CYBERARK®

WHITE PAPER

CYBERARK BLUEPRINT FOR PRIVILEGED ACCESS MANAGEMENT RAPID RISK REDUCTION PLAYBOOK

Table of Contents

Summary

Privileged accounts are a common target for malicious attackers. Cybercriminals and other bad actors can exploit compromised privileged account credentials to steal confidential data and disrupt critical IT systems. Businesses must strengthen privileged access security to reduce risks, but implementing an effective privilege access management program—identifying weaknesses, evaluating potential exposure, introducing new security controls—can be a daunting proposition for many organizations.

CyberArk's Blueprint for Privileged Access Management Success is specifically designed to help businesses improve their security posture and mitigate risk in a methodical and efficient manner using field-proven measures. The CyberArk Blueprint Rapid Risk Reduction Playbook helps organizations quickly implement the most critical elements of the CyberArk Blueprint to rapidly strengthen security and reduce risk. This paper reviews the CyberArk Blueprint and explains how the Rapid Risk Reduction Playbook can help jumpstart your privileged access management implementation and accelerate risk reduction.

CyberArk Blueprint Helps Reduce Privileged Access Risks

Privileged access management is front and center for today's information technology and security leaders. External attackers and malicious insiders can gain unauthorized access to privileged accounts and traverse networks to steal confidential information, disrupt critical systems and applications, and impair business. Forrester estimates that at least 80% of data breaches have a connection to compromised privileged credentials.[1]

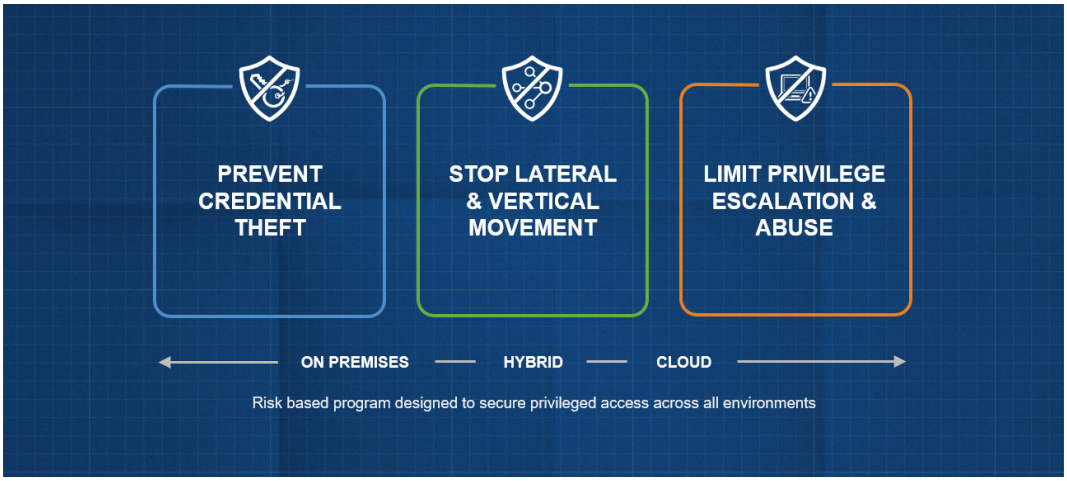
CyberArk has developed a prescriptive blueprint to help businesses establish and maintain an effective program to strengthen privileged access security. The CyberArk Blueprint for Privileged Access Management Success is designed to defend against three common moves every perpetrator makes to steal data and disrupt systems. This "thinking like an attacker" approach yields a prioritized, phased implementation plan that closely aligns actions with potential risk reduction.

While every organization's IT environment is unique, adversaries can attack virtually any business by: 1) gaining unauthorized access to privileged account credentials, 2) traversing the network looking for high-value targets, and 3) using elevated privileges to steal confidential information or disrupt services.

