StackIdentity

Transforming Permanent Access to Just-in-Time with Just-Enough Access

WHITE PAPER

Introduction: Breaking Free from the Risks of Permanent Access

The cybersecurity landscape has become a battleground where attackers have time on their side. Ransomware attacks, credential theft, and unauthorized access continue to wreak havoc on enterprises across the globe. Permanent access plays a significant role in nearly every major breach—from sophisticated nation-state attacks to ransomware incidents. Attackers exploit long-standing privileged access that remains available far longer than it should, giving them ample opportunity to penetrate systems and exfiltrate data.

The traditional approach of managing privileged accounts through static, always-on access is outdated and increasingly dangerous. Post-mortem analysis from major breaches reveals that one of the root causes is often **access that should never have existed** in the first place. It's time for a paradigm shift: moving from static, permanent access to Just-in-Time (JIT) and Just-Enough Access (JEA)—a modern and intelligent approach to access management.

The Problem: Attackers Are Not Waiting for Your Quarterly Audits

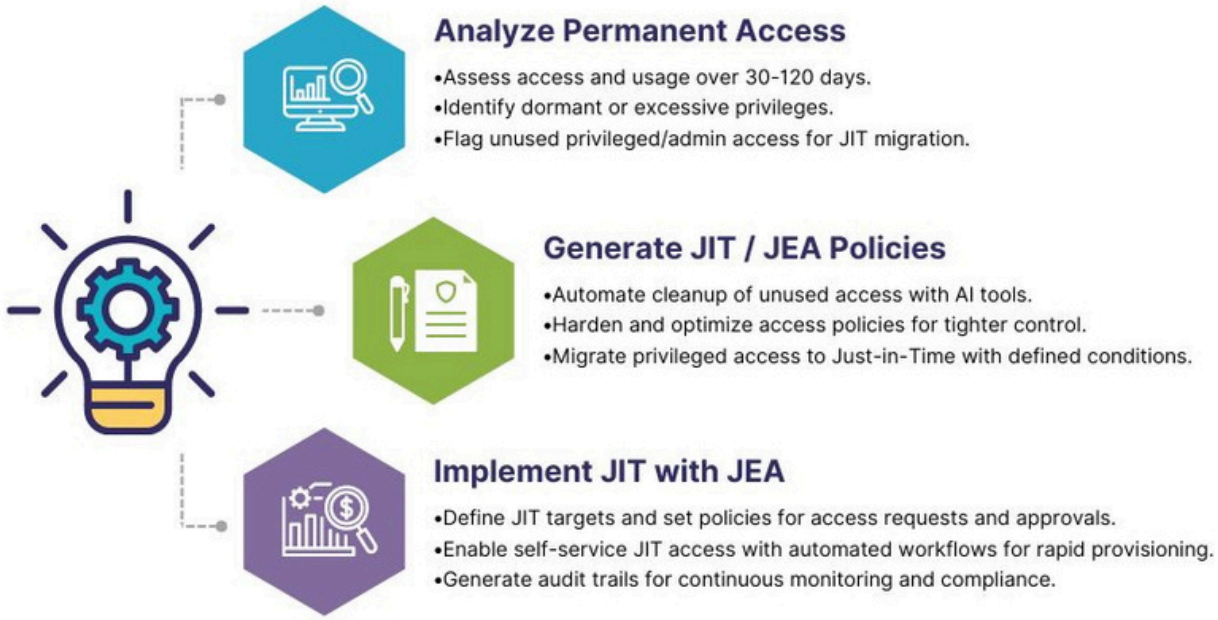
Bad actors are relentless. They are not waiting for the next quarterly audit or access governance review to exploit vulnerabilities. Every day, they target identity systems, weak credentials, and governance gaps in traditional Identity Governance and Administration (IGA) solutions. Long-standing access offers them a persistent foothold, allowing them to quietly gather intelligence and launch attacks when they see fit.

This is why the traditional approach to privileged access is failing. Static, permanent access opens the door to misuse and leaves enterprises vulnerable to breaches that cause significant financial, operational, and reputational damage.

The Shift: From Standing Access to Just-in-Time Access

The solution is clear: eliminate standing access and replace it with a Just-in-Time, Just-Enough Access model. This paradigm shift ensures that access is granted only when needed, for a specific purpose, and for the minimum required time.

Just-in-Time (JIT) access grants temporary, on-demand access to systems and data, and Just-Enough Access (JEA) ensures that the level of access is tightly restricted to what's necessary for the task at hand. Together, they minimize the attack surface, mitigate the risk of credential misuse, and allow organizations to enforce a true least privilege model, which is often unattainable through traditional methods.



Stage 1: Analyzing and Understanding Permanent Access

To begin the transformation to JIT and JEA, organizations need to first identify and understand the scope of their permanent access. This stage involves a comprehensive analysis of usage patterns across identities, accounts, and resources.

