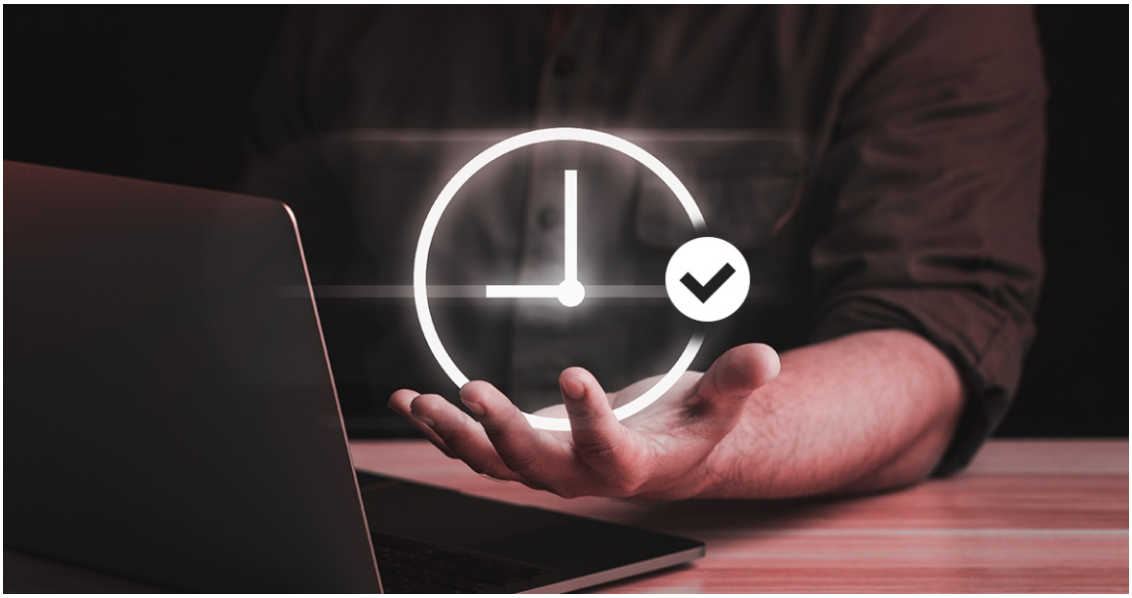
Mitigating the Always-on Risks by Implementing Just-in-Time Privileges (JIT) with ARCON | PAM



Privileged access to systems bypasses normal IT security procedures. Privileged users have elevated access to critical information. Therefore, security leaders must implement just-in-time (JIT) privileges to target systems for mitigating data breaches vulnerability arising from always-on privileges.

Table of content

Overview

One of the key security concerns in Privileged Access Management (PAM) is the lack of implementation of the least privileged principles. Typically, administrators, who in general do not require unconstrained access to systems, are given broad permissions with always-on privileges as a standard IT procedure for "operational ease." Secondly, non-admin privileged users' access, although restricted with granularity, is not foolproof. In both cases, organizations risk privileged access misuse, accidentally or through human error.

The essence of JIT approach is that the right person has access to the right systems at the right time for the right purposes. A user may be a non-admin privileged user, or a system administrator, but with JIT approach - any privileged access would be only on "need-to-know" and "need-to-do" basis. This way, a JIT approach helps to de-risk the PAM threat vector to a large extent and eliminates risk of always-on privileges.

In this whitepaper, we have discovered the gaps that lead to privilege misuse and explained how ARCON | PAM provides necessary tools to implement the JIT approach for various PAM use cases.

Security gaps when there are no JIT privileges approaches - some examples

In the table below, we have highlighted some incidents from the past in which too many and always-on privileges resulted in compromise of corporate confidential information.

Incident	Year	Country	The Damage	Reason
Two employees in an electricity conglomerate from USA misused their privileged rights to steal information of one of their upcoming manufacturing units in China	2019	China & USA	Critical Information about the new plant got leaked and the entire project got to a standstill.	Misuse of privileged rights. Always-on privileges allowed the bad actors to compromise corporate information.