With that in mind, the CyberArk Blueprint is based on three guiding principles:

1. Prevent credential theft
2. Stop lateral and vertical movement
3. Limit privilege escalation and abuse

[1] The Forrester Wave™: Privileged Identity Management, Q4 2018

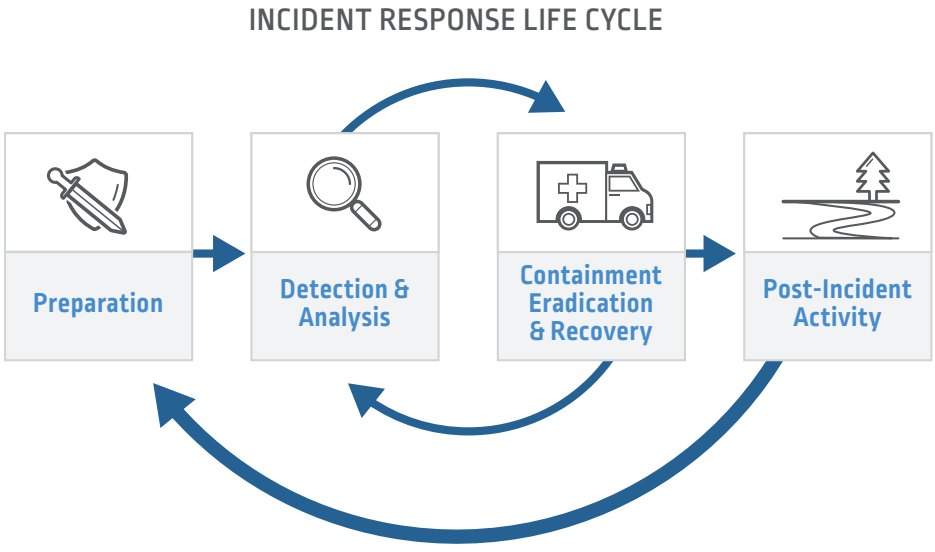


Three Guiding Principles of the CyberArk Blueprint

CyberArk Blueprint Rapid Risk Reduction Playbook Targets Greatest Risk

The CyberArk Blueprint Rapid Risk Reduction Playbook focuses on the highest-priority elements of the CyberArk Blueprint for Privileged Access Management Success plan, helping you address the most urgent requirements in the shortest possible time. Later on, you can implement more elements of the CyberArk Blueprint for less-urgent use cases.

The Playbook adheres to incident response best practices recommended by leading authorities such as the U.S. National Institute of Standards and Technology in the NIST Computer Security Incident Handling Guide, the European Union Agency for Network and Information Security in the ENISA Good Practice for Incident Management publication, and the Australian Cyber Security Centre in the ACSC Strategies to Mitigate Cyber Security Incidents. For example, the Playbook addresses the preparation; detection & analysis; and containment, eradication & recovery phases of the NIST incident response life cycle, as shown below.



Source: NIST Special Publication 800-61 Revision 2

The Playbook helps you improve preparedness by proactively securing access to the most frequently targeted privileged accounts. And it helps you identify compromised accounts, isolate attackers and establish corrective measures by analyzing privileged session activity. For example, say a privileged account was used to initiate an attack. If the compromised account was vaulted, you could determine who had access to the account and which systems they accessed, and use that information to potentially mitigate the attack. If the account was not vaulted, you could examine similar accounts throughout the enterprise to detect and isolate potential breaches. You could also expand the scope of your privileged access security plan to cover the at-risk accounts.

The Playbook helps you address the containment, eradication, and recovery phases of the incident response life cycle. Once compromised accounts and/or privileges have been identified, they can be vaulted with one-time passwords and exclusive account options. This prevents the credentials from being used to further the attacker's objectives.

You can also address the containment, eradication, and recovery phases of the incident response life cycle by removing components the attackers used during the incident. For instance, you could disable or delete breached accounts, introduce proxy-based access to critical systems and expand privileged account monitoring across the enterprise.

The CyberArk Blueprint defines a five-stage, prioritized privileged access management program framework that aligns program milestones with risk reduction potential. The Playbook focuses on the first three stages of the blueprint, honing in on the most frequently targeted accounts, which represent the greatest potential risk, as highlighted in the table below. The Playbook adheres to the blueprint's guiding principles, helping prevent credential theft, stop lateral and vertical movement, and limit privilege escalation.

