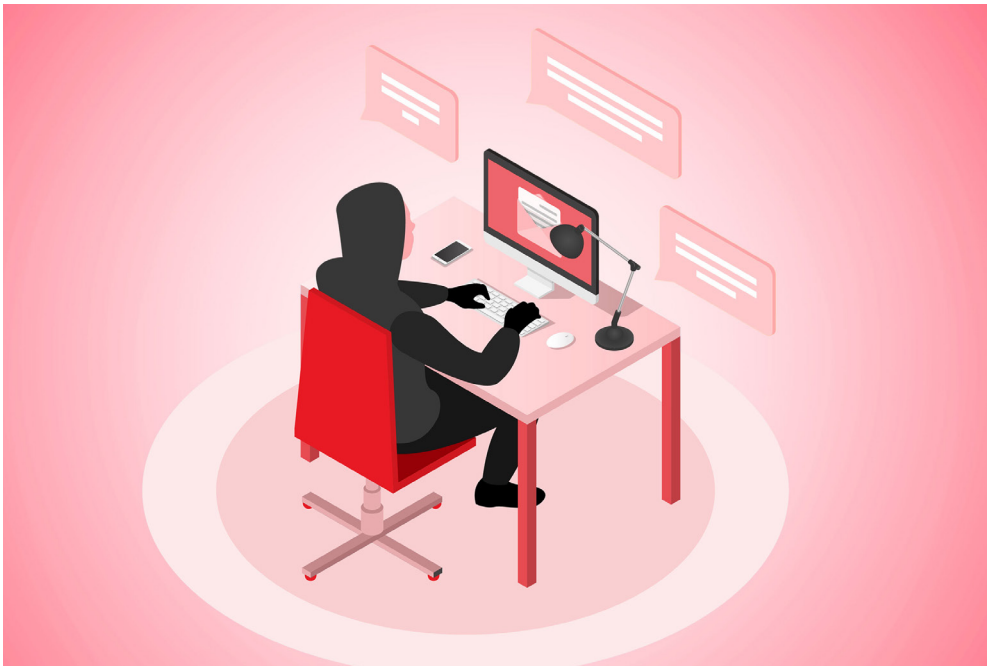
Leverage Just-in-time Privileges with ARCON | Privileged Access Management

The notion - 'Right person has the right to access the right target systems at the right time' is simplified with the ARCON | PAM Just- in-Time (JIT) privileges tool.
The solution offers best Privileged Access Management practices to overcome the risk arising from standing privileges, laying the foundation for the Zero Trust Architecture.

Table of content

Part 1. Too Much liberty is counterproductive



Liberty is one of the most critical components of a progressive and democratic society, however, too much liberty, as many historical evidences suggest, can be counterproductive. If there are no checks and balances along with lack of institutional structure to command rules and regulations, corruption and chaos would destabilize a society. Enterprise's Privileged Access Management practice is very much the same. Whereas a well-defined privileged access regulations as to people and policies offer an unambiguous workflow environment, excessive standing privileges may result in a catastrophe. As these accounts have 'elevated access' to highly sensitive information, privileged account abuse due to unaccounted standing privileges can result in massive data breach incidents that can be hard to recover both from a financial and reputational perspective.

From the onset, managing, monitoring and controlling privileged users was never a simple task due to the fact that privileged accounts are often shared and privileged users are distributed across multiple data center environments. What makes them more risky is with increased adoption of cloud computing, virtualization, and DevOps practice, the sheer number of privileged accounts have exploded. Due to the above, there is always room for malicious actors to exploit vulnerabilities arising out of standing privileges if they are operated in uncontrolled environments.

Part 2. Just-in-time (JIT) Privileges concept reduces data breach attack surface

As a rule of thumb, for every 10 devices, enterprise has at least one privileged user. This number will keep increasing as every layer of IT infrastructure expands with more number of devices and applications. The risk factor in turn multiplies when an enterprise creates long-standing privileges without any justification for creating new privilege entitlements. Organizations are opening the doors to malefactors if those 'elevated access' to sensitive information are not given in 'need-to-know' and 'need-to-do' bases. The whole concept of Least privilege can be jeopardized if malicious corporate insiders with an unnecessary high number of privileges start to exploit privileged access as they maneuver within an IT ecosystem.

