International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 9, Issue 12, pp 13-18, December-2025

https://doi.org/10.47001/IRJIET/2025.912003

Zero Trust in Practice: Enhancing Privileged Access Security with Just-in-Time (JIT) and Self-Service Models

Suresh Pairu Subramanyam

Technical Manager, United States

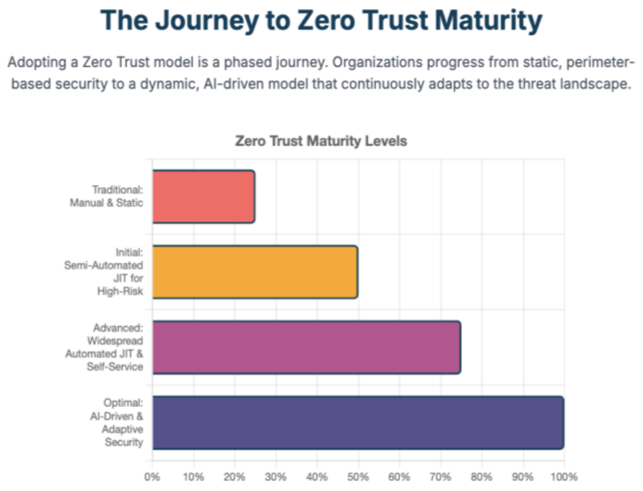
***Abstract* - The enterprise security landscape is current, remote work and hybrid cloud adoption highlights the inadequacy of legacy or traditional perimeter-based security controls, hence, the shift to Zero Trust, where in this new paradigm, privileged accounts are viewed as assets – most important and highly targeted. This document will discuss how Just-in-Time (JIT) Access and Self-Service models enable businesses to operate under a Zero Trust concept using Privileged Access Management (PAM). JIT enables dismantling "always-on" or "standing" privileged account risks by provisioning temporary time-based privileges for both human and non-human identities only when needed. Different from traditional PAM approaches that typically leave unwanted sources vulnerable thereby leading to "privilege creep," unmonitored "orphaned accounts" available for attack, JIT will narrow the window considerably to more than 90% reduction in the threat window associated with privilege attacks. It also covers how self-service access, fueled by smart workflows and Risk-Based Authentication, can strike that fine line between tight security and productivity through seamless experience for the user. The paper finally imagines a world where Zero Trust PAM would be inseparably linked to Artificial Intelligence and Automation in delivering pro-active, end-to-end security leveraging Identity Threat Detection and Response (ITDR). At the end of it all, the value of strategic and actionable insights for an organization is immense, especially when operating in highly regulated industries. Insights that will help systematically move the organization from a 'trust-by-default' state to one of 'trust-by-exception,' thereby are creating a security-aware environment without impeding users.**

Keywords: Zero Trust, Privileged Access Management (PAM), Just-in-Time (JIT) Access, Self-Service, Zero Standing Privilege, Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), Risk-Based Authentication (RBA), Identity Threat Detection and Response (ITDR).

1. Introduction: The Zero Trust Imperative in a Compromised World

1.1 The Evolving Threat Landscape

The old 'castle-and-moat' is not just somewhat but fundamentally inadequate to the modern problems of cybersecurity. Static defense and implicit trust can no longer be relied on in today's dynamic environment of remote work and ubiquitous cloud computing, coupled with further advanced persistent attack threats as well as insider threats. There has to be a quite transformative change in the overall paradigm that moves from a centric approach toward a data-centric framework. This new philosophy is ostensibly based on a "never trust, always verify" principle which has assumed the role of a foundational element of security strategies in both private and public sectors.



