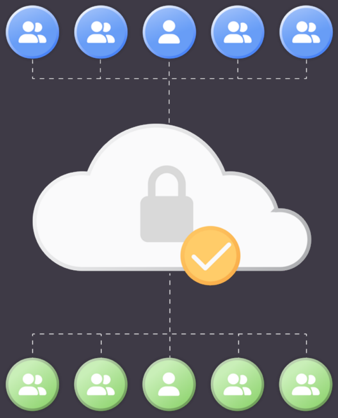
ConductorOne

Key Differences Between JIT Access and Traditional PAM



Just-in-time (JIT) access and privileged access management (PAM) are both methods of controlling and monitoring highly privileged access to networks and servers. Both ensure that no one has unchecked, ongoing privileged access to systems, applications, or infrastructure. Each method requires additional criteria or action, such as an additional login or ticket generation, before an administrator can be granted access.

However, JIT access and PAM are not synonymous. Important differences between PAM and JIT access emerge when you configure the approvals and protections around the use of access.
If you need to reduce ongoing administrative access or provide evidence of authorization each time confidential data is accessed, JIT access might be the expanded management method you need.

What is privileged access management (PAM)?

PAM is a security practice that focuses on controlling, monitoring, and securing access to highly privileged accounts. It involves creating permanent accounts with special privileges that are not directly assigned to individual users or user groups, such as network administrators. Instead, these accounts are secured within a system that requires authentication from an administrator. After authentication, the account credential is released. Typically, this credential comprises a username/password combination, which is then granted to the authenticated user until it is returned. Alternatively, the credential may automatically connect the user to the target system. Once the credential is issued, the password is changed so the account can no longer be used. For a user to regain access, the authentication and checkout process must be repeated.

PAM configurations may vary depending on factors like whether there's a time limit for the credential checkout or for when the credential password is reset. At its most basic functionality, a PAM system acts as a database to manage and record the use of administrative credentials. The careful application of best practices is a requirement for any PAM implementation to be of value. If you only implement PAM to lock away credentials, you're just adding work for your administrators without providing any real benefit. Why miss the opportunity to upgrade security with multi-factor authentication, responsive credential changes, and activity-based approvals?

What is just-in-time (JIT) access?

JIT access is a more advanced form of privileged access management with more controls. PAM restricts access to the credentials and records it uses; JIT access makes credentials available only when needed, not on demand. Depending on the complexity of its implementation, JIT access may also include integrations with systems that automatically validate the legitimacy of the capability request. For instance, PAM could require that an administrator log in to a system and "check out" administrative access credentials. JIT access, on the other hand, could allow that action only through connection with a client request in a ticketing system, giving enterprises with confidential client data better evidence of client contract compliance.

Additionally, JIT access requires a predefined end time, which may not be present in a non-JIT PAM system. For instance, access can be tied to a ticketing system or a set of approvals that are required before JIT access is granted. Once the user accesses the elevated privilege, the access remains valid for a only certain amount of time, after which the user automatically loses it. Therefore, even if a credential is stolen when active, its life span is short and may be tied to specific systems.

Why not just use PAM?

Privileged access management can ensure that ongoing access to the protected accounts is unavailable if properly configured. A PAM system typically stores the credentials and provides them on demand. While it may or may not integrate with other monitoring systems, giving access to management systems usually relies on an administrator's ability to self-determine the requirements for using a privileged account.

This means that anyone who can log in to the PAM system has on-demand access to the credentials used to administer systems and networks. There is no specific time limitation required for any PAM system. If the system allows it, an administrator could log into the system, check out an administrative password, and use that access credential for the entirety of their workday. This practice speeds up their daily activities, but it also greatly increases the risk that they'll make administrator-level mistakes. To ensure serious mistakes don't happen needlessly, you should assign the correct permissions and make legitimate privilege elevation frictionless. Otherwise, administrators will look for these solutions to work around the imposition of a PAM system.

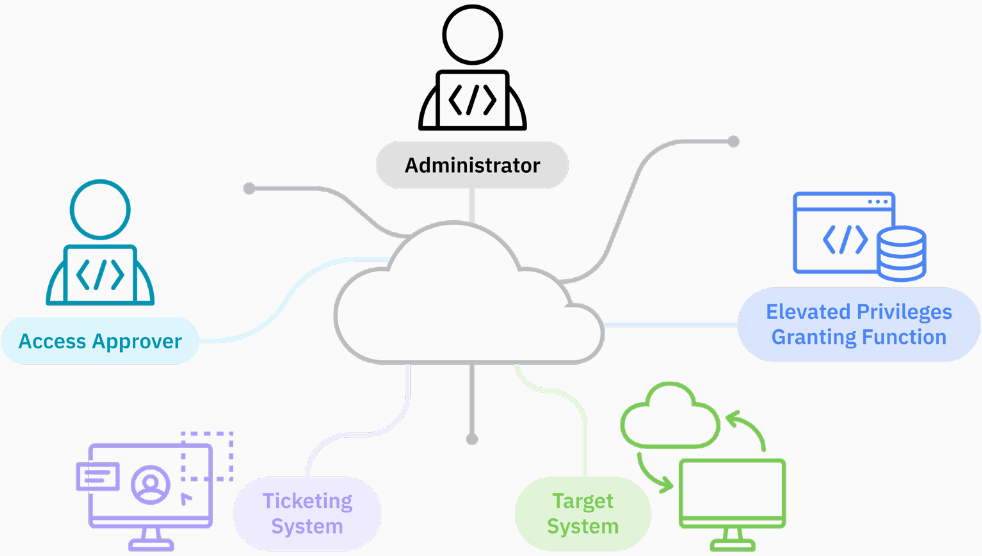
Advantages of JIT Access vs. Traditional PAM

If PAM doesn't meet the requirements of your environment, JIT access might provide the necessary features to bridge that gap. JIT access products usually include time-limited credentials, automatic escalation for approval, integration with support ticketing systems, and greater logging capability. These are features that effectively reduce the exposure of your administrative access while preserving the convenience of single-system access requests.