Conversely, Just-in-time Privileges lays 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.

Part 3. Enterprise Use Cases that require removing standing privileges

Before we discuss several use cases for basing the urgent need to implement the ARCON | PAM JIT privileges tool, let's discuss what privileged users are entitled to do in an enterprise IT set-up. Privileged entitlements allow users to access the following target systems and applications in various environments.

Environment	IT Resources	Privileged Access Users
On-premises	Network Devices, Databases, Servers, Applications, and Services	Privileged Access Users
Cloud	Management Consoles, Hosted Applications, Virtual Machines, and Root Accounts	Personal Accounts, Elevated Personal Accounts (Network Admin) Elevated shared Account (Applications, \ services, VMs, Middleware)
DevOps	Scripts, Executable Deployments, and CI/CD tools	Developers, Testers, Deployment c onsultants

The damage caused by abuse or misuse of 'elevated access' to these highly critical IT resources magnifies in the case of standing privileges. With JIT privileges practice, enterprise IT risk control teams can ensure all users act as standard users-- not as privileged users, and get privileged access only when it is recognized by the Administrator (using a set of processes and workflows) that a particular user who has raised a request, wants to perform a defined privileged task at the specified time.

Use Case 1: Removing standing privilege by limiting access to systems and applications

It is important to remember that no IT user can be granted 'always on' privileges. Even in the case of administrators that are responsible for changing the security configuration of systems and applications, have their privileged credentials vaulted along with session management. Which means that no privileged access is over and above the other. So why does the IT administrative department take risk by assigning standing privileges? Why do personal privileged accounts exist? It is always better to find out how frequently one wants to access systems. Accordingly, the IT team should grant JIT privileges.

Use Case 2: Restrict access time wise to remove unnecessary 'always on' access

John Doe, a Database administrator, works in an insurance company, which has consulting contracts with third-party vendors. As a database admin, John has to ensure that the sensitive data is stored securely to fulfill the regulatory requirements and maintain data integrity. However, since third-party has privileged access to internal systems for frequent maintenance tasks, the threat level automatically rises with 'always on' privileges even as the maintenance task demands once every fortnight access to systems. With the JIT privileges tool, the IT administrative team can assign JIT privileges to the third-party depending on when they require those.

Use Case 3: Removing standing privileges by limiting the count of IT administrative and operational staff

There is a tendency among IT administrative departments to make certain identities, mostly system administrators, work as super users. Those identities hold the key to access multiple systems even though they seldom access all. This mistake could lead to accidental deletion of files whilst it also increases the count of standing privileges. With JIT Privileges approach, the IT administrators can lower the count of IT users by a ssigning privileges to only who is requiring it.

Use Case 4: Limiting privileged access at granular level

Complex privilege identity management is often a deterrent for IT security teams to provide privileged access for multiple users, leading to excessive standing privileges. ARCON | PAM JIT privileges tool not only removes standing privileges but also offers a capability to restrict access and commands based on server wise/ user wise / group wise.

Part 4. ARCON JIT Privileges tool builds the foundation for Zero Trust Architecture

The two vital pillars to build a robust Zero Trust enterprise IT architeture are 'Never assume trust' and 'continuously re-assess 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 has to be proved by the IT users.

Secondly, ARCON|PAM provides a robust risk detection capability. With highly effective tool Knight Analytics, every user identity is constantly monitored and user behavior anomalies like doing something different from baseline activities are flagged in real-time with risk scores. This practice of continuously re-assessing the trust ensures that risky profiles are never granted privileged access.

Conclusion

ARCON PAM | JIT Privileges is a powerful tool which ensures privileged access is allowed according to an approval workflow while adhering to security.
The benefits include:

1. Removal of standing privileges
2. Privileged Access is denied once the defined privilege task is completed
3. Enhances administration's IT experience by reducing time spent on creating AD credentials
4. Builds the foundation for Zero Trust framework
5. Implementation of Least Privilege principle

About ARCON

ARCON is a leading Information Risk Management solutions provider specializing in Privileged Access Management and Continuous Risk Assessment solutions.

ARCON Privileged Access Management (PAM) is a leading global product and a robust solution that mitigates risks arising out of privilege identity and access management

Connect with us