The Journey to Zero Trust Maturity

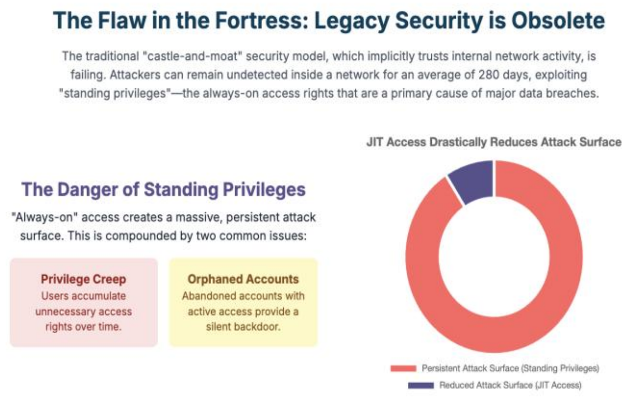
Adopting a Zero Trust model is a phased journey. Organizations progress from static, perimeter-based security to a dynamic, AI-driven model that continuously adapts to the threat landscape.

1.2 The Problem of Standing Privileges

In this changing environment, privileged accounts-those with elevated access to important systems and data-are the main goals for attackers. The age-old method of providing "always-on" or "standing" privileged access has created a constant and wide attack surface. This gives bad actors plenty of time- from weeks to even months- within which they can use compromised credentials to move around inside systems and steal information. The problem is made worse by what is

ISSN (online): 2581-3048
Volume 9, Issue 12, pp 13-18, December-2025
https://doi.org/10.47001/IRJIET/2025.912003

known as "privileged access creep," where users build up privileges that are no longer needed for their work, as well as by "orphaned accounts;" these are user accounts that have been left behind but still keep their rights to access active. Such unmonitored accounts become a silent door for attackers, so they are an especially attractive target for cybercriminals.



The Flaw in the Fortress: Legacy Security is Obsolete

The traditional "castle-and-moat" security model, which implicitly trusts internal network activity, is failing. Attackers can remain undetected inside a network for an average of 280 days, exploiting "standing privileges"—the always-on access rights that are a primary cause of major data breaches.

The Danger of Standing Privileges

"Always-on" access creates a massive, persistent attack surface. This is compounded by two common issues:

Privilege Creep
Users accumulate unnecessary access rights over time.

Orphaned Accounts
Abandoned accounts with active access provide a silent backdoor.

JIT Access Drastically Reduces Attack Surface
Persistent Attack Surface (Standing Privileges)
Reduced Attack Surface (JIT Access)

1.3 Scope and Objectives

This paper critically synthesizes how the Just-in-Time (JIT) access and self-service models effectively put into action the Zero Trust principles within a Privileged Access Management (PAM) strategy, going much further than an academic discussion by provisioning an in-depth understanding of the technologies, their basic tenets, issues regarding practical implementation, and results that can be measured. It hence becomes strategic and actionable for organizations in highly regulated sectors striving to improve their privileged access security.

II. Foundational Principles: A Synthesis of Zero Trust and Privileged Access

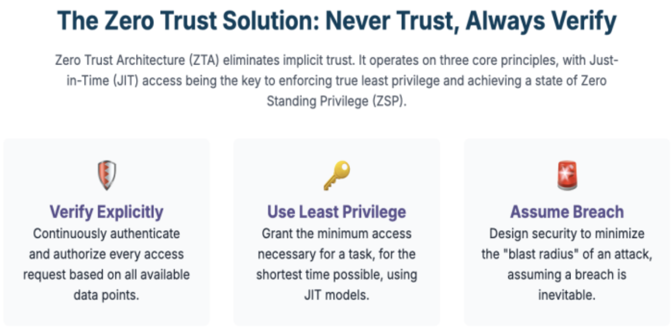
2.1 Core Tenets of Zero Trust Architecture

Zero Trust is a holistic security framework, not just an assemblage of offerings. The basic tenet of it is based on three core pillars that must be implemented consistently across the digital estate which covers everything and anything- from user to identity, device to application and infrastructure.

- **Verify Explicitly:** This rule says that every access, no matter where it comes from, should be fully authenticated, authorized, and encrypted before being allowed. It should be dynamic and ready to change based on all information available about who is trying to access it, what the health of their device is and what circumstances are surrounding the request [1].

