CYBERARK®

WHITE PAPER

CYBERARK BLUEPRINT FOR PRIVILEGED ACCESS MANAGEMENT SUCCESS

Table of Contents

Summary

Privileged access management (PAM) is top of mind for today's security and IT leaders. External attackers and malicious insiders routinely exploit privileged accounts to steal confidential information or disrupt business-critical applications and services. Businesses must strengthen privileged access security, but implementing an effective privileged access management program is a challenge for many organizations as the privileged threat landscape is large, complex and continuously evolving.

CyberArk has developed a comprehensive blueprint to help organizations assess and prioritize privileged access vulnerabilities, strengthen security and reduce risks. Leveraging CyberArk's vast experience and deep subject-matter expertise, the CyberArk Blueprint for Privileged Access Management Success lays out a prescriptive, risk-aligned plan for establishing and maintaining an effective privileged access management program.

This paper reviews common privileged access management challenges and explains how the CyberArk Blueprint can help organizations improve privileged access management systems and practices, reduce security vulnerabilities and mitigate risk.

Introduction – Privileged Accounts Pose Significant Security Risks

Privileged accounts represent one of the largest security vulnerabilities any organization faces today. When employed properly, privileged accounts are used to maintain systems, facilitate automated processes, safeguard sensitive information and ensure business continuity. In the wrong hands, these accounts can be used to steal confidential data and cause irreparable damage to the business. Forrester estimates that at least 80% of data breaches have a connection to compromised privileged account credentials.[1]

Privileged access management is fundamental to cybersecurity. Gartner and other industry analysts identify privileged access management as a top priority for security and risk management leaders.[2] Information technology and security organizations must tightly control access to privileged accounts, credentials and secrets to minimize vulnerabilities and reduce risk. Formulating, executing and maintaining an effective privileged access management program can be a complicated undertaking.

- **Privileged accounts are ubiquitous.** They exist in systems, databases and applications; they reside on-premises and in the cloud; and they are used by people as well as by applications, automated processes, machines and bots. Organizations must track and secure hundreds or thousands of privileged accounts scattered across the distributed environments. Digital transformation is changing the enterprise. More organizations are undergoing digital transformation projects such as adopting the cloud, migrating to SaaS, leveraging DevOps and automating with DevOps. Organizations must continuously adapt their privileged access management systems and practices to keep pace with innovation.
- **The threat landscape is constantly changing.** Attackers continually hone their skills, finding new ways to penetrate networks and avoid detection. Organizations must continuously evolve their privileged access management programs to stay one step ahead of the bad actors.

IT and security teams can overcome these challenges and minimize privileged access risks by:

- Taking a close look at how attackers exploit privileged access. What are the most common privileged access attack vectors? How does the perpetrator think and behave in each case?
- Taking a practical, phased approach to privileged access management. Identifying the most-critical privileged accounts, credentials and secrets. Zeroing in on accounts that could jeopardize mission-critical infrastructure or expose confidential data.

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

[2] Gartner, Smarter with Gartner, Gartner Top 10 Security Projects for 2019, June 18, 2019

- Developing a prioritized plan to reduce vulnerabilities and strengthen security. Which actions are most important? Which items can be achieved quickly and with minimal resources? Which require significant time and effort?
- Continuously reassessing and improving the privileged access management plan to address evolving threats and new technologies.

CyberArk Blueprint Helps Reduce Privileged Access Risks

CyberArk has developed a prescriptive blueprint to help organizations establish and evolve an effective privileged access management program. The CyberArk Blueprint for Privileged Access Management Success (or CyberArk Blueprint for short) is designed to defend against three common attack chain stages used to steal data and wreak havoc. Simple, yet comprehensive, the CyberArk Blueprint provides a prioritized, phased security framework that closely aligns privileged access management initiatives with potential risk reduction, helping organizations address their greatest liabilities as quickly as possible.

The CyberArk Blueprint was built with contemporary organizations and extensibility in mind. It prescribes privileged access management controls and best practices for organizations using conventional on-premises infrastructure and software development methods, as well as for organizations embarking on digital transformation projects such as migrating infrastructure to the cloud, adopting CI/CD practices, optimizing processes through robotic process automation or implementing SaaS solutions for business-critical applications.

