CYBERARK®

WHITE PAPER

CYBERARK SERVICES

Table of Contents

Improving Privileged Account Security by Maximizing the Value from CyberArk Solutions

Organizations increasingly recognize that one of the most effective preventative steps to protecting their business is to secure privileged accounts. Yet in complex enterprises with thousands, or even tens of thousands of privileged accounts, this is not always easy. Organizations want to move quickly but where to start?

> "The consultant and your local sales engineering staff are a huge asset to your company. Being able to get an expert opinion rapidly was a huge factor in our ability to quickly get a full project plan developed. The plan put everyone both here and in the US at ease that our project goals are achievable."
>
> — Security Director, Top 25 Global Bank

Choosing the CyberArk Privileged Account Security Solution means making the commitment to better protect the enterprise by locking down privileged accounts and secrets wherever they live: on-premises, in cloud or hybrid environments, and DevOps pipelines. CyberArk Services help expedite the development of best practices in a privileged account security program by providing the expertise and experience where and when needed. Clients could also realize ROI of their CyberArk solutions faster by engaging with CyberArk Services. Overall, the goal of CyberArk Services is to provide frameworks and help build the in-house expertise necessary to move towards a robust privileged account security program.

Securing Privilege Is Not a One-time Event

CyberArk Services provides options to move quickly in establishing a privileged account security program and also to stay current by identifying new vulnerabilities from an ever-changing threat environment. Internal teams gain expertise through hands-on experience with CyberArk Services and Customer Support teams delivered through formal training and certification opportunities.

CyberArk helps enterprises start to build a privileged account security program through structured engagements that use frameworks for bringing together people, processes and technologies. CyberArk's Sprint framework was developed in conjunction with a CISO panel to help organizations quickly protect privileged credentials. CyberArk has also developed another framework, the Privileged Account Security Hygiene program, which helps internal teams to "think like an attacker." Through the "Privileged Account Security Hygiene program," organizations will regularly examine and re-evaluate programs for new potential vulnerabilities and ensure outstanding risks are addressed. Along with the use of Red Team attack simulations, internal teams can measure progress using periodic infrastructure scans to discover unprotected backdoors.

A Broad Range of Services Based on Deep Privileged Account Security Experience

CyberArk's highly skilled privileged account security experts have worked with thousands of successful enterprise implementations worldwide. Service professionals help organizations strategically build out their privileged account security program through a unique combination of technology and cyber security expertise.

- **CyberArk Security Services** include:
  - Consulting Services for privileged account security program design, including securing DevOps and cloud environments;
  - Implementation Services to simplify initial deployment, as well as the expansion of program deployment;
  - Onboarding Services to prioritize and jump-start usage and management of privileged accounts;
  - Program Management Services to coordinate, track and facilitate communication for a smooth and cost-effective development of a privileged account security program.
- **CyberArk Red Team Services** provide a safe, ongoing way for security operations teams to test their ability to effectively defend against cyber-attacks, in on-premises, cloud and DevOps environments.

- **CyberArk Training and Certifications** help build and maintain internal expertise in fundamental and advanced topics to better manage the privileged account security program.
- **CyberArk Customer Support Services** ensure the Privileged Account Security Solution is up-to-date and running efficiently.

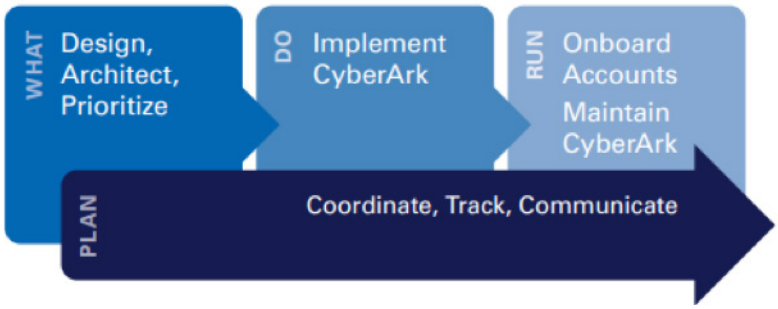
Most services are customized to align with the specific cyber security and IT compliance priorities of the organization as well as to help realize the maximum business benefit and value from investment in the CyberArk Privileged Account Security Solution.

CyberArk Security Services

CyberArk Security Services expedite privileged account security programs by providing the expertise to identify and prioritize the most important privileged accounts. Once identified, CyberArk Professionals will offer design, implementation and project-management expertise to achieve the optimum privileged account protection posture. In short, CyberArk Security Services help organizations maximize tangible value sooner.

While each customer's situation and needs can be very different, a typical customer engagement is supported by a project team which may include:

- Consulting services for program design (the "what to do");
- Implementation services for program execution (guiding the internal team engaged in the actual "doing");
- Onboarding services for the privileged accounts (the "running" of the program");
- Program management expertise to help coordinate and enable a successful, cost-effective privileged account security program (the "planning").