- **Use Least Privilege Access:** It is a basic rule of both Zero Trust and good Privileged Access Management (PAM) to allow users only the least access and rights they need to carry out their approved tasks.

- **Assume Breach:** This principle demands an assumption-based preemptive strategy that breaches in security are likely or have already occurred. It aims to minimize the "blast radius" of any breach enabled through microsegmentation supported by continuous monitoring and a fully enabled incident response. The implementation of Zero Trust by the U.S. federal government under agencies such as the Cybersecurity and Infrastructure Security Agency and the Office of Management and Budget highlights an enormous shift in security philosophy and strategy.



The Zero Trust Solution: Never Trust, Always Verify

Zero Trust Architecture (ZTA) eliminates implicit trust. It operates on three core principles, with Just-in-Time (JIT) access being the key to enforcing true least privilege and achieving a state of Zero Standing Privilege (ZSP).

Verify Explicitly
Continuously authenticate and authorize every access request based on all available data points.

Use Least Privilege
Grant the minimum access necessary for a task, for the shortest time possible, using JIT models.

Assume Breach
Design security to minimize the "blast radius" of an attack, assuming a breach is inevitable.

2.2 Zero Trust Applied to Privileged Access Management (PAM)

Privileged Access Management has evolved at the core with the embedding of Zero Trust principles. The merging between these two spaces, or advanced PAM implementations and Zero Trust Initiatives, represent an evolution beyond static credential vaulting to dynamic access control [2]. A proper version of least privilege requires a coming together of two different yet intertwined methodologies: Just-Enough Access (JEA) and Just-in-Time (JIT) access. Although in most cases traditional PAM just emphasizes JEA by limiting how much access a user can have, the vulnerability window is open for exploitation continuously. On the other hand, JIT addresses time dimensions by controlling for how long access is granted, hence greatly minimizing the threat window. Hence, there should be neither an either-or relationship but rather a synergistic relationship between components of a holistic implementation of JEA and JIT as parts of a real Zero Trust-based PAM process where decreasing vulnerability spaces with accessible right ranges and limiting time frames that such rights are available. These principles help organizations move from a default trust model to a trust-by-exception model, where access is only given when needed and for just the shortest time required.

III. The Mechanics of Zero Standing Privilege: JIT and Self-Service

3.1 Just-in-Time (JIT) Access Provisioning

Just-in-time (JIT) provisioning access represents a dynamic, on-demand method that delivers temporary time-based privileges for human and non-human identities. It is essentially the primary method for reducing standing access and has led to much discussion as best practice among industry analysts.

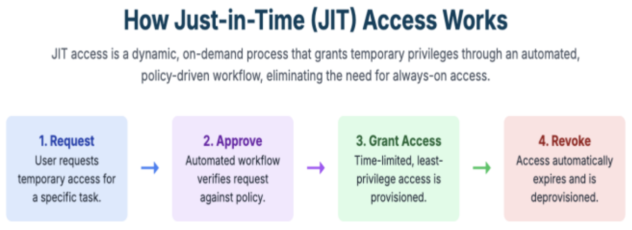
The process follows a structured and automated workflow:

- **Request Initiation:** The user makes a request to temporarily gain access to a particular resource so that a specific task can be completed. Every single request is documented properly to ensure visibility and accountability in the process.

- **Automated Workflows:** Just-in-Time (JIT) access management would heavily depend on automation of the request workflow, approvals, and provisioning as well as deprovisioning access. This is highly required to maintain productivity if not increase it while reducing administrative burdens and eliminating the scope of human error[3].

- **Secret Vaulting:** No, users do not have direct access to privileged credentials. It is centrally managed and stored in a secret vault- like that provided by CyberArk or BeyondTrust. The automatic rotation of the credentials makes sure that end-users never get to know the password, thus making the credentials null and void as soon as a session ends.

- **Auto-Expiration and Deprovisioning:** Access will automatically end once the job is done or when the set time limit runs out. Such fast deprovisioning helps stop permission from lingering and kills the risk of privilege creep, thus making sure there is a zero standing privilege environment.