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. Additionally, CyberArk draws on the insights of its Threat Research and Innovation Lab.
- CyberArk Security Services and Customer Success 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.[3]

Three Guiding Principles for Privileged Access Management Success

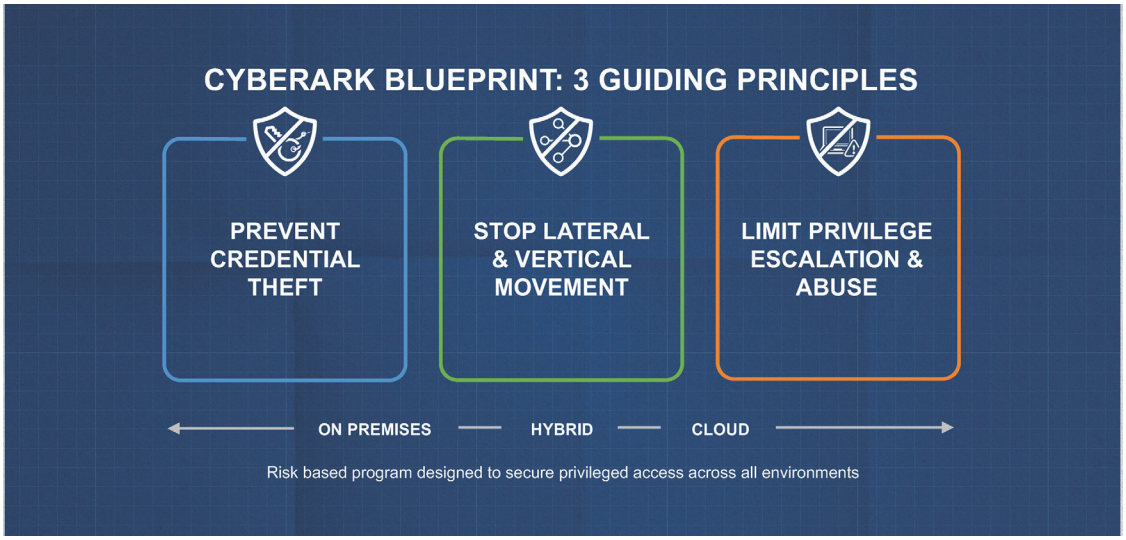
While every organization's IT environment is unique, perpetrators can attack virtually any business by following well established steps in the attack chain: 1) gain unauthorized access to privileged account credentials, 2) traverse the network looking for high-value targets, and 3) use elevated privileges to steal confidential information or disrupt services. The CyberArk Blueprint helps organizations strengthen their security posture by thinking like an attacker and defending against the three techniques adversaries typically use to access privileged accounts, steal data and take down systems.

More specifically, the CyberArk Blueprint for Privileged Access Management Success is based on three guiding principles:

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

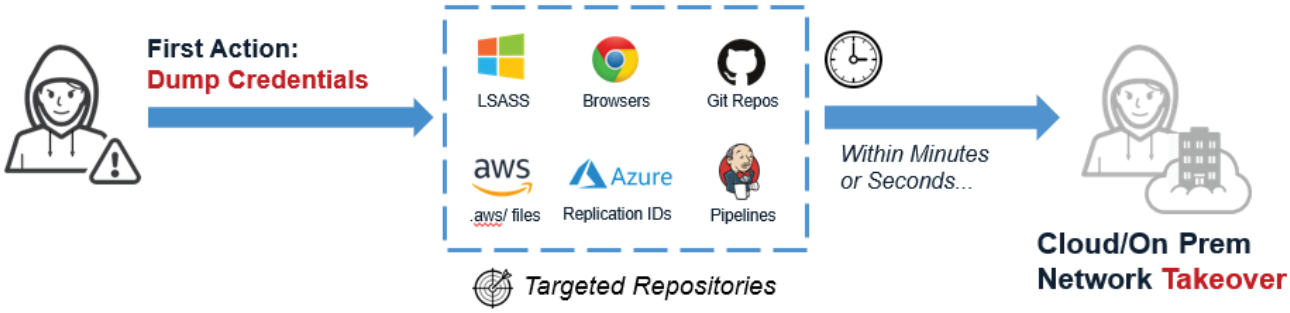
[3] Magic Quadrant for Privileged Access Management, Gartner, 2018