An insider from one of the largest aerospace organizations misused his privileged identity to steal military manufacturing information	2006	China	The military blueprint was compromised.	Misuse of privileged entitlement and absence of JIT access methods.
On the verge of leaving the healthcare organization, a malicious insider misused his "dormant" privileged account to access critical shipping data and delayed deliverables	2020	USA	Shipping system server of the organization was compromised leading to deletion of critical shipping data and eventually vital PPE (personal protective equipment) deliveries got delayed	Misuse of unrequired and unnecessary standing privileges- had the access been removed on time, the incident could have been avoided
A government organization in North America faced a massive data breach where personal data of many teaching professionals were compromised by a malicious insider by misusing his privileged entitlements	2020	North America	Almost 360000 teachers' personal data were compromised, and privacy was breached	Privileged access rights were misused, if standing privileges were removed and time-based access policies were incorporated, then it could have been prevented

Just-in-time (JIT) Privileges concept reduces data breach attack surface

As per thumb rule, enterprises have at least one privileged user for every 10 devices. This number keeps increasing as every layer of IT infrastructure expands with more devices and applications. The risk factor, as a result, multiplies when an enterprise creates long-standing privileges without any concrete justification for creating new privilege entitlements. This way, enterprises open new doors for malefactors if 'elevated accesses' to sensitive information are not given on 'need-to-know' and 'need-to-do' bases. The whole idea of "Least privilege" principle can be jeopardized if malicious insiders with unnecessary standing privileges start to exploit privileged access as they maneuver within an IT ecosystem.

Conversely, Just-in-time Privileges lay the foundation of least privilege concept. This approach mitigates risks arising from 'Always-on' privileges practice. The attempt of the JIT privilege principle is to discard all standing privileges by allowing administrators to grant privileges only when the need arises and revoke privileges after the IT task is completed. This arrangement significantly reduces the data breach attack surface as enterprise security and risk management teams can lock the doors for malicious elements to execute an attack on information assets through misusing privileged access.

The JIT Methods supported by ARCON

Method 1 – Time-based Approach for privileged accounts

John Doe is an IT administrator in a technology company and has multiple collaborations with third-party vendors. As an IT admin, John always ensures that confidential enterprise data is stored securely in encrypted form with limited access to the database and fulfills the regulatory requirements and maintains data integrity. Since third-party vendors have privileged access rights to internal systems for different maintenance tasks frequently, the threat level automatically rises with 'always-on' privileges. The maintenance task demands access to the systems once every fortnight but still John allows 'always-on' privileges to the vendors.

With ARCON's JIT privileges tool, the IT administrative team can assign JIT privilege rights to the third-party only when they require for a predefined period. The privileged rights are revoked automatically at the end of the task or end of the time (whichever is earlier).

ARCON enforces elevation of privileged rights to the users, allows access to privileged accounts or the ability to execute privileged commands. This elevation can be configured and re-configured by the IT administrator regularly. Furthermore, if we talk about time-based access, then the admin can pre-schedule a designated time when the end-user can be elevated only for that time.

Application Elevation policy of JIT approach is a management method that assures that users have zero access to any of the applications unless such access is explicitly granted. It enables the configuration of privileges so that users can request privilege elevation at specific times, for a specific period, and only for the required applications. The admin has the full right to minimize/ maximize time-limit of access - even in between the access period.

Method 2 - JIT Provision/ Deprovision for Access (Infrastructure Apps)

Just-In-Time provisioning offered by ARCON | Privileged Access Management provides end-users with access rights for a limited period only during on-demand situations. The temporary privileged rights given to the end-users are revoked immediately after the end of the task. In this approach, the users can be provisioned, i.e., allowed access for the predefined duration and even de-provisioned, i.e., deny access automatically after the pre-defined duration is expired. Provisioning and Deprovisioning of end-users indirectly certify and de-certify the users based on their roles, rights, and credibility.

JIT Provision/ Deprovision enhances privileged access security realm as it prevents all-time access and provides access only when it is required. At the same time, the logs and reports of every user are maintained for all the access provided, and all the systems/ applications accessed by the user. It enhances IT efficiency as it reduces the time spent on creating credentials in Active Directory. ARCON | PAM Just-In-time privilege ensures access is allowed according to an approval workflow while adhering to security.

