IT CURATED

4 Benefits of Just-In-Time (JIT) Privilege

ONE IDENTITY
Quest

Identifying the Risk

Active Directory (AD) has been a prime target for hackers ever since its initial rollout. It is the de facto authentication method for most enterprises because it is so widely used and is connected to nearly everything. But with such flexibility and ease of deployment comes the risk of attack. Once an attacker gains admin-level access to AD, it is simple to move between any systems connected to AD and obtain access to a plethora of proprietary and business-critical data across those systems. It also becomes very easy to deploy ransomware. Issues like these make Just-In-Time (JIT) Privilege essential for businesses.

An organization typically has a few trusted admins with specialized accounts that grant constant access to the AD such as Domain, Enterprise, and Schema Admins. These privileged profiles provide top-level administration, but they are highly vulnerable. An attacker with access to one of these profiles can take over the entire organization. The goal of JIT Privilege is to eliminate the ransomware’s target.

It's vital to understand the root cause of breaches to prevent them from happening. A ransomware attack may compromise an entire business by exploiting a permanently privileged account in AD. The goal of JIT Privilege is to eliminate the attacker's target. It detects and blocks unauthorized actions before they can harm your organization.

One Identity Just-In-Time Privilege is a solution designed to address a significant security issue. It gives admins privileged access only when necessary. When the account is not in use or signed out, JIT Privilege disables it and removes it from all privileged groups. It also changes the password and stores it securely, following a Zero Trust Least Privilege model. This way, accounts are protected from compromise or unauthorized access.

Reducing Vulnerabilities

One Identity Just-In-Time Privilege reduces the risk of data theft by providing several benefits, including:

1. Removing the attack vector:

AD, at its core, is a single-sign-on solution, designed to provide an easy user experience for businesses. However, like any other software, AD must be used correctly and securely to protect the data it stores. Here are some tips to keep in mind when using AD:

- Any user authenticated in AD can see nearly everything – by default. This means any standard user with no assigned privileges in AD can see which accounts are privileged. This is part of what is known as the "enumeration" phase of the attack: attackers need to know which accounts can own the enterprise.

- Privileged accounts that belong to groups that can own anything, or are nested within these groups, (i.e., Domain Admins, Enterprise Admins, Schema Admins) are extremely vulnerable and the primary target of any AD attack.

JIT removes the elevated privileges from the accounts when they are not in use. If an attacker enumerates the critical enterprise groups, the JIT Privilege-managed accounts will not show as privileged.

2. Simplifying and tracking privilege use:

Admins have a standard user account as well as a privileged account. They are expected to use the regular one for day-to-day office work and the privileged account for admin work. However, whether the task requires high-level rights or not, most admins use the privileged account. This may be subject to audit policies, and the events may be logged, but true control and auditing are rarely invoked. Admins are comfortable with unrestricted access to everything. They trust the accounts they use are only used by them and have not been compromised – but how do they know?

When an admin logs into a newly AD-connected system, the credentials are cached and stored locally. The attacker can exploit this vulnerability by mining these footprints (a.k.a. hashes) and using them to sign back into the accounts (even if MFA is required). With JIT Privilege, these traces are rendered useless because the passwords are changed immediately when the account is signed back in. The footprints remain, but they are no longer useful to the attacker.

Not only does this ensure the account is unusable, but JIT Privilege also provides:

- Approval of account usage through a workflow process.

- A comprehensive record of the person who signed in to the account, the duration of the usage, and the reason for its use.

- Information regarding when the account was signed out.