How Just-in-Time (JIT) Access Works
JIT access is a dynamic, on-demand process that grants temporary privileges through an automated, policy-driven workflow, eliminating the need for always-on access.
1. Request
User requests temporary access for a specific task.
2. Approve
Automated workflow verifies request against policy.
3. Grant Access
Time-limited, least-privilege access is provisioned.
4. Revoke
Access automatically expires and is deprovisioned.

3.2 Self-Service Access Models

Moving to a self-service model will be important in reducing the operational friction and enabling the users to raise requests for the access they need without manual intervention. Coupled with automated workflows, this will highly contribute towards achieving secure yet seamless user experience. Security policies of these self-service requests are based on an evolution of paradigms of access control.

- **Role-Based Access Control (RBAC):** This approach is known and popular for access regulation based on the role of a user, which can be his job title or department. Though easy to implement, Role-Based Access Control becomes unyielding and causes a "role explosion," particularly in larger complex organizations where there would be a need to define thousands of roles to an adequate level of granularity [4].

- **Attribute-Based Access Control (ABAC):** Attribute-Based Access Control (ABAC) allows an organization to use and adjust more granular controls towards sensitivity of access decisions based on attributes related to the user, resource, and environment such as time, location, or even device. Implementation of ABAC dynamically breaks the static role model by allowing sensitivity and contextual policies to be enforced "inline" with business operations.

- **Risk-Based Authentication (RBA):** RBA is a crucial evolution toward intelligent and adaptive enforcement of security policies. It weighs risks related to a login attempt or request in real-time. This model develops a behavioral profile for each identity, comparing current activities to that baseline established over time. As the risk score increases—due, perhaps, to unusual login hours or from an unrecognized device—more stringent authentication steps are enforced [5]. The path from RBAC's static nature to ABAC's rule-based dynamism and ultimately leads to real-time behavioral analysis through RBA encapsulates Zero Trust's 'Verify explicitly' principle by validating every request in context. RBA can adjust its security controls dynamically on the basis of detected risk level to hinder attacker lateral movement after initial compromise.

IV. Empirical Insights and Practical Outcomes

4.1 The Case for Reduced Standing Privileges

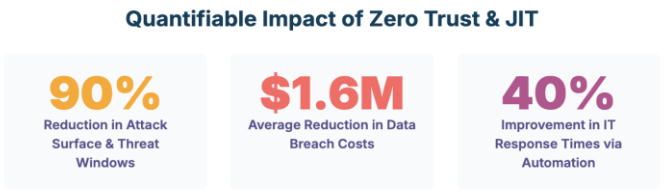
Just-In- Time access naturally helps organizations in their effort to reduce the risks of standing privileges, which are the main targets for attackers. Since it is only available for a limited period of time, JIT greatly reduces the attack surface and hence the opportunities available to threat actors against idle or long-established privileged accounts [6]. This speaks directly to the risk of privilege abuse and lateral movement that typically follows steps once an attacker has compromised an identity. It wants to shrink from continuous availability the threat window down to just the minutes or hours necessary for completion of a particular task.

4.2 Quantifiable Benefits and Metrics

The reason behind going for a Just-In-Time (JIT) and self-service model is validated by different quantitative and qualitative results. Though not coming from peer-reviewed journals, vendor case studies, and industry assertions do provide very good perspectives on the real benefits that accrual of such adoption [7]. The following table tries to synthesize quite a few of these reported results.

Vendor/Analyst	**Reported Outcome**
BeyondTrust	Privileged threat windows and attack surfaces may be reduced by more than 90%
CyberArk	Protected 50,000 privileged accounts at Cisco and monitored 25,000+ sessions per month
CyberArk	The US Hospital case study highlights how passwords only exist for single sessions and are not remembered by users
CloudEagle.ai	Automating workflows prevents bottlenecks, improving IT response times by 40%
Gartner	Projected that 40% of privileged access would rely on JIT control of privileged elevation by 2022

These metrics demonstrate that a compelling return on investment (ROI) is achievable, extending beyond pure security posture to include improved operational efficiency, streamlined compliance, and simplified auditing.