CyberArk Blueprint Stages 1-3 with Playbook Objectives Highlighted

		PAM CONTROLS & TECHNOLOGIES		
	GOAL	Foundational Privileged Access Management	Least Privilege	App Secrets Management
STAGE 1	Secure privileged IDs with the potential to control an entire environment	IaaS admins, Domain admins, VM & hypervisor, Windows Server local, MFA		3rd Party Security Tools such as vulnerability scanners (via C3 integrations)
STAGE 2	Focus on locking down the most universal technology platforms	CI/CD consoles Workstation Local Admin, Privileged AD users, *NIX root		3rd Party Business Tools such as with Robotic Process Automation platforms (via C3 integrations)
STAGE 3	Build privileged access security into the fabric of enterprise security strategy and application pipelines	Cred boundaries, *NIX root similar, 3rd Party Vendors, out-of-band access, database built-in admins	IT admin workstations	Dynamic Apps

The Playbook is intended to implement the most-critical security controls as quickly as possible. Many organizations execute the Playbook in 30 to 60 days. Some take longer. In practice, the Playbook duration is dependent upon an organization's size, complexity, maturity, culture, and sense of urgency. In the aftermath of a breach, or in other instances when business leaders have an urgent desire to strengthen security, corporate politics are often set aside, bureaucracy is often overturned, and companies are often able to accelerate security initiatives and some of the later-stage Blueprint recommendations can be pulled into the Playbook objectives.

Stage One of the Playbook – Secure High-Value Targets

In the first stage of the Playbook, focus on securing high-value targets that represent the greatest potential risk to the business. Identify and secure any privileged accounts that can be exploited to control an entire environment, such as domain admin and IaaS admin accounts. Prevent unauthorized access and reduce risk by isolating privileged sessions, vaulting and rotating passwords, employing multifactor authentication, and intelligently monitoring and analyzing privileged session activity. Stop lateral and vertical movement by vaulting and rotating passwords and isolating Windows Server local admin accounts in both on-premises and cloud environments.

Stage Two of the Playbook – Lock Down Most Common Technology Platforms

In stage two, lock down the most commonly deployed technology platforms. Secure privileged on-premises, cloud-hosted and cloud-federated Active Directory accounts used to administer servers and workstations by vaulting and rotating passwords, and by isolating privileged sessions.

Stage Three of the Playbook – Incorporate PAM into Enterprise Security Strategy

In stage three, reduce privilege escalation risks by implementing OS-level least-privileged access controls for workstations, laptops, desktops, and virtual desktop instances (VDIs). Endpoint privilege management solutions help you limit exposure by removing local administrative rights from endpoints and tightly controlling user and application permissions based on policy. By enforcing the principle of least privilege—granting users the minimum set of privileges required to perform their jobs—you can prevent vertical movement and improve your security posture. And by instituting application controls—preventing ransomware and other malware, and restricting the operation of unsanctioned applications—you can reduce risk and uncertainty.

Ensuring a Successful Outcome

Implementing a comprehensive, enterprise-wide privileged access management program is a process, not an event. The Playbook is a critical first step in your overall privileged access security journey. To ensure a successful outcome you must properly prepare for the Rapid Risk Reduction initiative and you must continuously extend the breadth and depth of your defenses after the Playbook is executed.

Also keep in mind the CyberArk Blueprint is structured to defend against the most common threats posing the highest risk to the business. Every customer's situation is unique. If you are executing the Playbook in response to a cyberattack, you may need to adjust priorities and re sequence tasks to address your specific circumstances. For example, if you detect the privileged credentials on a universal technology platform (e.g. a local admin account on a workstation) have been compromised such as, you may need to isolate, vault and rotate those credentials while applying the principle of least privilege across all local admin workstations.

Over time you'll need to fully implement all five stages of the CyberArk Blueprint for ultimate security.

Before the Playbook is Executed

Before carrying out the Playbook, do some upfront planning to identify stakeholders, project team members, and the hardware and software resources you'll need for the program. Create a project plan defining the specific privileged access security controls and technologies you plan to implement. Define success criteria and the tools and methods you will use to evaluate progress and measure success.

At the Conclusion of the Playbook

Conduct a postmortem after the Playbook has been executed. Identify what went well and what processes need to be improved going forward. Use lessons learned from the effort to establish ongoing privileged access security systems and practices. Develop a formal plan to carry out regular privileged access security enhancements to improve the depth and breadth of your defenses.