Key Actions:

- **Assess** permanent access exposure over 30 to 120 days, using log data to analyze who has access to what and how frequently it's used.
- **Identify** least privilege exposures, including dormant or excessive access, orphaned accounts, and rarely used entitlements.
- **Flag** privileged, admin, and non-human identity access that remains active but unused, and prioritize these for elimination or migration to JIT.

This deep analysis reveals how much unnecessary access is granted and highlights opportunities to shift toward JIT access.

Stage 2: Making Decisions Based on Analysis

Once the permanent access landscape is mapped, the next stage is deciding how to act on the findings. This is where policies and decisions must be made to mitigate risks.

Key Actions:

- **Eliminate** unused access and clean up least privilege exposures automatically using AI-driven tools.
- **Rightsize and harden** access policies for services and infrastructure to ensure tighter control over privileges.
- **Migrate permanent privileged access** to Just-in-Time by defining precise conditions under which temporary access can be granted, including approvals and restrictions.

This stage is about shrinking the attack surface—reducing the number of identities with permanent access and enforcing policies that limit the scope and duration of access.

Stage 3: Implementing Just-in-Time with Just-Enough Access

The final stage is the actual implementation of JIT with JEA. This is where organizations define policies, automate workflows, and deploy the tools needed to operationalize the shift away from permanent access.

Key Actions:

- **Define JIT targets** for administrators, privileged users, and automated pipelines.
- **Set up JIT policies** to control who can request temporary access, for which resources, and what level of access is appropriate. For example, allow JIT for cross-account cloud access or sensitive databases only after approvals are obtained.
- **Enable end-user self-service** for requesting JIT access, along with automated approval workflows to ensure rapid provisioning without compromising security.
- **Generate audit and compliance trails** to provide continuous monitoring and evidence of access control adherence.

With these policies in place, organizations can transition from static, vulnerable access to a **dynamic, demand-driven** access model that drastically reduces risk.

How to Get Started with JIT and JEA: Targeting the Right Environments

To begin your journey toward Just-in-Time and Just-Enough Access, it's critical to start with dynamic and over-permissioned environments where permanent access poses the most significant risk. These environments typically have high levels of privilege and are frequently targeted by attackers.

1. Cloud Environments

Cloud platforms are highly dynamic, with frequent changes in resources, users, and permissions. Over-provisioned access is common, leading to vulnerabilities. Implementing JIT in cloud accounts and services ensures that access is only granted when needed, preventing attackers from exploiting overly broad or long-standing permissions.

2. Privileged and Administrator Access

Privileged accounts, such as those used by administrators, are the crown jewels for attackers. Permanent access for these users provides a direct pathway into critical infrastructure. By shifting these accounts to JIT, you can ensure that no access is available until it is explicitly requested and approved, minimizing the window of opportunity for misuse.

3. Enterprise Databases

The rise of Generative AI and automation tools has made enterprise databases more vulnerable than ever before. These databases often store highly sensitive data, and permanent access to them represents a major security risk. Moving database access to JIT, coupled with JEA, ensures that access is only granted for specific tasks, dramatically reducing the chance of unauthorized access.

4. Hybrid and Multi-Cloud Infrastructures

Organizations increasingly operate in hybrid environments where traditional on-premise systems blend with cloud infrastructure. These environments are complex and transcend typical trust boundaries, making them particularly vulnerable to access-related risks. JIT policies that span multiple environments ensure that access is consistently controlled across the enterprise, regardless of where data resides.

Core Technologies that Underpin JIT with JEA

To successfully implement JIT and JEA, organizations need a cohesive set of technologies, including:

- **Graph-based identity correlation** to visualize relationships between identities, entitlements, and actions.
- **Self-service provisioning** to enable users to request JIT access securely and efficiently.

- **Automated remediation** to eliminate standing access and enforce least privilege automatically.
- **Continuous monitoring** through Cloud Infrastructure Entitlement Management (CIEM) is integrated with identity providers (IDP) to ensure that the least privilege is maintained over time.
- **Comprehensive tagging** strategies to classify and manage resources for precise access control.

Conclusion: The Time to Implement JIT with JEA is Now

The shift from permanent access to Just-in-Time and Just-Enough Access isn't just a technological upgrade—it's a security imperative. Attackers are becoming more sophisticated and persistent; permanent access gives them an open door into your most sensitive systems.

The time to act is now. By targeting dynamic, over-permissioned environments like the cloud, privileged accounts, and hybrid infrastructures, and implementing JIT and JEA policies, you can dramatically reduce your attack surface, enforce least privilege, and protect your organization from the growing tide of identity-based threats.

Don't wait for the next breach—start your transformation today.