The following sections take a closer look at some of the advantages of JIT access over traditional PAM.

Static vs. Dynamic Access

Although JIT access is an incarnation of PAM, it offers advantages over the general static PAM functionality. PAM usually provides constant access rights, regardless of the immediate need. JIT access is dynamic, and it adapts to real-time requirements to minimize unnecessary ongoing access. Unless specifically configured, PAM-owned accounts remain operable and accessible, regardless of whether there is an immediate need for them. The static approach makes for easier management, but it also comes with heightened security risk compared to a JIT access solution. Attackers can exploit the constantly available privileges and concentrate their efforts on evading detection.



Reduced Attack Surface

“Attack surface” usually refers to the extent of a network or the exposure of applications that an attacker can exploit. Rather than limiting the network’s scope or the number of exposed applications, JIT access reduces the attack surface by reducing the number of active privileges accessible at any given moment. Once the user completes the task at hand or when the time allocated to the permissions expires, the JIT system revokes the elevated privileges. While the physical attack surface remains unchanged, the cyberthreat’s window of opportunity is reduced.

Security and Regulatory Compliance

Most technology compliance requirements include a section on working with administrative credentials only when necessary. Most daily tasks can be performed with a user’s normal account, not with administrator access. JIT access, often linked to a justification or a work ticket, eliminates the possibility of performing daily tasks (or even casual browsing) with administrative access. When elevated access is not continuous, employees become more aware of the significance and responsibilities of administrative privileges.

While compliance differs from security, compliance with security standards or guidelines can often improve your security posture. JIT access can be a very useful tool for maintaining requirements for security compliance. Many data protection and privacy regulations mandate control over sensitive information access, including elevated access. Organizations must minimize the use of privileged accounts, reserving them only when they are necessary. This may be explicit, as in some versions of the National Institute of Standards and Technology (NIST) requirements, or implied, as with Center for Internet Security (CIS) guidance. In either case, just-in-time access ensures that elevated privileges are not used excessively.

Security Awareness

Most employees retain the content of their security awareness training, including the use of minimum necessary privileges. Unfortunately, this does not mean that employees abide by it. There is a significant contrast between the security rules that they accept and their daily behavior.

An organization implementing JIT access reflects a shift from performative training to a deliberate, documented process for granting additional privileges based on clear justification. Employee actions and documentation can be measured against the requirements outlined in the training. This provides concrete data to assess if security awareness is truly embedded in the organization’s culture or if a different approach is needed.

Logging Capabilities

Advanced JIT systems incorporate user behavior analytics (UBA) to detect deviations from typical access patterns, an essential part of identifying potential insider threats. This feature is often less developed in PAM solutions. The detailed logging and data richness of JIT systems aid significantly in forensic analysis following security incidents. Investigators can trace actions leading up to an incident more accurately, which is an advantage less pronounced in many PAM systems. JIT systems can automate the generation of compliance reports, a time-saving feature that ensures accuracy and timeliness. This automated reporting capability is often more challenging with PAM systems, where manual compilation might be necessary.

Considerations for Using JIT Access

JIT access is more complex to plan and set up than PAM. PAM implementation is not exactly intuitive; it generally requires connections with other access platforms, such as user account management and potentially multifactor authentication. However, these access platforms can sometimes be found as part of single-provider ecosystems, with detailed documentation and recommended configurations. That is rarely the case with JIT access.

Setup Complexity

JIT access usually requires a detailed understanding of an organization’s network architecture and user roles to tailor access permissions accurately. For JIT access to scale, the functions must be automated to grant and revoke privileges based on specific criteria. That criteria can encompass the user’s current role and machine, the verifiable task, a time frame, and/or the risk associated with the access.

Integrating JIT access into existing systems can be a challenge if your provider demands backward compatibility with applications and databases already in place. It can also limit software and architecture choices in the future, as it requires integration across the environment’s most important assets. However, when JIT access is correctly implemented, errors concerning permanent privileges become almost nonexistent. This may sound like an exaggeration, but consider the practicalities. If a person outside of an expected operational or administrative role is accidentally granted an account in the JIT system, the instances where they could misuse it are exceedingly rare. The other components—approvals, related work tickets assigned to their user account, appropriate time of day, multifactor authentication—would not be present to close the circuit and release the credentials.

Tool Integration

The effectiveness of JIT access is heavily dependent on the maturity of an organization's access policies and the rigor of its approval processes. If these are not well defined or if the JIT system is not configured correctly, it could inadvertently introduce risks, such as inappropriate access being granted or delays in revoking access.

Additionally, technical impacts are broader when it comes to JIT access. Implementing JIT access in heterogeneous IT environments may leave gaps between your tool capability and any legacy systems and applications. If your JIT access integration with applications does not cover any of these, there must be a secondary option that still avoids issuing standing administrative accounts. Introducing a second procedure or tool not only increases administrative overhead and complexity, but it also brings into question whether the JIT system you chose was the right option.

Conclusion

JIT access is a significant upgrade over traditional PAM. With JIT access, organizations can significantly reduce their attack surface, enhance compliance with regulatory standards, and improve the overall manageability of privileged access. Some JIT access providers, such as ConductorOne, have off-the-shelf, codeless integrations that simplify JIT access. Consider which features are most necessary in your environment, such as break-glass accounts and automatic approval for on-call resources. While it may introduce initial complexities in setup, the long-term benefits of improved security and compliance adherence make JIT access a compelling choice for modern organizations.