EBOOK

BUYER'S GUIDE TO SECURING PRIVILEGED ACCESS

A MODERN BUSINESS PERSPECTIVE ON HOW TO EVALUATE ***PRIVILEGED ACCESS MANAGEMENT SOLUTIONS*** ▶

CYBERARK®

TABLE OF CONTENTS

INTRODUCTION

Identity Security for the modern enterprise is more critical than ever before.

Current events highlight increasing cyber attacks by hackers who want to steal your data. They'll keep the data if they find it's valuable for their own purposes or ransom the data if it's more important to the victim. In case after case, through random or targeted strikes, compromised identities and the manipulation of privileged access have become the key elements of modern attacks.

This isn't new; identity and access management issues fill the pages of history and mythology. Yet, the modern business is diverse and complex — especially as it increasingly depends on Software-as-a-Service (SaaS) applications and other cloud-based virtual infrastructures. Many businesses use a hybrid approach that combines on-premises and remote solutions. Yet, adapting isn't just a matter of moving technology from "here" to "there." Most businesses still retain a significant amount of traditional maintenance needs that must co-exist with the new infrastructure — all of which requires a secure and flexible approach to identity security.

Privileged access is the gateway to an organization's most valuable assets, and that gateway is a factor in nearly every major security breach. You need an effective solution for securing enterprise identities, protecting credentials and secrets, and managing privileged access. This guide highlights key requirements to help a business select a partner and accomplish this critical need. Use the questions in this guide and build your strategic plan to manage, access, monitor transactions and mitigate threats swiftly and effectively.

Percentage of Organizations Comprised by At Least One Successful Attack

Management of privileged identities, credentials and secrets has been a challenge since the dawn of history yet has never been more important. A record 86% of organizations reported suffering from a successful cyber attack in 2020, and the trend continues to increase.

Source: 2021 Cyberthreat Defense Report, CyberEdge Group

1 SUPPORT A HYBRID INFRASTRUCTURE

Until recently, many enterprises either had in-house infrastructure or relied upon an external solution. As cloud offerings have become more pervasive, businesses need both types of infrastructure to coexist within the enterprise architecture. It's challenging to maintain identities and access control across such a diverse environment. There is risk in not supporting both traditional and modern identity security. Without an integrated and cohesive solution, customer needs could go unfulfilled, hackers could exploit a technical gap or critical services could be unsupported.

An infrastructure's purpose is to drive value for the business — your information and technology enable innovation, support current and prospective clients, and ensure customer success. Your Identity Security solution must enable secure and reliable management for a full range of work roles throughout the enterprise. Of course, that includes traditional network and system administrators but also the sales manager controlling access to confidential and privileged customer relationship management (CRM) information, a researcher developing your next groundbreaking invention and human resource professionals ensuring your employees' safety and privacy.

The right privileged access management (PAM) solution enables an evolving set of hybrid technologies that drive operational efficiencies across all identities, infrastructure and applications for hybrid, multi-cloud and SaaS workloads — and does so cost-effectively.

Can your PAM solution …

- **… enable a unified, automated and risk-aware platform across all identities and applications?**
- **… seamlessly connect users to resources across on-premises, multi-cloud and SaaS workloads efficiently?**
- **… maximize your IT investment by enabling integration with existing applications and to a new, evolving infrastructure?**

2 SUPPORT DIVERSE TYPES OF TRANSACTIONS

Businesses are adapting the way they conduct operations, including software design and creation. The integration of development, security and operations (DevSecOps) is changing the model; where human administrators once manually processed access control steps, activities are now increasingly done by automated systems — often at network speeds.

Businesses also use robotic process automation (RPA) to extend the power of automation into new realms for enabling digital business. Applied to the right processes, software robots can improve productivity, quality and accuracy of data, and compliance with requirements. For example, RPA can manage an increasing suite of sensors, products and tools as part of the "Internet of Things." Yet, RPA is different than traditional business automation, and these differences introduce a growing challenge of securing the access and the protection of the credentials used by software robots. Managing that privileged access is critical to the scalability, efficient maintenance and the continued benefit afforded by software robots.

Your Identity Security solution must include an effective approach that integrates seamlessly with automation, scripts and workflow-oriented application program interfaces (APIs). These capabilities enable your enterprise to confidently take full advantage of the efficiency and productivity benefits automation technology offers without jeopardizing cybersecurity.

Can your PAM solution …

- … consistently manage the many embedded credentials among DevSecOps, cloud and traditional applications?
- … enable secure vaulting and management of privileged account credentials used by software robots and RPA administrators?
- … support automated application lifecycle management, ensuring immediate productivity and reducing IT delays?
- … enable just-in-time PAM through shared accounts and break glass approach?

3 PRIORITIZE THE USER'S EXPERIENCE

While robots may be doing many of the repetitive tasks, much of the work of the modern business is still performed by human beings who expect a flexible and intuitive user experience.

People are a critical part of securing the enterprise. Any procedure adding complexity or burden to privileged identity and access management brings additional risk, reduces productivity and impedes effectiveness. In contrast, the right solution increases user satisfaction and makes it easy for them to be secure, supporting the right balance of usability and risk management. The customer experience must be frictionless.

The right interface is one that maximizes self-service capability and seamlessly integrates into the existing technology stack. It also makes it easy for an increasingly remote workforce to be securely identified, authenticated and authorized as part of a cost-effective and efficient life cycle.

Can your PAM solution …

- ✓ **… strike the right balance between frictionless access and effective identity security?**
- ✓ **… monitor and secure remote access to maximize effectiveness while enforcing least privilege requirements?**
- ✓ **… support self-service capabilities and automated workflows to enable users to be efficient and productive?**

4 READY FOR TOMORROW'S CHALLENGES TODAY

While privileged identity management needs are not new, the environments being secured are continually changing. Capabilities that might have been considered science fiction only a few years ago are now commonplace. As technology evolves in new and exciting ways, to keep pace with these evolutionary realities you need an identity security partner that is continually innovating. A vendor with a product that only meets today's immediate needs — but that isn't already planning for tomorrow — may not be the most effective partner in the long run.

You are innovating, too, and doing so faster than ever. Today's agile and just-in-time development processes depend upon effective system integration and access. Without it, continuous integration and deployment pipelines shut down, resulting in delays or disruptions to critical business application and services for the business and its customers. Your PAM solution must be one that enables interoperability while securing your infrastructure.

Identity itself is evolving, too, as sensors and operational technology join microservices, software robots and virtual services. The best solution will ensure continued alignment with both the security needs and digital business opportunities of tomorrow.

Can your PAM solution …

- … show a proven track record of 20+ years aimed at continual innovation and technical advances?
- … demonstrate the business acumen for strategic acquisitions to address emerging threats and use cases?
- … point to $500 million worth of research and development to improve identity security solutions?
- … draw upon industry-leading threat researchers dedicated to examining emerging attack techniques to drive improvement for the security community?

5 DEFEND AGAINST ADVANCED AND EVOLVING THREATS

The right solution needs to stay a step ahead of the hackers. As cybercrime becomes more profitable and organized, your solution needs to help you stay informed and prepared. The U. S. National Security Agency recommends that you consciously operate and defend resources as if the adversary already has a presence within your environment. In this "assume breach" model, the right PAM solution must assume every transaction is untrusted and must apply the principle of least privilege practices through dynamic security policies.

Many solutions are built to protect inside information and thwart attackers on the outside. The reality is that there is no more "inside" and "outside." The PAM solution must originate with engineers and analysts who understand threat actors' tactics, techniques and procedures (TTPs), staying abreast of new methods that provide effective identity security and protect the avenues that an adversary would exploit.

The modern business needs a technically excellent suite of products backed by proven research into incident prevention, detection and response. As product engineers gain intelligence about hackers' tactics and methods, that understanding should be baked into the solution. That suite will also provide measurable risk reduction to demonstrate effective return on a solid product and service investment.

Can your PAM solution …

- … demonstrate success in thwarting over 3 million ransomware variants?
- … reduce cost and risk to your enterprise through a successful and continually improving identity security program framework?
- … enable a Zero Trust approach that leverages adaptive authentication and authorization, supported by a tamper-proof audit trail of all activity?

6 SUPPORT A BROAD ECOSYSTEM

An effective Identity Security solution should be able to demonstrate that it can draw upon an extensive portfolio of partnerships and alliances. Those relationships enable effective integration and cooperation that protect the business's investment in technology. Integration helps each component do what it does best, while ensuring that the whole system provides security in harmony.

Because identity is the thread that binds every facet of an enterprise's information and technology, the right solution can demonstrate the ability to interoperate with a broad array of applications, services and providers. As systems become increasingly interdependent and as a zero trust approach drives increased authentication needs, that integration becomes mission-critical.

Business leaders should be cautious of solutions that may initially seem less costly, yet don't provide sufficient integration or support alliances with other product offerings. Skimping on proven integration techniques or failing to take advantage of experienced service experts can result in stranded technologies and technical debt. A solution without effective integration can introduce system and security risk, add complexity and increase development costs.

Can your PAM solution …

- … demonstrate an alliance of certified, proven and supported bi-directional third-party integrations to ensure the value of your existing assets and services?
- … help your organization maximize the return on your investment in existing IT infrastructure?
- … support integration through an extensible platform for everything from homegrown applications to external services?
- … easily integrate via trusted industry standards and protocols like SAML, REST and OAUTH?

7 DEMONSTRATE PROVEN DEPENDABILITY

One of your business's most critical assets is your data, yet that data is likely spread across a wide area of in house, online and external partner systems. The right identity security solution needs to protect that data against threats to confidentiality, integrity and availability. The right identity security partner needs to be one with a proven track record for a visionary product approach, leading-edge customer service and stable corporate presence.

As requirements increase regarding privacy and security controls for customers and systems around the globe, regulators and auditors will expect to see an identity security solution that fulfills (or exceeds) data protection requirements. To protect your brand and reputation and to streamline reviews, select a product suite that is recognized by auditors as an effective and compliant methodology for protecting the information required by — and entrusted to — your business.

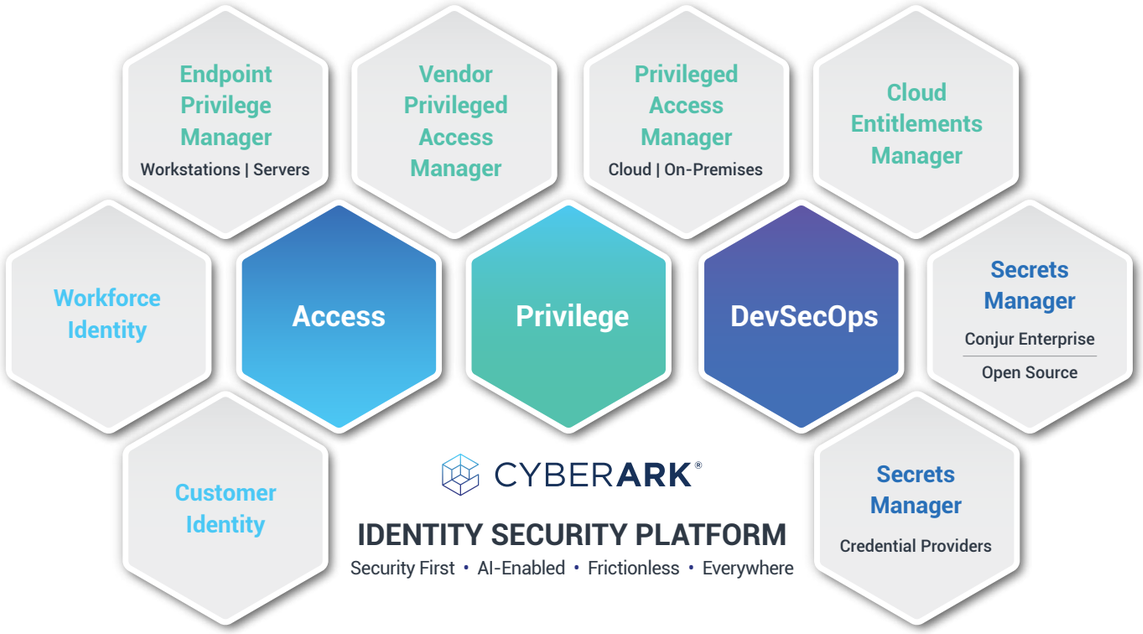
When you consider the importance of securing privileged access, the experience of your technology provider matters.

Can your PAM solution …

- … demonstrate 20+ years of trusted experience by nearly 7,000 customers, including more than half of the Fortune 500 enterprises?
- … proclaim itself as a leader for Privileged Access Management and winning cybersecurity vendor from multiple sources and well-respected analyst firms?
- … help you ensure conformance with customer expectations through tools and services that are recognized and trusted by regulators, auditors and authorizing officials?

CYBERARK IDENTITY SECURITY PLATFORM

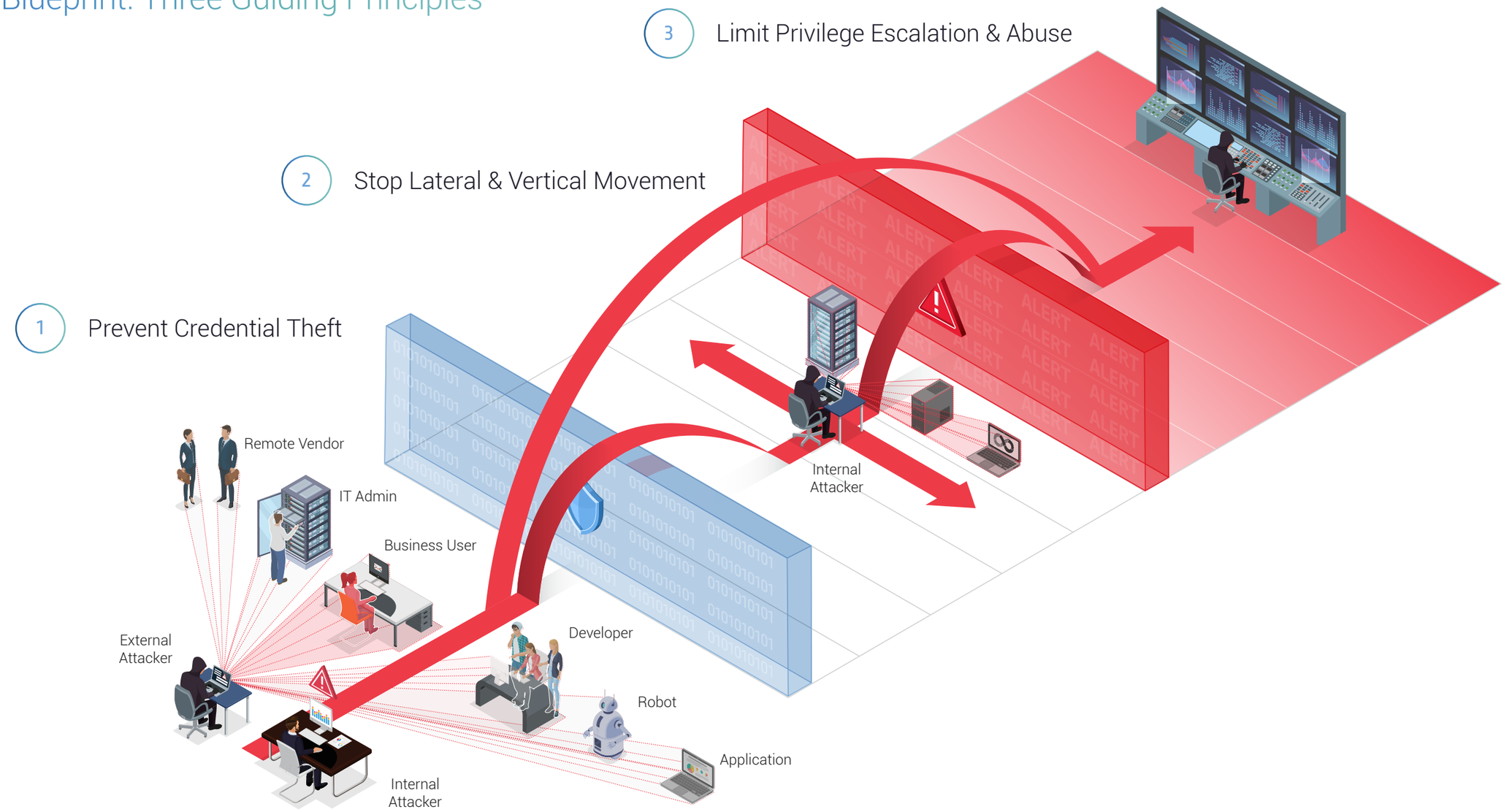
As business leaders and security managers of modern enterprises consider these practices, the CyberArk Identity Security Platform, based on the pillars of PAM, is the industry's most comprehensive, unified platform for securing human and machine identities. To manage reliable privileged access, secure DevOps environments and provide trustworthy access to business resources, CyberArk's products and services offer industry-recognized and customer-proven solutions. As companies continue to expand their footprints into hybrid on-premises and cloud-based solutions, including privilege management for SaaS offerings, they can rely on CyberArk as a stable and trusted partner.



CyberArk's Blueprint for Identity Security Success that includes PAM offers peace of mind that your most critical assets are secure while your business agility accelerates. The Blueprint is a vendor-agnostic framework for assessing your current strategy and defining a roadmap for success. The framework is both prescriptive and scalable, and provides a risk-based approach to prevent, stop and limit the common identity attack chain. Built upon decades of expertise in the people, process and technology domains that are critical to Identity Security success, the Blueprint is based on three critical principles:

1. Prevent credential theft, especially those identities that represent the "keys to the kingdom."
2. Stop hackers' (including unauthorized insiders) lateral and vertical movement in your infrastructure.
3. Limit privilege escalation and abuse that jeopardize your critical and sensitive information.

CyberArk Blueprint: Three Guiding Principles



CONCLUSION

The road to preventing cyber attacks on your valuable data has become critical to any modern enterprise. Protecting your credentials and secrets, and managing privileged access is a requirement as businesses evolve in this fast-paced world. Adopt a leading privileged access management solution to thwart major security breaches and reduce the risk of cyberthreats to any financial and reputational damage to your organization.

Are you ready to build your roadmap to PAM success? Visit **www.cyberark.com** to learn more and schedule your personalized demo today!

REQUEST A DEMO

CYBERARK IS THE GLOBAL LEADER IN IDENTITY SECURITY. CENTERED ON PRIVILEGED ACCESS MANAGEMENT, CYBERARK PROVIDES THE MOST COMPREHENSIVE SECURITY OFFERING FOR ANY IDENTITY – HUMAN OR MACHINE – ACROSS BUSINESS APPLICATIONS, DISTRIBUTED WORKFORCES, HYBRID CLOUD WORKLOADS AND THROUGHOUT THE DEVOPS LIFECYCLE. THE WORLD'S LEADING ORGANIZATIONS TRUST CYBERARK TO HELP SECURE THEIR MOST CRITICAL ASSETS.

U.S., 08.21 Doc. 202401

CYBERARK®