The Blueprint is designed to protect any customer environment, strengthening privileged access security for on-premises, cloud or hybrid infrastructure. It lays out a pragmatic, risk-based implementation plan that introduces security controls in stages, helping businesses address their most pressing needs in the short-term, while providing a long-term plan to address the more advanced security use cases.



Guiding Principle One: Prevent Credential Theft

Many organizations rely on inefficient manual processes to assign and track privileged account credentials. Passwords and keys sometimes remain unchanged for months or even years after they are issued. Former employees, contractors and business partners often maintain access to critical applications and systems long after termination, exposing the business to data breaches and malicious attacks. Disgruntled employees or external attackers can exploit dormant accounts or stale passwords to mount sophisticated attacks.



Adversaries Steal Credentials to Mount Attacks

In addition, attackers can obtain non-human credentials (secrets used by applications, machines, bots, etc.) from public source-code repositories like GitHub (developers often hard-code secrets into applications and scripts in clear text), from credential files used for cloud services like AWS and from configuration or pipeline files used by CI/CD platforms like Jenkins or Ansible.

Once a savvy attacker gains access to privileged account credentials they can breach other critical enterprise resources in just minutes. CyberArk security professionals have seen adversaries go from penetrating a workstation to gaining full domain admin rights on a domain controller in less than 20 minutes!

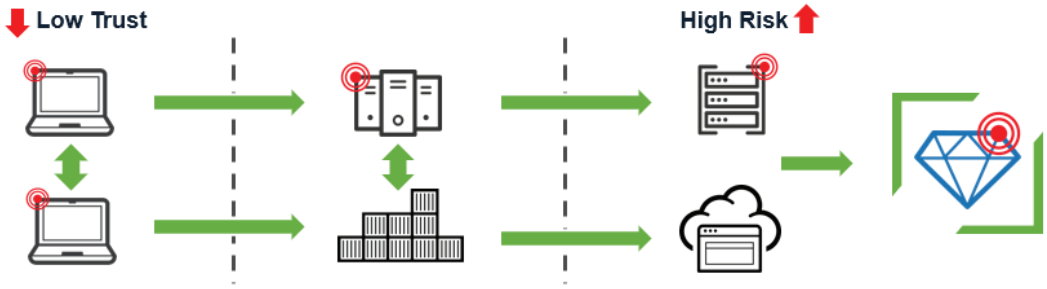
To prevent credential theft, CyberArk recommends organizations:

1. **Discontinue disjointed, manual credential and secrets management processes.** Introduce a hardened and secure digital vault to centrally store and track privileged account credentials. Automatically rotate passwords and keys based on policies.
2. **Isolate privileged sessions.** Use a secure proxy server to decouple endpoints from target systems, segregate privileged session traffic and avoid transmitting credentials and revealing them to end users. With this approach, users authenticate to the proxy server and then gain privileged access to target systems via a separate session.
3. **Remove hard-coded credentials from applications, robotic process automation platforms, CI/CD tools and other non-human entities.** Introduce a centralized, automated application access management solution to keep secrets out of repositories, source code and hard drives. With this approach, authorized applications automatically retrieve secrets from the secure digital vault in real-time.
4. **For an additional layer of protection, implement credential theft blocking controls directly at the OS level.** Actively monitor common credential stores such as the LSASS process, browser caches, remoting tools like WinSCP or VNC, service accounts, and SAML key repositories. Proactively block unauthorized access to these repositories. Cutting off access to these well-known credential sources makes it more difficult for attackers to make headway.

Guiding Principle Two: Stop Lateral and Vertical Movement

With credentials in hand, an adversary will often pivot from lower-value systems to higher-value targets that contain sensitive information or can be used to control an environment. This can take two forms:

1. Moving laterally within the same "risk tier" in the hopes of finding better, more useful credentials, or
2. Moving vertically from one risk tier to another (move from workstations to servers for example) to get ever closer to the "crown jewels."