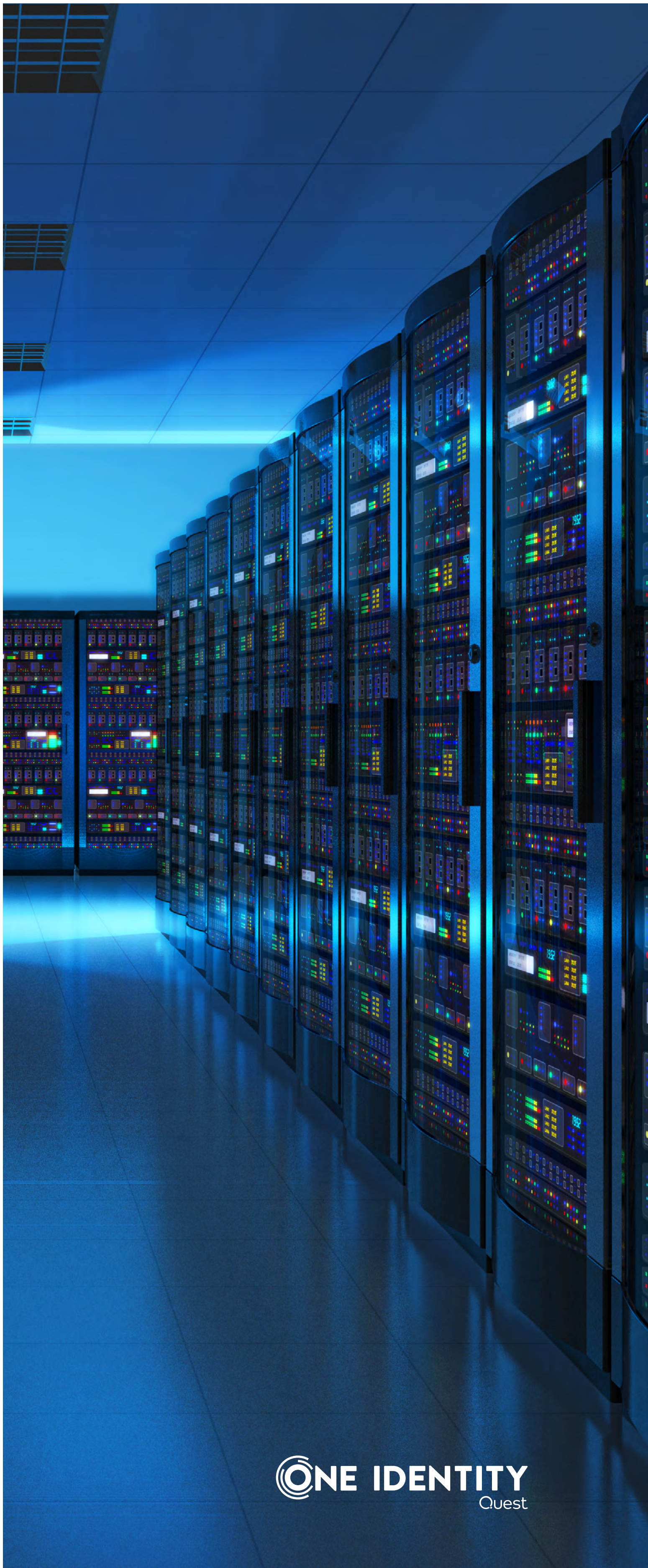
Administrators no longer have to wonder or worry whether their privileged account was used in their absence.

3. Saving time with a secure and simple process:

JIT Privilege allows IT managers to automate admin access and privileged entitlements. It allows IT teams to streamline the process of monitoring and granting privileges, as they can easily approve workflows and review privileged account use. Admins who need daily privileged account access may be allowed to check out credentials without workflow approval from security or management. The automation simplifies and streamlines access, and the resulting solution is highly secure and fully audited.

4. Complying with security policies and best practices:

Large AD-centric organizations frequently audit their highly privileged groups. It is important to be aware of who owns the accounts in these groups and to reduce vulnerability by keeping group membership to a bare minimum. JIT Privilege only populates the privileged group membership when the privileges are in use. The auditors will need to change the question from “Who is in the privileged group?” to “Who has privileged access in AD?” — a simple change for the sake of stronger security. With this change, the auditors will now be able to see not only who has access to privileged AD accounts but who has used these privileges over time. This can allow further pruning of unnecessary privileged access.



Summary

When considering how to secure an enterprise, it is important to address the obvious: AD privilege.

Finding ways to secure vulnerable identities and processes may be more elaborate than simply removing the vulnerability in the first place. Just-In-Time Privilege from One Identity is specifically designed to protect critical enterprise groups in AD by removing members who are not currently using the privilege. It disables accounts when not in use and nearly eliminates AD credential exploits while providing admins and auditors simple access to just what they need when they need it.

Microsoft Active Directory and One Identity Active Roles: Better Together

The One Identity solution

At One Identity, we are committed to helping businesses of all sizes secure their systems and data with a unified identity security solution. Our JIT solution combines the powerful AD Management capabilities of Active Roles with the unmatched password management capabilities of Safeguard to dramatically reduce the risk of cyberattacks on privileged accounts.

One Identity's Just-In-Time Privilege is part of the One Identity Unified Identity Platform, which helps customers strengthen their overall cybersecurity posture and protect the people, applications, and data essential to business. Our Unified Identity Platform brings together best-in-class capabilities for Identity Governance and Administration (IGA), Access Management (AM), Privileged Access Management (PAM), and Active Directory Management (AD Mgmt) to help organizations transition from a fragmented to a holistic approach to identity security. One Identity is trusted and proven on a global scale – managing more than 250 million identities for more than 5,000 organizations worldwide. For more information, visit **www.oneidentity.com**.