

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

Reduces Attack Surface

The Point:

Permanent privileged accounts increase the risk of exploitation. JIT privilege eliminates standing access, ensuring users have access only when needed.

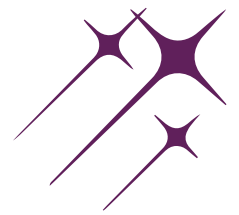
Business Value:

- o Minimizes exposure to credential-based attacks.
- o Lowers the risk of lateral movement in cyberattacks.
- o Reduces the number of privileged accounts attackers can target.



For more content like and follow me: [@bertblevins](#)

Enhances Security and Compliance



The Point:

Many compliance regulations require strict control over privileged access. JIT privilege ensures access is granted only when necessary and logged for auditing.

Business Value:

- o Helps meet compliance requirements (e.g., GDPR, HIPAA, PCI DSS, NIST).
- o Provides a detailed audit trail of privileged access activity.
- o Reduces insider threats by limiting unnecessary standing access.

How to Implement:

- o Enforce multi-factor authentication (MFA) for JIT access requests.
- o Use session recording and logging to track all privileged activities.
- o Implement access expiration policies to ensure temporary access is revoked automatically.

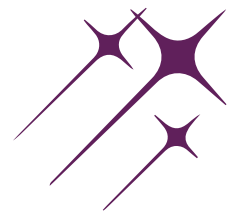
How Compliance Views This:

- o PCI DSS 7.1 & 8.1: Requires limiting privileged access and enforcing strong authentication.
- o HIPAA Security Rule: Mandates strict controls over access to sensitive data.
- o Best Practice: JIT ensures that access is tightly controlled and documented, making audits smoother and reducing the risk of non-compliance fines.



For more content like and follow me: [@bertblevins](#)

Improves Operational Efficiency



The Point:

Traditional privileged access management requires manual intervention, slowing down workflows. JIT privilege automates access provisioning and revocation.

Business Value:

- o Reduces IT overhead by eliminating the need for manual access approvals.
- o Speeds up workflows by granting on-demand access without delays.
- o Enhances user experience by providing access only when necessary.

How to Implement:

- o Integrate JIT access workflows into identity and access management (IAM) systems.
- o Automate access provisioning and deprovisioning using privileged access management (PAM) solutions.
- o Use self-service access requests with approval workflows to streamline operations.

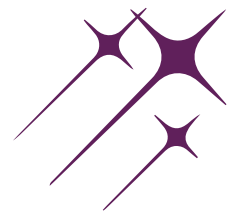
How Compliance Views This:

- o SOX (Sarbanes-Oxley Act): Requires strict access controls and automated enforcement.
- o FISMA & NIST 800-171: Recommend automation to improve security and reduce manual errors.



For more content like and follow me: [@bertblevins](#)

Limits Privileged Credential Misuse



The Point:

JIT privilege eliminates persistent privileged credentials, reducing the likelihood of credential theft or misuse.

Business Value:

- o Prevents misuse of standing admin privileges by insiders or attackers.
- o Reduces the risk of compromised credentials being reused in future attacks.
- o Enhances security posture by enforcing zero standing privileges (ZSP).

How to Implement:

- o Use one-time-use credentials or ephemeral access tokens for privileged actions.
- o Implement privileged session management to monitor and control JIT access usage.
- o Regularly review JIT access logs and reports to detect anomalies.

How Compliance Views This:

- o ISO 27001 A.9.4.3: Requires organizations to enforce strict privileged access control.
- o GDPR Article 32: Recommends limiting access to only necessary personnel.
- o Best Practice: JIT ensures that privileged credentials cannot be misused outside of authorized timeframes, reducing risk exposure and enhancing compliance adherence.



For more content like and follow me: [@bertblevins](#)



**Share your
thoughts in
comments
below**



For more content like and follow me: [@bertblevins](#)