PAM depends on a dedication to ongoing security; penetration tests are one way you can prove the effectiveness of your systems in a safe environment.

Provide Ongoing Training and Awareness Programs

Limited awareness of the risks associated with privileged access can hinder the adoption of PAM best practices. Users with privileged access are typically also privileged within the organization; they're administrators, executives, and directors who are used to having unrestricted access to resources.

This jars against the PAM methodology, which requires access to be limited to the greatest extent possible, usually by taking a JIT approach. In order for users to accept the paradigm, you should provide training programs that clearly communicate the risks of privileged access and how PAM defends against them. This will foster a safer security culture where users don't expect to be granted permissions that they don't actively consume.

How Does Cloud PAM Differ from On-Premise PAM?

PAM isn't unique to the cloud—it enhances on-premise security as well. Though the purpose of on-premise PAM remains the same, it often differs in implementation due to the inherent discrepancies between cloud and on-prem infrastructure.

Good PAM solutions will nonetheless allow you to work across different clouds and networks. They will unify your identities and protect all your resources, regardless of whether they reside in the cloud or an on-premise machine.

You can gauge whether your PAM solution is likely to support combined cloud and on-prem environments by evaluating how it performs across the following topics.

Infrastructure and Access Model

A significant difference between cloud and on-premise PAM is the scope of access that each variant needs to support. On-premise PAM secures privileged access to the physical servers, network devices, app deployments, data, and infrastructure within an organization's own data centers. In an on-premise environment, these are usually the only privileged resource types that exist.

By contrast, cloud PAM involves several more asset types: your cloud provider logins, IAM solutions, virtual machines, containers, and serverless functions must all be protected as well. This demands a PAM solution that's designed to support these extra use cases.

Although PAM is important for both on-premise and cloud environments, it's arguably most critical when you're operating in the cloud. An unauthorized individual gaining access to an improperly secured administrator account for a cloud platform such as AWS or Azure could lead to a complete compromise of your infrastructure.

Scalability and Elasticity

Cloud environments are highly dynamic. This is one of the leading reasons why cloud computing—and, by extension, cloud-native applications—have become so popular. You can spin up new infrastructure components, add network endpoints, and try out apps in minutes.

This flexibility presents challenges for PAM. A constantly changing resource list increases the probability that improper access controls will be applied. Cloud PAM solutions must therefore match the scalability and elasticity of the environments they manage. PAM needs to apply to every resource, across every distributed compute node; this requires your PAM systems to have full awareness of all the resources you provision across your clouds.

On-premise PAM is comparatively simpler to scale as the surrounding infrastructure tends to remain fixed for longer periods of time. You know what your network endpoints are and which devices need to be protected. This reduces the work required to identify and isolate privileged resources.

Shared Responsibility Model

Similarly, on-premise PAM also results in a simple apportionment of responsibility: you're entirely responsible for the infrastructure as well as the security and PAM measures you implement. This can be daunting, as there's no backup option or anywhere to deflect criticism if something goes awry.

Cloud PAM is different because it falls within the scope of the shared responsibility model that most cloud providers utilize. This effectively shares responsibility for security operations between the cloud provider and your organization. It means that some security incidents could be demonstrably attributed to the third-party provider rather than a first-party failing on your side.

This doesn't mean you can transfer all responsibility for PAM to your cloud provider. The shared responsibility model usually assigns the provider responsibility for securing access to your cloud platform, ensuring only authorized users can connect. However, you must still set up appropriate access controls within the platform to prevent unauthorized data access and sharing.

Integration with Cloud Provider Services

Cloud PAM solutions integrate with individual clouds' native services. This enables automated management and monitoring of your resources. It also ensures that new resources, such as virtual machines and databases, benefit from automatic protection from your PAM implementation.

Direct cloud PAM integrations consequently reduce administrative overhead. The PAM solution can take control of privileged access by using the cloud provider's APIs to discover resources and then apply the correct access restrictions. Admins don't need to manually find and configure privileged resources after they're provisioned. On-premise PAM is more limited in this regard. You might not be able to achieve the same level of integration with your own infrastructure unless you allocate significant resources to developing custom automated tooling. On-premise solutions are inherently nonstandard, with limitless combinations of software and device combinations. This can hamper efforts to apply overarching control layers, such as those required for PAM.

Network Boundaries and Isolation

Friction can occur in cloud PAM implementations when network boundaries have to be considered. Distributed cloud networks often span multiple geographic regions and availability zones and across several physically distinct data centers. Managing access across these environments places additional demands on the PAM solution.

This involves more than just rolling out and synchronizing access policies across different regions. Other controls, such as automated anomaly detection, also need to be tuned for distributed environments. When users can access a resource from multiple data centers, PAM must account for this when evaluating whether an access attempt is likely to be suspicious.

This is another case where on-premise PAM is usually simpler. As on-premise infrastructure is generally contained within a single physical network, PAM doesn't need to support border-crossing scenarios.

Automation and Orchestration

The best PAM solutions use automation and orchestration to continually provision and manage access policies. This is easier on cloud platforms, which are designed to be automated via APIs and infrastructure as code (IaC) tools. Cloud provider identity platform integrations can simplify the deployment, rotation, and deprovisioning of PAM configurations.

As on-premise infrastructure is usually more bespoke, similar capabilities are harder to achieve for on-premise PAM. A greater reliance on existing manual processes and workflows is required, which can reduce efficiency compared to PAM on cloud platforms. In on-premise situations, you need to implement your own tooling to orchestrate access controls for different infrastructure components.

Connectivity and Access Control

Cloud PAM is more than just your infrastructure. As already outlined, it also secures access to critical management planes, such as your cloud provider’s consoles and APIs. This means that cloud PAM solutions require their own secure network connectivity so that you can access the controls they provide.

When adopting a cloud-based PAM system, you should link your existing identity provider so that users can authenticate. You must also set up an access control mechanism that allows users to interact with the PAM solution. Because compromising the PAM platform would let attackers manipulate your policies and privileged resources, this access should itself be subject to PAM mechanisms.

On-premise PAM systems also require stringent connectivity and access controls to maintain security. However, this can be easier to achieve because the routing will be through your existing local network. You can avoid exposing your PAM solution to the public internet, thus reducing the risk you face.

How Does PAM Relate to IGA?

PAM is part of IGA because it helps control user access to sensitive resources. While IGA concerns the broader practice of using defined policies and frameworks to manage user identities, PAM is one of the components to include in your frameworks.

PAM functionality—such as mandatory reauthentication before sensitive resources are accessed—ensures your identities are subject to continual governance, which is the fundamental requirement of IGA. This strengthens oversight and compliance, mitigating the threat of security incidents stemming from improper access controls.

Nonetheless, you’ll need more than just PAM to implement a complete IGA strategy. This is because IGA is used for end-to-end identity management, spanning the complete identity lifecycle from provisioning through to auditing, recertification, and eventual decommissioning. PAM governs how identities access resources, but it doesn’t address how those identities are created and handled by their management systems.

Conclusion: Use PAM to Protect Your Cloud Security

PAM strengthens the security protections around your most sensitive resources—whether apps, data, or infrastructure—by enforcing additional safeguards before they can be accessed. No user should have continuous access to these assets, even if they’re an administrator or executive within your organization.

Implementing PAM allows privileged access attempts to be properly reauthenticated, logged, and secured. Utilizing JIT access will prevent users from retaining permanent access to resources, in turn helping you adhere to least privilege principles. This hardens your security environment by mitigating the threat of compromised user accounts that belong to senior individuals.