Adversaries use Stolen Credentials to Move Laterally or Vertically

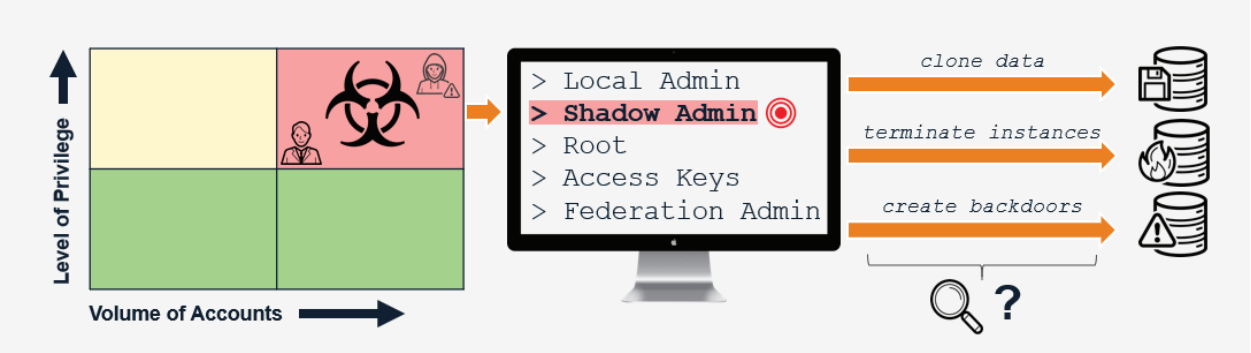
To prevent lateral or vertical movement, CyberArk recommends organizations:

1. **Use credential boundaries with session isolation to limit an attacker's range of motion.** For example, don't grant a single-domain account access. Instead split up access, using distinct accounts for datacenter administration and server administration.

2. **Rotate and randomize credentials to stop lateral and vertical movement.** Rotating credentials limits an attacker's window of opportunity. While eliminating shared common credentials across endpoints prevents traversal.
3. **Move to a *Zero Trust* model.** Enable just-in-time privilege elevation, allowing users to access privileged accounts or run privileged commands on a temporary, as needed basis, only when required.

Guiding Principle Three: Limit Privilege Escalation and Abuse

Privileged accounts are pervasive. Every host, application, database and platform has its own built-in administrative credentials. Many organizations administer privileged credentials manually and have limited visibility and control over privileged session activity. And to make matters worse, many organizations over-privilege end-users and application processes, granting them full admin rights, regardless of their actual requirements. The proliferation of privileged accounts, and lack of administrative visibility and control create a wide attack surface for malicious insiders and external attackers to exploit.



