KPMG and CyberArk

Protect your information with a tested privileged account security solution

The list of news headlines continues to grow: Millions of dollars diverted through a financial services communication network. Hundreds of millions of credit card numbers stolen from retailers. Millions of individual health records compromised. The common thread across many of these breaches—and the countless others that continue to go undiscovered—is the compromise of privileged credentials.

Privileged credentials represent "the keys to the IT kingdom." Intended for use only by authorized administrators, privileged credentials have very little, if any, restrictions on their capabilities. These credentials unlock accounts that can be used to modify system configurations, access sensitive information, and even shut systems down, making them a preferred target of external attackers and malicious insiders alike. An untold number of global superpowers and Fortune 100 companies have fallen victim to privileged credential theft, resulting in malicious attacks on their data and disruptions of service that resulted in irreparable harm to their reputation and expensive, lengthy litigation.

Humans comprise the new perimeter, and even with the best technology and security training, they continue to fall victim to targeted attacks. The use of spear phishing and social engineering has exploded, often granting attackers their first foothold inside an organization's systems. From an initial entry point, attackers can use the limited, local access to escalate privileges, pivot throughout the environment, and ultimately gain complete administrative control over entire domains. Because these attackers operate using legitimate, yet compromised, privileged accounts, the attacks often go undetected for months, allowing for uninterrupted reconnaissance and the strategic placement of malware that can be used to exfiltrate data, cause system outages, and wreak havoc across the organization. These risks are exponentially increased in organizations that provide vendors and third parties with access to the corporate network.

It is critical that organizations properly secure privileged credentials, including passwords and Secure Shell (SSH) keys, by taking a broad approach to privileged access management (PAM). This approach should include:

- Defining an enterprise strategy and roadmap, typically across a three- to five-year horizon, that lays out the objectives of the PAM program
- Identifying critical data, the infrastructure that supports the storage and processing of this data, and the accounts used to support each technology layer
- Understanding who requires access to these accounts, why this access is required, and enforcing controls to restrict access to only these teams and individuals
- Integrating logging and monitoring, and alerting technologies that may already exist in the environment
- Building PAM into the existing systems development lifecycle (SDLC) and change management processes.

Why KPMG

KPMG Cyber helps businesses maintain the confidentiality, integrity, and availability of critical business functions in a world where cyber attacks and unauthorized data leaks threaten organizations across the globe. KPMG Cyber utilizes its extensive experience across diverse business and technical environments and various industries. This allows KPMG LLP (KPMG) to better understand your organization's risk exposure and organizational needs, enabling full consideration across people, process, and technology that helps you align security capabilities with your organization's enterprise strategy and objectives.

When addressing PAM, KPMG Cyber builds upon experience performing security and identity assessments, developing enterprise security strategies and processes, and executing solution implementations. This leads to a thorough understanding of your organization's current state and security posture, a detailed roadmap to improve in key areas to rapidly reduce risk and address compliance issues, and the subject matter professionals who can help you execute this road map to implement and operationalize capabilities while addressing the necessary technological and people-based changes that may be needed.

By working with KPMG, you can benefit from:

An acknowledged leader in cyber security—KPMG International has been named a leader in the Forrester Research Inc. report, The Forrester Wave™: Information Security Consulting Services, Q1 2019, achieving the highest score for current offering and strategy (tied).

KPMG's established track record with CyberArk—KPMG has been working with CyberArk since 2011. Over that span of time, we have completed numerous PAM implementations for clients in a varying range of industries.

Our commitment to continued education—Due to the volume of PAM projects that we have executed on past engagements and to support for those to come, KPMG has a staff of more than 50 team members who have taken CyberArk-led product training.

Our distinct deployment methodology and engagement accelerators—We have developed a distinct deployment methodology based on a combination of multiple industry frameworks, as well as our wealth of experiences deploying PAM solutions in the field.

Is the Privileged Access Security offering by KPMG and CyberArk right for you?

- Have you experienced the departure of any dissatisfied employees—especially system administrators—who may have had access to privileged accounts?
- Do certain accounts share the same password across multiple systems or throughout the environment?
- Do you confidently know who is accessing what data throughout your enterprise IT environment?
- Does your organization maintain large sets of PII and PHI data?
- Has your company been the target of a data breach?
- Does your organization provide vendors and third parties with access to your network environment, systems, or applications?
- Are you required to meet regulatory and compliance requirements, especially those that pertain to sensitive data controls?

Why CyberArk

CyberArk focuses on protecting against targeted cyber threats that can penetrate organizations and attack the heart of the enterprise while remaining undetected. CyberArk is trusted by some of the world's leading companies—including more than 40 percent of the Fortune 100—to protect their highest-value assets, enabling these companies to meet and exceed even the most stringent audit and IT compliance requirements.

