CYBERARK

SOLUTION BRIEF

REDUCE RISK WITH CYBERARK JUST-IN-TIME PRIVILEGED ACCESS MANAGEMENT

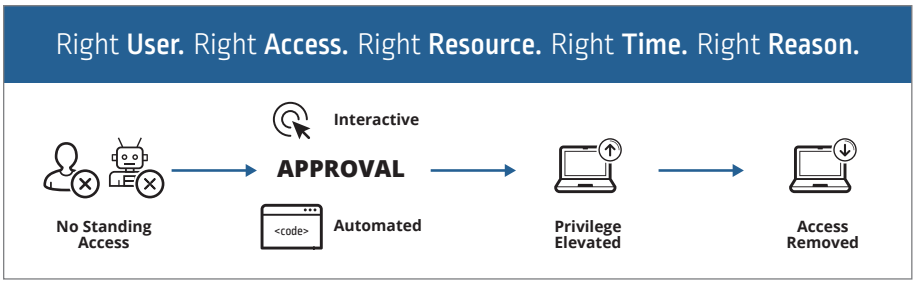
PREVENT COSTLY ACCOUNT TAKEOVERS

Provide the Right Users the Right Access to the Right Resources at the Right Time for the Right Reasons

Privileged accounts represent one of the largest security vulnerability an organization faces today. In the wrong hands they can be used to steal sensitive data and cause irreparable damage to the business. These powerful accounts and the access they provide can spell game over for an organization if not properly secured. However, these accounts are sometimes granted "always on" access, when in reality they are only required for brief periods of intermittent time. Securing access "just-in-time" or only providing the appropriate levels of access to the right resources for the right amount of time is a method within Privileged Access Management (PAM) that adheres to the principle of least privilege because it strips away standing access and only provides access to these privileged accounts when absolutely essential. The CyberArk Privileged Access Security Solution supports a variety of just-in-time (JIT) security controls to ensure the right users (human or non-human) have access to the right resources, at the right times, for the right reasons and builds on the principle of least privilege to minimize privileged access that is not directly required.

KEY BENEFITS

- Reduce risk by eliminating standing privileges
- Improve user productivity by avoiding drawn-out approval processes
- Simplify operations by automating access request and consent functions via policy
- Improve least privilege security posture by elevating privileges only when and where required
- Improve compliance and threat detection and remediation with real-time session monitoring and recording



With Real-time Session Monitoring and Recording

CyberArk has a variety of JIT PAM functionality that reduce exposure and risk by eliminating unnecessary standing privileges and letting administrators interactively or automatically grant authorized users access to specific systems, applications or functions for finite periods of time, on an as-needed basis. CyberArk also has out-of-the-box integrations with many leading ITSM and IGA solutions to automate approval and authentication processes via policies. JIT security improves user productivity by streamlining workflows, ensuring individuals can quickly access what they need, when they need it—without enduring drawn-out, manual approval processes. JIT access can also, in some cases, provide the quickest time to value by reducing the cost, time and resources needed to implement appropriate levels of privileged access.

MULTIPLE JIT PRIVILEGED ACCESS MANAGEMENT METHODS SATISFY DIVERSE REQUIREMENTS

CyberArk supports three distinct JIT privileged access management methods, satisfying a variety of requirements and use cases stemming from an organization's risk profile:

- **Temporary Elevation** –where a user's access rights are raised for a predetermined period so they can perform certain privileged functions.
- **Ephemeral Accounts** – where single-use privileged accounts are created on-the-fly, and immediately deprovisioned or deleted after use.
- **Broker and Remove Access** – where shared privileged accounts are provisioned in advance but aren't enabled until a user expressly requests and is granted access by an administrator.

JIT Method	Temporary Elevation	Ephemeral Accounts	Broker and Remove Access
CYBERARK SOLUTIONS	▪ JIT Elevation and Access with CyberArk Endpoint Privilege Manager ▪ JIT Elevation and Access with CyberArk Core Privileged Access Security Solution ▪ JIT Elevation and Access with Short-Lived SSH Certifcates	▪ Privileged Session Manager SSH Proxy and Active Directory Bridging ▪ AWS STS Integration	▪ CyberArk Core Privileged Access Security Solution ▪ CyberArk Alero

Every organization is different and may want to remove standing access for a specific subset of internal resources for any number of reasons. While other privileged access vendors may offer singular approaches to JIT access, CyberArk offers the broadest set of just-in-time use cases to enable least privilege and helps to ensure that access is only provided when needed and for no longer than required - regardless of user type, target system or environment. This can be done through federation and governance of just-in-time access policies, or the use of CyberArk as an intermediary to broker sessions but never expose the users to actually use a username and password.