Quantifiable Impact of Zero Trust & JIT

90%
Reduction in Attack Surface & Threat Windows

$1.6M
Average Reduction in Data Breach Costs

40%
Improvement in IT Response Times via Automation

4.3 The Critical Role of AI and Automation

Automation becomes a key enabler for Zero Trust PAM allowing organizations to improve their security postures without increasing administrative burdens. It makes complex workflows easier to manage, reduces the opportunity for manual mistakes to occur, and ensures the consistent application of security policies [8]. The future state of Zero Trust Privileged Access Management is tied to the continuing evolution of artificial intelligence in security moving from a reactive stance to that of proactive defense.

The breach requires setting up a threat detection mechanism for any threats that have bypassed the preventive controls. It is in this regard, Identity Threat Detection and Response (ITDR) comes into play. ITDR will leverage AI/ML to perpetually observe user activities to flag anomalies that may indicate misuse of credentials or privilege escalation or lateral movement by an attacker. Such a system is critical as it acts as a “safety net” for all threats that have not been mitigated by initial preventive controls. In essence, with the introduction of ITDR, Zero Trust Privileged Access Management ceases to be largely a preventive approach but rather becomes truly proactive under an end-to-end security strategy that learns new threat patterns and adapts accordingly. Any conversation regarding Zero Trust PAM cannot be complete without bringing up this emergent, mutually supporting domain that holds the core assumption of breach.

V. Balancing Usability and Security in High-Regulation Sectors

5.1 The Challenge of User Friction

The main challenge with the implementation of stringent security controls is the subsequent level of user friction that may be experienced. If a policy is too restrictive, it will inhibit productivity and prompt users to look for insecure workarounds — like writing passwords down or even sharing passwords [9]. This will inadvertently compromise the very secure environment that one intends to set up. Secure privileged user enablement with minimal frustration is always the best practice.

ISSN (online): 2581-3048
Volume 9, Issue 12, pp 13-18, December-2025
https://doi.org/10.47001/IRJIET/2025.912003

5.2 Strategies for a Seamless User Experience

A successful Zero Trust implementation requires a deliberate focus on balancing security with usability.

- **Automate Workflows:** Automation is the best way to remove friction. With automation of provisioning, deprovisioning, and approval workflows, manual efforts can be reduced which means removing unnecessary delays that were added in the first place.
- **Empowerment through Self-Service:** Easy self-help portals, tied in with things like Slack or command lines give users the freedom they need to work safely. When users can ask for and control their own short-term access what is often seen as a block turns into a push for getting things done.
- **Balance and Prioritization:** It should also emphasize controls that are "beneath the surface" to users so as to avoid the fallacy of Expense in depth; that is, additional controls may not provide any significant value towards enhancing security but rather introduce unnecessary friction [10].

5.3 Cultural and Leadership Buy-in

The Zero Trust rollout is a massive cultural change — not just technical tweaks — and therefore requires strong executive sponsorship to beat back resistance from both IT operations and users who will lose track of how much standing, persistent access they actually have. This was proven in a U.S. hospital that implemented the Zero Trust Privileged Access Management (PAM) solution when the information security manager noted that changing the culture was "the biggest personal accomplishment" of the exercise. Explaining the process and its benefits to all concerned will go a long way toward forming a security culture where users understand what JIT access is and what zero standing privilege means.

VI. Conclusion and Recommendations for Implementation

6.1 Summary of Findings

It has been demonstrated that the strategic application of Just-In-Time (JIT) and self-service models is essential to enable the Zero Trust principles regarding privileged access. Therefore, it can successfully abolish standing privileges, minimize the attack surface, and make compliance and auditing easier. Security vs. productivity is balanced through automation and a user-centric design enabled by enforcing policies continuously and adaptively. The AI security evolution will enable a proactive and even predictive security moment that will facilitate addressing complicated forms of attacks centered around identities within the scope of ITDR.