Method 3 - JIT Elevation for Privileges -

JIT elevation can be categorized into two different use cases:

i) elevation of users
ii) elevation for application access

Any damage caused by misuse of 'elevated accesses' magnifies the dangers of standing privileges. With JIT privileges practice, enterprise SRM (Security and Risk Management) teams can ensure all users act as standard users and not as privileged users. They can get privileged access only when it is approved by the IT administrator by using a set of approval processes and workflows. Hence, privilege elevation of users occurs when there is an elevation request raised by a user, who wants to perform a defined privileged task at a specified time.

Elevation of users can happen in groups as well. Any user group dedicated to perform any set of tasks can raise elevation request to perform any assigned task. Time and role-based elevation of user groups help IT administrators to keep track of their activities seamlessly.

In this regard, ARCON | Endpoint Privilege Management (EPM) provides ' Temporary Elevation' option to the user. This option can be used whenever a user requires admin access to perform any activity, he/she will have the privilege to raise a request to elevate his/her privilege from standard user to a privileged user with admin rights. ARCON | EPM allows any on-boarded user to gain access to an application based on the user roles and responsibilities for a specified time. Once the time exceeds, the admin rights of the respective user will be automatically revoked, thus ensuring Just-In-Time access.

This way, it helps the enterprise to follow Zero Trust security posture and even stay compliant with the regulatory standards that demand time and role-based access to every critical system.

Method 4 - JIT ephemeral access (for cloud use cases)

JIT privilege can be an essential component for cloud environments, especially multi-cloud environment. With hundreds or thousands of human and non-human (digital) identities accessing cloud resources, consoles, and workloads for day-to-day use cases, the emerging IT security challenges have left enterprises open to data breach risks. It is not just the human identities that need to be protected, but machine identities/non-human identities (devices and cloud workloads such as scripts, containers, VMs, CI/CD tools, RPA tools) must be controlled.

With the help of JIT ephemeral access, enterprises' Just-in-Time privilege interactive access automatically generate rules and role-based temporary access rights for third parties. Amazon Web Services (AWS) Console or Command Line Interface (CLI) component that interacts with AWS Secure Token Service (STS), allows an administrator to customize accounts with unique AWS roles. When a user logs in to the AWS management console, they are assigned to a particular AWS position and regulation, and they can only execute approved operations on the AWS network.

Ephemeral credentials work as temporary access codes that only exist for the duration of the authentication and authorization of privileged connections where the users do not require to enter passwords when communicating. Once the session is over, the credentials are immediately rotated making any further access attempt invalid.

ARCON JIT privilege builds the foundation of Zero Trust architecture

The two vital pillars to build a robust Zero Trust enterprise IT architecture are 'never assume trust' and 'continuously reassess the trust.' Weak privileged access management is often the reason behind the break of trust. Most data breach incidents happen when an organization maintains excessive standing privileges. In this backdrop, the security team fails to detect the misuse of trust leading to systems misuse or abuse.

With ARCON | PAM JIT Privileges tool, the IT security team effectively closes the possibility of misusing the trust. As privileges are granted on-demand, 'trust' is never assumed but must be proved by the IT users. Secondly, ARCON | PAM provides a robust risk detection capability. With the highly effective AI/ML-based Knight Analytics tool, every user identity is constantly monitored and any user behavior that is different from baseline activities are flagged off in real-time with risk scores. This practice of continuous reassessment of trust ensures that risky profiles are never granted privileged access.

Conclusion

The practice of on-demand Privilege Elevation addresses the challenges of whom to allow access for which application, for what purpose and when. Serious security concerns, especially over-privileged users or excessive standing privileges are always there to play a spoilsport. Once the JIT privilege tool is implemented, the enterprise IT risk control teams can ensure all the end-users as standard users and these users are granted privileged rights only when there is a demand. The administrator can also ensure secure access control as the JIT approach ensures -

1. Removal of standing privileges
2. Denying of Privileged Access once the defined privilege task is completed
3. Foundation for Zero Trust security framework
4. Implementation of Least Privilege principle
5. Reduces data breach threat vector

About ARCON

ARCON is a leading enterprise information risk control solution provider, specializing in Privileged Access Management (PAM) and continuous risk assessment solutions. Our mission is to help enterprises identify emerging technology risks and help mitigate them by robust solutions that predict, protect and prevent.