TEMPORARY ELEVATION

Organizations can use CyberArk Endpoint Privilege Manager to grant temporary local admin access to Windows workstations, servers, and Macs on a per-request basis, for a fixed length of time, after which privileges are revoked from their sessions and applications. JIT Elevation and Access with Endpoint Privilege Manager is an agent-based solution that provides a full audit trail of all privileged access activities, and also allows administrators to terminate applications and sessions in real time.

Organizations can also leverage CyberArk Core Privileged Access Security as an agentless alternative to JIT Elevation and Access, allowing users to gain Windows local admin access through the CyberArk web console for a set period of time upon successful request.

JIT Elevation and Access with Short-Lived SSH Certificates enables secure access to existing or newly created instances in Linux systems without the need to manage accounts or credentials. When a user requests access, CyberArk signs an SSH Key and provides a certificate just-in-time as a one-time use before it is discarded. This method isolates and secures just-in-time SSH access to existing or newly created instances without the need for credentials, public keys or standing access on *NIX targets.

EPHEMERAL ACCOUNTS

For Amazon Web Services: Together, CyberArk Core Privileged Access Security integrates with the AWS Security Token Service (STS) to give AWS Identity and Access Management users temporary, limited-privileged credentials based on roles or administratively defined policies. The solution lets you control privileged access to the AWS Management Console or AWS APIs, and it records and monitors all privileged access activities in real time allowing for remediation capabilities in the event of anomalous behavior or activities.

For Unix and Linux Systems: Organizations can also use the CyberArk Least Privilege Server Protection for *NIX solution to grant temporary access to Unix and Linux systems based on Microsoft Active Directory permissions. The solution automatically creates a short-lived, ephemeral account and establishes a one-time session for an authorized user which requires re-authorization if further access is required. The account is immediately deleted when the session is terminated.

BROKER AND REMOVE ACCESS FOR QUICK DEPLOYMENT

Finally, organizations can use CyberArk Core Privileged Access Security to smoothly implement JIT security controls using pooled privileged accounts on target systems. A user can request access to the account for a defined time period via the CyberArk web console. Once approved, either by a manager or via policy, the user is granted restricted access to the target system until the time window expires. All sessions are automatically isolated, recorded and monitored in real-time to prevent misuse or lateral movement.

CyberArk® Alero™ can be leveraged by organizations who provide access to third parties who require access to critical internal resources. As part of the onboarding process, Alero Administrators provision access to these third party vendors for a period of time (either in days or in number of sessions), upon which they are automatically deprovisioned and need to be onboarded again if further access is required. Similarly, because of Alero's full integration with CyberArk Core Privileged Access Security, all sessions that these third parties create are automatically isolated, recorded and monitored in real time.

RECOMMENDATIONS

Just-in-time access is a conceptual framework that can be solved in a variety of ways within an overall PAM strategy with the goal of implementing least privilege best practices. However, before deciding which route is appropriate it is important to acknowledge that JIT is not a silver bullet to securing the organization. As with anything, there are both security and operational considerations when selecting a strategy to eliminate standing access and institute JIT, weighing when it is even appropriate to begin with. Every organization should first identify the use cases, platforms and groups that they are looking to secure, then decide where it is appropriate to implement JIT and move forward accordingly. CyberArk has the industry's widest variety of options for JIT access controls that help to remove standing access and privilege and keep critical resources secure.

About CyberArk

CyberArk is the global leader in privileged access management, a critical layer of IT security to protect data, infrastructure and assets across the enterprise, in the cloud and throughout the DevOps pipeline. CyberArk delivers the industry's most complete solution to reduce risk created by privileged credentials and secrets. The company is trusted by the world's leading organizations, including more than 50 percent of the Fortune 100, to protect against external attackers and malicious insiders. To learn more, visit us at www.cyberark.com.