6.2 Future Research and Development

The evolution of AI security in its application defines the future of Zero Trust Privileged Access Management (PAM). It is, therefore, through AI and ML that predictive security will soon be achieved such that threats are preempted before they come into existence based on an understanding of user behavior as well as context. The further integration of Identity Threat Detection and Response (ITDR) functions would result in the creation of holistic security protection from end to end, evolving with new forms of threats and going beyond simple prevention to include real-time detection and response in all its dimensions.

6.3 Final Recommendations

A tiered approach is recommended for organizations beginning their journey to Zero Trust. The first step should be to conduct an audit, identifying high-risk accounts with standing privileges and prioritizing them for remediation. Implementation should be incremental, as well as mission-focused; meet the tactical needs before moving on to more strategic, longer-term goals. The next steps are what is required to be successful in the long run:

- **Prioritize the highest-risk use cases:** Begin the Just-In-Time (JIT) implementation with high-value accounts such as domain admins and third-party contractors to optimize time to value.
- **Automate everything possible:** Invest in solutions that automate provisioning and deprovisioning, and approval workflows to reduce the friction that must be introduced to remove human error.
- **Integrate with existing systems:** It should work hand-in-hand with the existing identity infrastructure, which may involve Active Directory and external systems like ITSM and SIEM for centralized visibility and control.
- **Foster a culture of security:** Zero Trust is, in fact, not only an exercise in technology transformation but also one of change management. Strong leadership support and clear communication go a long way toward building a new culture successfully.

REFERENCES

[1] S. Ahmadi, "Autonomous Identity-Based Threat Segmentation for Zero Trust Architecture," *SSRN preprint*, 2025.

[2] S. Aggarwal, S. Mehra, and S. Sathar, "Combined Hyper-Extensible Extremely-Secured Zero-Trust CIAM-PAM Architecture," *arXiv preprint*, Jan. 2025.

[3] D. Ajish, "The Significance of Artificial Intelligence in Zero Trust Technologies: A Comprehensive Review," *Journal of Electrical Systems & Information Technology*, vol. 11, article no. 30, 2024.

[4] S. Arora and A. Tewari, "Zero Trust Architecture in IAM with AI Integration," *International Journal of Science and Research Archive*, vol. 8, no. 2, pp. 737–745, 2023.

[5] M. Rana, "Enhancing Zero Trust Cybersecurity with AI," *Journal of Information Systems Engineering & Management*, vol. 10, 32s, 2025.

[6] G. Karamchand, "Zero Trust and AI: A Synergistic Approach to Next-Generation Cyber Threat Mitigation," *World Journal of Advanced Research and Reviews*, vol. 24, no. 3, pp. 3374–3387, 2024.

[7] K. Khan, "Solid Access Management: AI-Based Zero-Trust Architectures for Corporate Security," *Newark Journal of Human-Centric AI & Robotics*, vol. 4, 2024.

[8] N. Bistolfi, A. Georgescu, and D. Hodson, "The Data Enclave Advantage: A New Paradigm for Least-Privileged Data Access in a Zero-Trust World," *arXiv preprint*, 2025.

[9] K. Huang, Y. Mehmood, H. Atta, J. Huang, M. Baig, and S. Balija, "Fortifying the Agentic Web: A Unified Zero-Trust Architecture Against Logic-Layer Threats*,"* *arXiv preprint*, Aug. 2025.

[10] R. Nair Rajendran, S. K. Anumula, D. K. Rai, and S. Agrawal, "Zero Trust Security Model Implementation in Microservices Architectures Using Identity Federation," *arXiv preprint*, Nov. 2025.

Citation of this Article:

Suresh Pairu Subramanyam. (2025). Zero Trust in Practice: Enhancing Privileged Access Security with Just-in-Time (JIT) and Self-Service Models. *International Research Journal of Innovations in Engineering and Technology - IRJIET*, 9(12), 13-18. Article DOI https://doi.org/10.47001/IRJIET/2025.912003

****