The CyberArk Privileged Account Security solution combines multiple technology modules in a single broad solution. Designed from the ground up with security in mind, the CyberArk solution can serve as a critical component in helping your organization secure, manage, and control access to privileged user and application credentials to help you proactively prevent the abuse and misuse of privileged accounts. The software can also help you monitor and analyze privileged account activity to quickly detect and respond to potential privileged account threats across the enterprise. Combined, the solution enables:

- Continuous discovery to maintain a complete and accurate inventory of privileged accounts throughout the environment
- Secure storage of privileged account credentials and access controls to help prevent unauthorized account usage, including support for multifactor authentication
- Robust logging and monitoring of privileged activity to not only maintain an audit record of who accessed credentials and systems, but also detailed logs and video recordings of all activities
- Automatic credential management, including password and SSH key rotation and enforcement of password complexity, history, and other requirements
- Centralized enforcement of least privilege policies to provide users with the permissions needed for their day-to-day roles while eliminating unnecessary privileges
- Behavioral analysis of user and account activity to detect and alert on anomalous activity that may indicate an attack is in process

Better together: KPMG and CyberArk

Enforcing the appropriate controls and mechanisms to protect privileged accounts takes more than just a technology solution. With experience working together on more than 50 successful client projects in multiple regions, KPMG and CyberArk can help your organization develop and implement a broad PAM program that aligns with organizational priorities, risk appetite, and compliance needs. By combining a leading information security team with an advanced privileged account security technology solution, your organization can rapidly reduce the risk posed by unmanaged privileged accounts and address compliance needs related to access controls.

Many organizations purchase a PAM solution with a narrowly focused, single use case in mind. Whether that use case is secure password storage or even basic tracking of the use of privileged accounts, this often leads to a lack of planning at the enterprise level. Technology should be used as an enabler to drive the overall PAM program and strategy, not the other way around. The KPMG and CyberArk alliance takes this into consideration while engaging with clients to protect and monitor privileged accounts, as well as detect, alert, and respond to privileged account threats.

Potential benefits from working with KPMG and CyberArk

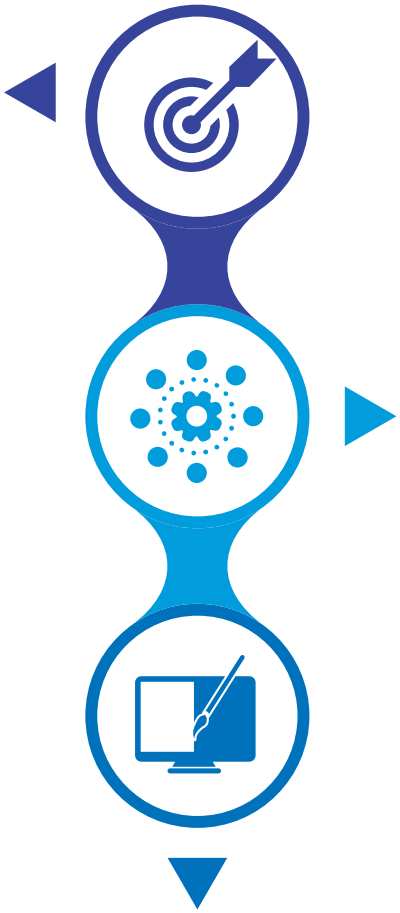
By working with KPMG and CyberArk, your organization can benefit from:

- A broad PAM strategy, roadmap, and approach developed with the experience, knowledge, and know-how of a leading information security consulting team combined with an advanced privileged account security technology
- Implementation of a security agenda that prioritizes risk reduction and regulatory and compliance requirements to help minimize enterprise risk and limit market exposure
- A holistic approach that helps organizations protect and monitor privileged access, as well as detect, alert, and respond to privileged account threats before irreparable damage happens

The PAM offering is comprised of a three-phase approach:

Strategic planning and requirements development

- Understand the organization's needs, goals, and objectives and develop a broad strategy and approach to improving security controls
- Define privileged accounts in the context of the organization's technology and risk environment
- Develop a framework to identify, analyze, risk rank, and prioritize privileged accounts and assign appropriate controls
- Define a target operating model that provides a holistic view of operational roles and responsibilities, as well as detailed policies, processes, and procedures
- Identify business, functional, and technical requirements for a PAM solution



Technology implementation and process development

- Discover privileged accounts throughout the environment and identify:
  - Why these accounts exist
  - Who is responsible and accountable for the account's usage
  - The level of risk that these accounts pose to the environment
  - The appropriate control level for these accounts
  - How to prioritize these accounts to apply the appropriate controls
  - How to enforce these controls and monitor compliance
- Develop a scalable solution architecture that addresses the organization's needs in the current and future state
- Implement and configure the solution and develop supporting policies, processes, and procedures to enable continuous identification and analysis of privileged accounts
- Define integration points for PAM, including the SDLC process, change management, and risk assessments
- Execute use case testing to confirm that the solution meets organizational needs and addresses risk remediation and compliance requirements

Operationalization and continuous improvement

- Conduct end-user training to increase operational efficiency and user acceptance
- Integrate the solution with SIEM technologies for logging, monitoring, and alerting capabilities and implement analytics to better understand privileged account usage and further improve access controls
- Configure the solution to work with all technological layers, including those that require custom configuration to enable controls throughout the enterprise environment
- Reduce dependencies on manual processes and implement automated capabilities for system builds and other procedures

To determine if the KPMG and CyberArk Privileged Account Security offering is right for you, please contact:

Hemal Shah
Principal, Advisory, Cyber Security
214-601-8198
hpshah@kpmg.com

Mike Battillo
Senior Director, Cyber Security
617-529-6037
mbattillo@kpmg.com

Deborah Patterson
Senior Director, Alliances
512-423-6150
deborahpatterson@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia