Monitor User Access to Regulated IT Environments

Monitor and record privileged user activity to comply with audit requirements.

Why CyberArk?

CyberArk is the trusted expert in stopping cyber attacks before they stop business.

The Challenge

Privileged accounts provide direct access to an organization's most sensitive data, and these accounts are frequently targeted by attackers in an effort to steal credit card data, private health information, financial data and more. To protect consumers in this threat environment, several regulatory bodies now require organizations to proactively secure, monitor and record all privileged account activity to prevent unauthorized access to sensitive data and quickly detect if unauthorized access does occur.

To demonstrate compliance with most privileged account security requirements, organizations must be able to clearly audit all privileged user activity, ensure the integrity of the audit trail, and prevent users from bypassing privileged account controls. Without the proper tools in place, organizations can face a variety of challenges:

- **Inability to record and monitor user activity in real-time.** Many regulations require organizations to record privileged user activity, and some go a step further to require live monitoring of all user access to regulated systems. However, without effective tools in place it can be difficult – if not impossible – to track and view exactly who is accessing what privileged accounts and what is happening during those privileged sessions..
- **Siloed and incomplete audit trails.** In large, diverse IT environments, organizations are often forced to manually piece together log data from individual systems to create a more complete audit trail of privileged user activity. This process is difficult, time-consuming, prone to human error and can result in incomplete audit trails.
- **Ineffective security controls.** To meet regulatory standards, organizations are often required to monitor and record privileged user activity. However, if the controls in place to monitor and record this activity can easily be altered or bypassed, then the tools are ultimately ineffective, create unreliable audit trails, and increase the risk of failed audits.
- **Costly audit processes.** During the course of an audit, auditors typically look for specific activities as well as activities conducted by specific users. Without a way to easily search through months of activity logs, user histories, and session recordings, organizations can find themselves facing lengthy audit times and incurring high audit costs as a result.

To comply with many privileged account security requirements, organizations must be able provide comprehensive histories of all privileged account activity, as well as proof that the audit trail is genuine. Without the ability to audit all privileged activity in the regulated environment and assure the integrity of those audit trails, organizations can face failed audits, regulatory fines and other penalties.

The Solution

To effectively control and monitor all privileged user activity, organizations should consider establishing all privileged user sessions on a secure jump server and recording all activity that occurs via that jump server. With a secure jump server in place – between the user and the target system – organizations can effectively create a single point of control for all privileged session activity that cannot be bypassed by even the most skilled users.

Once all privileged sessions are forced through a secure jump server, organizations can use a tamper-proof recorder to record and monitor all session activity from a single, centralized location. An ideal solution should also enable interactive search so that audit and security teams can quickly and easily locate specific activities and incidents, replay a precise moment of a privileged session, and gain a complete understanding of exactly what occurred. To ensure audit integrity – as well as prevent malicious

users from covering their tracks – organizations should ensure that all privileged session recordings and audit logs are stored in a highly secure, access-controlled vault that is only accessible by authorized members of the audit and security teams.

With such a solution in place, organizations can effectively address compliance requirements, accelerate audit time and minimize audit costs.

Benefits

By implementing privileged session recording and monitoring via a secure jump server, organizations can:

- **Easily monitor and record privileged user activity.** By forcing all user access to regulated environments through a secure jump server, organizations can easily monitor and record all activity that occurs via that jump server. As a result, audit and security teams can monitor sessions in real-time to look for suspicious activity and immediately terminate suspicious sessions. Comprehensive recordings provide organizations with a complete history of who accessed what accounts and what each user did during each privileged session.
- **Gain a complete audit trail of all privileged user activity.** By monitoring and recording privileged user activity on a centralized jump server, organizations can track privileged user activity on most platforms all from a single location. This approach provides organizations with a centralized, reliable audit trail of all privileged activity across a wide variety of enterprise systems and custom applications.
- **Prevent users from circumventing controls.** To prevent users from bypassing session monitoring and recording, organizations should consider pairing a secure jump server with a credential vault. By integrating these complementary solutions, organizations can prevent privileged users from knowing privileged account credentials and using the credentials to directly access target systems. Further, by securing and hardening the jump server, skilled users are unable to turn off or alter recording capabilities.
- **Accelerate audit times to minimize audit costs.** By enabling interactive search of audit logs and session recordings, auditors can quickly search for and locate specific activities of interest. As a result, auditors can spend less time sorting through logs and more time evaluating the users and activities that matter most. This time savings can translate into shorter audit times and lower audit costs.

By implementing session monitoring and recording controls that can support the vast majority of IT systems, preventing users from bypassing these controls, and storing the audit histories in a tamper-proof, access controlled vault, organizations can confidently demonstrate compliance with requirements. This means organizations can accelerate audit times, reduce audit costs and more easily prove compliance with regulatory requirements.

CyberArk's Solution

CyberArk Privileged Session Manager acts a secure jump server, enabling organizations to record and monitor privileged session activity in real-time from a single, centralized control point. The solution supports a variety of systems including Windows, Unix, databases, mainframes, virtual infrastructures, web applications and more to ensure that organizations can track user activity throughout their regulated environments. Audit logs and session recordings are stored in the tamper-proof Digital Vault, accessible only by authorized members of the security and audit teams. When coupled with CyberArk's credential vault solutions, CyberArk Privileged Session Manager ensures that privileged credentials can never reach users or their devices, thus preventing users from bypassing controls to gain unmonitored access to privileged accounts.

CyberArk Privileged Session Manager seamlessly integrates into the CyberArk Privileged Account Security Solution, enabling organizations to secure, protect and detect suspicious usage of privileged account credentials from one common infrastructure that is managed behind a single pane of glass.