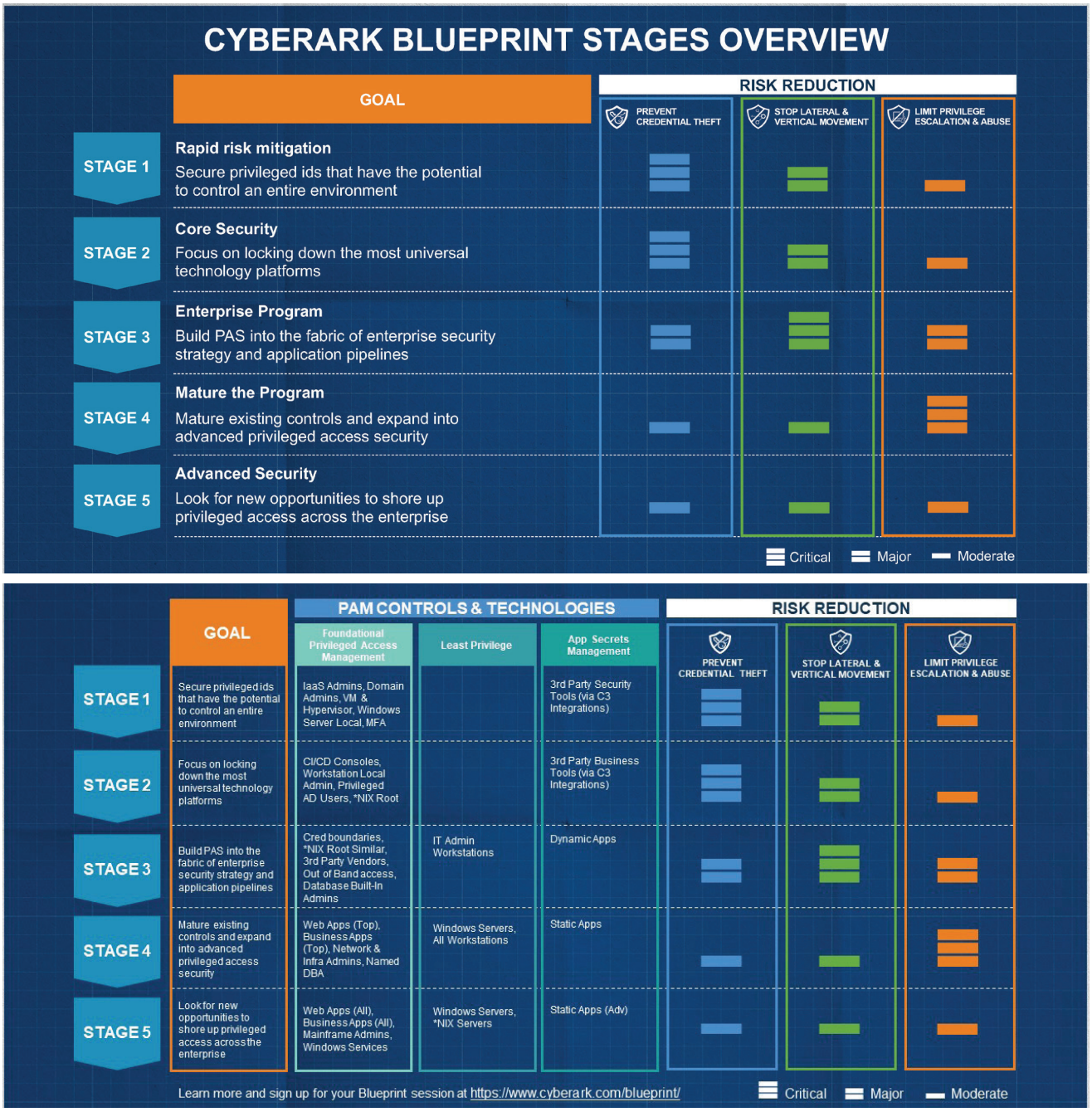
High Volumes of Privileged Accounts Create Large Attack Surfaces for Adversaries

To limit privilege escalation and abuse, CyberArk recommends:

1. Embrace the principle of least privilege to reduce attack surfaces and contain bad actors. Implement least-privileged access controls at the OS level in the most widely deployed platforms: Windows, Unix and Mac endpoints. Introduce just-in-time security controls, granting users access to specific systems, applications or functions for finite periods of time, on an as-needed basis.
2. Use a privileged threat analytics solution to automatically analyze privileged session activity, identify suspicious actions and detect in-progress attacks. Analytics solutions collect and analyze data from multiple sources, using advanced algorithms to intelligently establish baselines, evaluate threats and assess risks.
3. Privileged threat analytics solutions provide alert notifications of attacks and data breaches, assigning a risk score to each incident. Best-of-breed solutions automatically respond to high-severity incidents taking remedial actions to thwart in-progress attacks.

Phased Implementation Plan Aligns Prescriptive Actions with Risk Reduction

CyberArk recommends a phased privileged access management implementation plan that aligns program milestones with risk reduction potential, and aligns cybersecurity investments with benefits. Each stage of the implementation plan is formulated with the three guiding principles in mind. The prioritized plan targets the threats that pose the greatest potential risk in the preliminary stages, while shoring up other vulnerabilities over time. Stages one and two have a major impact on credential theft risk, stage three has a major impact on lateral and vertical movement risk, stage four has a major impact on privilege escalation and abuse risk and stage five is all about mitigating any remaining vulnerability.