CyberArk Engagement Team

CyberArk Consulting Services

CyberArk Consulting Services teams design, architect and prioritize the initiatives and approaches that will establish an organization's unique privileged account security program using the CyberArk Privileged Account Security Solution. CyberArk also offers specialized consulting services for secure DevOps and cloud environments.

CyberArk offers a wide variety of services which include the use of CyberArk's Sprint and Privileged Account Hygiene frameworks to meet the unique needs of each organization.

During Program Design, the Consulting team provides a powerful combination of deep enterprise expertise and proven security best practices. Depending on the organization's needs, Consulting Services engagements may include:

- Designing customized solutions that are aligned to requirements for availability, capacity and redundancy;
- Developing strategic recommendations to integrate the privileged account security program with the organization's overall security road map;
- Proposing a roll-out strategy based upon lessons learned, e.g. from post-breach environments, to quickly protect privileged credentials;
- Outlining a focused approach to risk reduction and reducing lateral movement while securing privileged credentials;

- Collaborating and aligning with project managers to define and drive measurable success;
- Defining a hygiene program and establishing fundamental requirements to build a privileged account security program.

A proactive, security-first approach combined with proven implementation methodologies and post-breach experiences helps ensure privileged account security programs are designed to maximize value and Return-on-Investment.

CyberArk Implementation Services

CyberArk Implementation Services teams simplify deployment and reduce the time and internal resources required to implement, expand and manage CyberArk solutions for a positive ROI.

CyberArk experts guide internal teams through the deployment of the CyberArk Privileged Account Security Solution based upon the recommended design, architecture and roll out strategy developed by Consulting Services for the organization's privileged account security program. CyberArk implementation teams include CyberArk certified, trusted experts who have advanced skills, enterprise-level field experience, and hands-on expertise not only in CyberArk solutions, but also, more broadly, in computing infrastructure and cyber security.

Consulting Services for Secure DevOps and Cloud Environments

Ensuring the security of DevOps environments and continuous integration and continuous delivery (CI/CD) processes is increasingly critical as organizations leverage these approaches to increase their business agility.

CyberArk has deep expertise helping customers to secure their DevOps and cloud environments. This includes developing strategies and business plans to ensure that secure DevOps is an operational reality, establishing operational metrics, developing, deploying and configuring CyberArk to secure cloud workloads on all the major cloud platforms.

Implementation services may include:

- CyberArk Privileged Account Security Solution installation and configuration
  - Pre-requisites planning and preparation;
  - Product installation (initial and during upgrades and migrations);
  - Component deployment and configurations;
  - Assist with onboarding an initial set of privileged accounts;
  - Enterprise integrations.
- Deployment expansion
  - Analysis, validation, and optimization of environmental health, performance and functions;
  - Expansion of product usage, deployment, and on-boarding of privileged credentials;
  - Best practices in operations, maintenance and administration.

CyberArk believes knowledge transfer from our experts to internal teams is an important goal and a prerequisite to ensure the long-term success of any privileged account security program. For example, the implementation services team will often coach a team on how and when to on-board additional accounts. CyberArk experts are fully engaged with an organization's technical leads during the entire engagement and assist in documentation.

Custom Extensions Development Services

While CyberArk supports most major systems and appliances out of the box, there are cases when an extension is needed to administer third party or in-house developed software. CyberArk's infrastructure can be extended using published APIs.

When needed, the CyberArk Security Services Extensions team can provide custom developed components and integrations for a broad range of needs including:

- Password management;
- Connectors for privileged session monitoring;
- Ticketing systems;
- Automation and custom integrations to simplify the on-boarding process.

> "We just completed the engagement and are extremely pleased. The consultant's experience made the process go smoothly and gave us great confidence – in fact, we can do the production upgrade remotely."
>
> – Project Manager, Leading Energy Company

CyberArk Onboarding Services

CyberArk Onboarding Services enable those customers with limited staffing to accelerate the onboarding of privileged accounts beyond those processed during the initial Implementation engagement. Onboarding services include:

- Expanding the number of privileged accounts covered and controlled through support for onboarding privileged credentials based on the previously established rollout plan and prioritization;
- Hands-on services for the operations and maintenance of CyberArk infrastructure during the engagement, including administration, monitoring and troubleshooting;
- Support for the new privileged account credential management and control based on the customer's previously established privileged account security controls and best practices.

To maximize efficiency and reduce the time needed to improve the security posture of the organization, CyberArk recommends that Implementation and Onboarding services be used in conjunction with CyberArk Consulting Services and CyberArk Program management Services.

CyberArk Program Management Services

CyberArk Program Management Services help maximize efficiency and accelerate deployment of the CyberArk Privileged Account Security Solution by bringing together people, processes, and technology with trusted expertise. The CyberArk Program Manager serves as a single point-of-contact to facilitate communications and effectively manage expectations throughout the project life-cycle. They provide streamlined access to specific CyberArk resources to maintain high quality execution, more rapidly resolve problems and avoid risks that may impact the project.