Prepare a concluding report for executives and business leaders explaining how the Playbook will help the company improve cybersecurity and reduce risk. Describe additional steps and investments required to further bolster security. Present risk in meaningful, relatable terms like business downtime, lost revenue, or regulatory penalties.

After the Playbook

CyberArk customers are also encouraged to arrange a Blueprint session to get additional support in designing and structuring a roadmap to extend privileged access controls across the organization. Now that the most critical and time-sensitive aspects of the Blueprint framework have been addressed, you can expand the scope of your privileged access security plan. Start by implementing the outstanding controls and technologies from Blueprint stages 1 – 3, as highlighted in the table below. Continue to strengthen your security posture over time by instituting stages 4 and 5 of the framework as shown below.

Continuously assess the effectiveness of your cybersecurity plan and make adjustments as needed. Execute penetration tests or carry out red team-blue team exercises to test defenses. Use network scanning tools to identify weaknesses and improve your security posture. Revise the plan and reprioritize security measures when appropriate.

Post-Playbook Activities

		PAM CONTROLS & TECHNOLOGIES		
	GOAL	Foundational Privileged Access Management	Least Privilege	App Secrets Management
STAGE 1	Secure privileged IDs with the potential to control an entire environment	IaaS admins, Domain admins, VM & hypervisor, Windows Server local, MFA		3rd Party Security Tools such as vulnerability scanners (via C3 integrations)
STAGE 2	Focus on locking down the most universal technology platforms	CI/CD consoles Workstation Local Admin, Privileged AD users, *NIX root		3rd Party Business Tools such as with Robotic Process Automation platforms (via C3 integrations)
STAGE 3	Build privileged access security into the fabric of enterprise security strategy and application pipelines	Cred boundaries, *NIX root similar, 3rd Party Vendors, out-of-band access, database built-in admins	IT admin workstations	Dynamic Apps
STAGE 4	Mature existing controls and expand into advanced privileged access security	Web Apps (Top), Business Apps (Top), Network & Infra Admins, Named DBA	Windows Servers, All Workstations	Static Apps
STAGE 5	Look for new opportunities to shore up privileged access across the enterprise	Web Apps (All), Business Apps (All), Mainframe Admins, Windows Services	Windows Servers, *NIX Servers	Static Apps (Adv)

Conclusion

Malicious insiders and external attackers can exploit privileged accounts to steal confidential data or disrupt critical applications. The CyberArk Blueprint Rapid Risk Reduction Playbook helps you identify and mitigate the privileged access security liabilities posing the greatest potential risk to your organization as rapidly as possible. Following the recommendations and guidelines of the CyberArk Blueprint, the Playbook can help you rapidly mitigate a malicious attack, data breach, or other urgent security incidents.

Why CyberArk?

The CyberArk Blueprint reflects the combined knowledge and experience of CyberArk's global Sales, Sales Engineering, Security Services and Customer Success organizations. As the undisputed leader in privileged access management, CyberArk is uniquely positioned to deliver a thorough and effective privileged access management blueprint:

- CyberArk solutions are trusted by 5,000+ customers, including more than 50% of the Fortune 500, across a wide range of industries including financial services, insurance, manufacturing, healthcare, and tech.

- CyberArk's Incident Response and Red Team have been front and center in helping companies recover from some of the largest breaches of the 21st century. And CyberArk offers the industry's only Threat Research and Innovation Lab.
- CyberArk Security Services, Customer Success, and PAS Program Office organizations have decades of real-world implementation and support experience, and have a detailed, first-hand understanding of privileged access management risks and best practices.
- Leading research and advisory firms recognize CyberArk as a privileged access management leader for both completeness of vision and ability to execute.

About CyberArk

CyberArk is the global leader in privileged access security, 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 500, to protect against external attackers and malicious insiders. A global company, CyberArk is headquartered in Petach Tikva, Israel, with U.S. headquarters located in Newton, Mass. The company also has offices throughout the Americas, EMEA, Asia Pacific and Japan.

To learn more about CyberArk, please visit www.cyberark.com.