Phased Plan Aligns Prescriptive Actions with Rapid Risk Mitigation

Stage One – Rapid Risk Mitigation

In the first stage of the plan, secure 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 system admin, domain admin and IaaS admin accounts. Prevent unauthorized access and reduce risk by isolating privileged sessions, rotating passwords, employing multifactor authentication and intelligently monitoring and analyzing privileged session activity.

Stage Two – Lock Down Most Common Technology Platforms

In stage two, lock down the most commonly deployed technology platforms. Secure privileged access to CI/CD platforms (consoles and CLIs) and robotic process automation platforms. Secure workstation local admin accounts, server admin accounts, and *NIX root account IDs, passwords and SSH keys.

Stage Three – Incorporate PAM into Enterprise Security Strategy

In stage three, incorporate privileged access management solutions and best practices into the overall enterprise security strategy and throughout application pipelines to reduce the risks associated with lateral and vertical movement. Implement credential boundaries for Active Directory, and ideally for federated access as well. Remove hard-coded secrets from dynamic applications (e.g. containerized apps, microservices) to prevent credential theft. Secure root-similar accounts on *NIX systems, and secure default built-in database admin accounts. Implement OS-level least privileged access controls for IT admin workstations. Introduce a just-in-time authentication and authorization solution to give remote third-party IT service organizations temporary, secure privileged access without requiring VPNs or special-purpose agent software.

Stage Four – Maturing the Program

In stage four, further strengthen the organization's security posture by expanding privileged access management depth and breadth. Go deeper by removing hard-coded credentials from static applications (e.g. legacy client/server applications). Secure named database admin accounts. Implement OS-level least privileged access controls on additional endpoints—Windows servers, Windows desktops, Macs.

Go wider by extending privileged access management to other IT infrastructure such as switches, routers and storage arrays. Implement privileged access controls for business applications and web apps with the greatest risk potential such as CRM and ERP solutions.

Stage Five – Shore up Remaining Vulnerabilities

In stage five, shore up any remaining vulnerabilities. Implement privileged access controls for all remaining business applications and web apps. Extend privileged access management to legacy mainframe systems and applications. Secure any remaining *NIX or Windows server privileged accounts.

Introduce advanced security practices. Automatically rotate credentials used in embedded OS services such as Windows Services, Scheduled Tasks or COM Objects. Ensure applications are strongly authenticated using multiple attributes when requesting secrets. Or move to a Zero Trust model with just-in-time elevation for privileged access.

Apply least privilege controls to all Windows and *NIX servers. Deny access to all applications and services by default. Use whitelisting to selectively grant access to specific applications and services on a case-by-case basis.

Conclusion

Malicious insiders and external attackers can exploit privileged accounts to steal confidential data or disrupt critical applications. The CyberArk Blueprint helps organizations formulate and maintain an effective risk-based privileged access management program that takes full advantage of CyberArk's vast knowledge and expertise. Designed to defend against the three most common attack scenarios, the CyberArk Blueprint provides a prioritized framework that closely aligns prescriptive actions with risk reduction, helping organizations address the vulnerabilities that pose the greatest potential threat, as quickly as possible.

By following the recommendations and guidelines laid out in the CyberArk Blueprint organizations can strengthen their security posture, reduce risks and make the most of their privileged access management technology investments.

Next Steps

Developing and executing an effective privileged access management program can be a complex undertaking. CyberArk has the experience, solutions and security services to help you succeed.

To begin your Blueprint journey, visit www.cyberark.com/blueprint and sign up for a Blueprint session to learn about how Blueprint can help you achieve PAM success!

Once you have completed a Blueprint session and have a roadmap, CyberArk and our partners offer a wide range of professional services to help you with every facet of your privileged access management program. For more information on the CyberArk Security Services PAM Program Development Package visit www.cyberark.com/blueprint. The package includes a focused approach based on the CyberArk Blueprint and helps you set and meet goals to achieve the highest level of protection against the most common attacks on privileged accounts, credentials and secrets.

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. 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.


CYBERARK®