CyberArk Program Managers adhere to Project Management Institute's (PMI) methodology, using transparent metrics to track and communicate the project's scope and progress. The project manager works with all the resources involved to reduce risk and ensure on-time, on-budget delivery. Responsibilities include:

- Communication Management
- Scope Management
- Resources Management
- Cost Management
- Risk Management
- Quality Management
- Change Management
- In-Support Transition

CyberArk Red Team Services

CyberArk Red Team services are designed to provide a safe way for security operations teams to test their ability to effectively defend against cyber-attacks on their compute and development environments. The CyberArk Red Team specializes in adversary simulation, and by using a variety of tactics, techniques and procedures (TTPs), they have developed expertise to specifically exploit cloud and hybrid environments, as well as DevOps pipelines and processes.

A Red Team engagement can provide clients with an attacker's perspective and deep insight into the security strengths and weaknesses of their cloud and on-premises environments. It also provides a baseline from which future security improvements can be measured. Key benefits include:

- **Measuring the risk of critical assets.** Understand how easy or difficult it would be for an external or inside attacker to reach the organization's "crown jewels." Identify various critical pathways to those assets.
- **Uncovering unknown vulnerabilities and weaknesses.** Understand the potential business impact of unknown vulnerabilities, and use these insights to prioritize remediation efforts.
- **Identifying strengths and weaknesses.** Gain an objective assessment of team strengths and weaknesses, and identify specific competencies that can be improved over time.
- **Evaluating preparedness for cloud environments and DevOps pipelines.** Gain an objective assessment of overall strengths and weaknesses of newer areas, including multi cloud, and CI/CD pipelines, that have very different threat models.
- **Measuring improvement over time.** Measure the organization's baseline security posture and quantify improvements over time. Quantifiable results can be used to help build a business case for additional security projects.

"We now have our first significant group of administrators using CyberArk—this is a huge milestone for me. We have also demonstrated to leadership that the product works in our complex global environment. The next major milestone is to migrate thousands of Windows administrators and application support staff."

—Director Security Infrastructure, Global Financial Services

"The Advanced Course has been a very important course for me and takeaway apart from the technical knowledge is the way training should be run."

—Cybersecurity Consultant

"Excellent documentation, instructors with practical experience behind lessons."

—Identity and Access Engineer III

CyberArk Training and Certification

CyberArk provides security-conscious professionals and IT specialists with the education, training and skills validation needed to implement and administrate the CyberArk solutions. CyberArk provides a variety of learning environments including online, virtual classroom (VCT) or live face-to-face classes.

CyberArk offers both fundamental and advanced courses to ensure customers and partners are fully trained in CyberArk's products. All courses are designed to provide extensive hands-on experience and are available globally as classroom and online instructor led training, as well as self-paced computer based training.

To maximize the value of investment in CyberArk technology, project team members should take the relevant fundamental classes for broad training before project kickoff and proceed to more advanced classes once they have gained basic, working experience (for example, focus on specific configuration and relevant workflows training).

In addition to training, CyberArk Certification Program give organizations the confidence to position themselves as cyber-security experts as well as adopting CyberArk's innovative and industry-leading CyberArk Privileged Account Security Solution.

To achieve the different levels of CyberArk certification, candidates must successfully complete and pass specific qualifying exams that are based on CyberArk training materials, product documentation and real-life use cases. CyberArk certification options establish a benchmark for internal teams, providing additional assurance that they are prepared to operate and manage CyberArk solutions.

CyberArk Customer Support Services

Customer Support's top priority is to ensure an organization's deployment of the CyberArk Privileged Account Security Solution includes the latest security updates so that the program is positioned against the latest threats. Customer Support experts also help ensure privileged account security programs are running efficiently in order to advance the organization's security posture, enhance network infrastructure, and are capable of securing newer technologies and solutions.

CyberArk offers a range of customer support services through which organizations can leverage a global team of highly trained technical support engineers, support facilities, and knowledge bases, including access to CyberArk's 24/7 Technical Support. Efficient hands-on case resolution is complemented by online technical support resources that allow organizations to take a more self-directed approach. For example, the knowledge base and support portal enable logging and tracking service tickets, accessing the community portal, obtaining and searching documentation, as well as allowing secure access to updated product releases.

Local support phone numbers are offered across the globe to simplify access to CyberArk's highly trained support engineers. Additionally, email access to the support team, fully integrated with the support portal, gives customers multiple channels of convenient access to interact with CyberArk.

For More Information

- CyberArk Onboarding Programs
- CyberArk Red Team Services
- CyberArk Red Team – Cloud Security Services
- "The CISO View – Rapid Risk Reduction: A 30-Day Sprint To Protect Privileged Credentials", CyberArk