CYBERARK®
The Identity Security Company™

EBOOK

Reimagine Your Privileged Access Management Program

Improve PAM efficiency, adoption and coverage with intelligent privilege controls.

Table of Contents

Introduction

In today's increasingly complex IT landscape, trends like persistent cyber threats, cloud and IoT adoption and the emergence of generative AI have heightened the need for effective privileged access management (PAM) solutions. New attack methods continue to emerge in the ever-evolving threat landscape, making it imperative for businesses to keep up by thoroughly protecting the most commonly targeted credentials and identities.

Moreover, today's PAM programs face a vast and dynamic threat landscape, upended by innovation and reshaped by new identities and new environments. Over 90% of organizations experienced at least one identity-related incident in the past year, with notable recent breaches at Okta, LastPass, Microsoft and Uber all stemming from identity compromise attacks on support and software engineers not typically considered privileged users. The SolarWinds supply chain attack, for example, went undetected for nine months, impacting over 18,000 organizations across the world. Data breaches can damage a company's reputation, disrupt business and revenue, and result in confidential data loss and regulatory fines. It demonstrates why organizations must rethink their security systems and practices for the digital world.

According to the IBM 2024 X-Force Threat Intelligence Index Report, over 85% of attacks on critical sectors, compromised could have been mitigated with patching, multi-factor authentication, or least-privilege principles.

As privileged access evolves and continues to be targeted, there is a need to embrace a defense-in-depth strategy for identities with high-risk that haven't always been secured by PAM programs, such as third-party vendors, developers and cloud operations teams. Similarly, as technology keeps evolving, PAM continues to be a critical component of any cybersecurity strategy and fundamental for on-premises, hybrid and cloud environments.

This eBook will provide you with key insights into the following:

1. Understand the importance of PAM for your cloud and SaaS environments.
2. Map new, cloud-first use cases and best practices for PAM programs.
3. Determine how CyberArk PAM solutions can help secure high-risk access.

71%

Year-over-year increase in cyberattacks that used stolen or compromised credentials.

Source: IBM, 2024 X-Force Threat Intelligence Index,2024

Why It's Time to Reimagine PAM for Your Dynamic Cloud and SaaS Environments

Today nearly all organizations develop and deploy applications in the cloud. As organizations increasingly rely on the cloud's operational benefits, securing administrative access across hybrid and multi-cloud IT grows in complexity. As IT evolves, organizations must holistically protect both system and operational access. According to the CyberArk 2023 Identity Security Threat Landscape Report, **77%** of respondents say developers have too many privileges — making these identities highly attractive targets. High-risk access for third-party vendors is another challenge. Without consistent visibility and control, external privileged access exposes organizations to additional risks of breaches, failed audits or cyber insurance premium rate increases. As a result, maintaining separate solutions for different environments creates overhead, inefficiency and limited visibility across systems.

Simultaneously, failing to implement a proper identity security posture can lead to failed audits or non-compliance, resulting in financial penalties, business delays and erosion of stakeholder trust. Regulatory non-compliance increased the average cost of a data breach by **$218,915** to a total of **$4.67** million in 2023[1].

Secure administrative access to infrastructure across all environments:

- Windows and Linux servers, databases
- SaaS apps
- Elastic VM, database and Kubernetes workloads
- Cloud-native service

Extend to secrets management:

- Secure, rotate and deliver credentials used by service accounts.
- Eliminate hardcoded passwords in scripts and automation tools.

Extend controls to third-party vendors:

- Provision external access just-in-time without VPNs, passwords, agents, or corporate devices.
- Securely provide offline access to credentials in air-gapped environments.
- Maintain central control of session isolation, monitoring, and recording.

Deliver PAM controls to:

- Secure machine accounts used by the IT organization.
- Eliminate hard-coded passwords to extend maintenance scripts and automation tools.

[1] IBM, "Cost of a Data Breach Report," 2023

Reimagining Your PAM Program for OT and IoT Security

There are many challenges when we look at operational technology (OT) security, such as aging, fragile technology, no longer supported operating systems and software — and a longer lifespan that suggests vulnerability. Organizations must reimagine their PAM programs to secure a broader set of identities with high-risk access.

1. Discovery of Devices and Firmware Updates

Privileged access management programs should continuously discover and onboard new devices and accounts when added to your network(s), enhancing control and oversight. Isolating access to monitor and record sessions helps proactively report on and achieve continuous compliance. Managing privileged credentials on certain OT devices can be daunting due to the complexity and lacking visibility of the whole environment.

2. Gateway and Remote Access Vulnerability

Manage endpoint privileges to secure workstations (with desktop MFA, if possible) to help stop the spread of ransomware and malware to OT. Enforce an endpoint privilege manager (EPM) to harden the systems, maintain strict endpoint privilege security, and enforce least privilege, reducing the risk of unauthorized changes to critical systems. Remote access capabilities in PAM solutions are designed to provide secure access to credential vaults without virtual private networks (VPNs), passwords, or agents, plus the ability to provide offline access to credentials.

3. Defense in Depth: Paperclip Resets, Unidirectional Gateways and Device Monitoring

Attackers will never stop innovating their methods to exploit credentials and data. They will also use old tricks like the paperclip reset on devices, allowing them to reset devices to default passwords and then take over. Securing and strengthening the flow of data in OT environments is essential. Unidirectional gateway, or a data diode, integrations with CyberArk's OT and industrial control system (ICS) partners allow you to monitor and detect any attempt to bypass PAM, helping to prevent unauthorized access and high-risk account usage.

Additionally, reimagining your PAM program helps organizations by expanding the scope of identities and environments for consideration, to improve security and scalability of privileged access management. A PAM solution should secure standing credentials and secrets used for just-in-time (JIT) privileged access, either on-premises or in the cloud.

Capabilities of an Effective PAM Program

To solve some of the challenges discussed above, a PAM program is foundational for improving security hygiene, satisfying audit and compliance requirements, defending against ransomware and implementing a Zero Trust security model. The enforcement of the Zero Trust approach enables defense against both internal and external attackers by assuming all users and applications are implicitly not to be trusted and must be authenticated and authorized regardless of their location or network.

It works by:

1. Reducing risk by increasing control and visibility of privileged access.
2. Addressing IT security audit for privileged control.
3. Meeting cyber insurance requirements for privileged controls.
4. Securing vendor and third-party access.
5. Expanding PAM across an organization.

Security Objectives

Prevent Credential Theft

- Discover, vault & rotate credentials
- JIT access with Zero Standing Privileges
- Detect theft/misuse and respond

Prevent Privilege Escalation

- Implement least privilege access
- Detect risky commands and respond

Stop Lateral Movement

- Isolate and protect sessions
- Remove local admin rights

Prevent Insider Threats

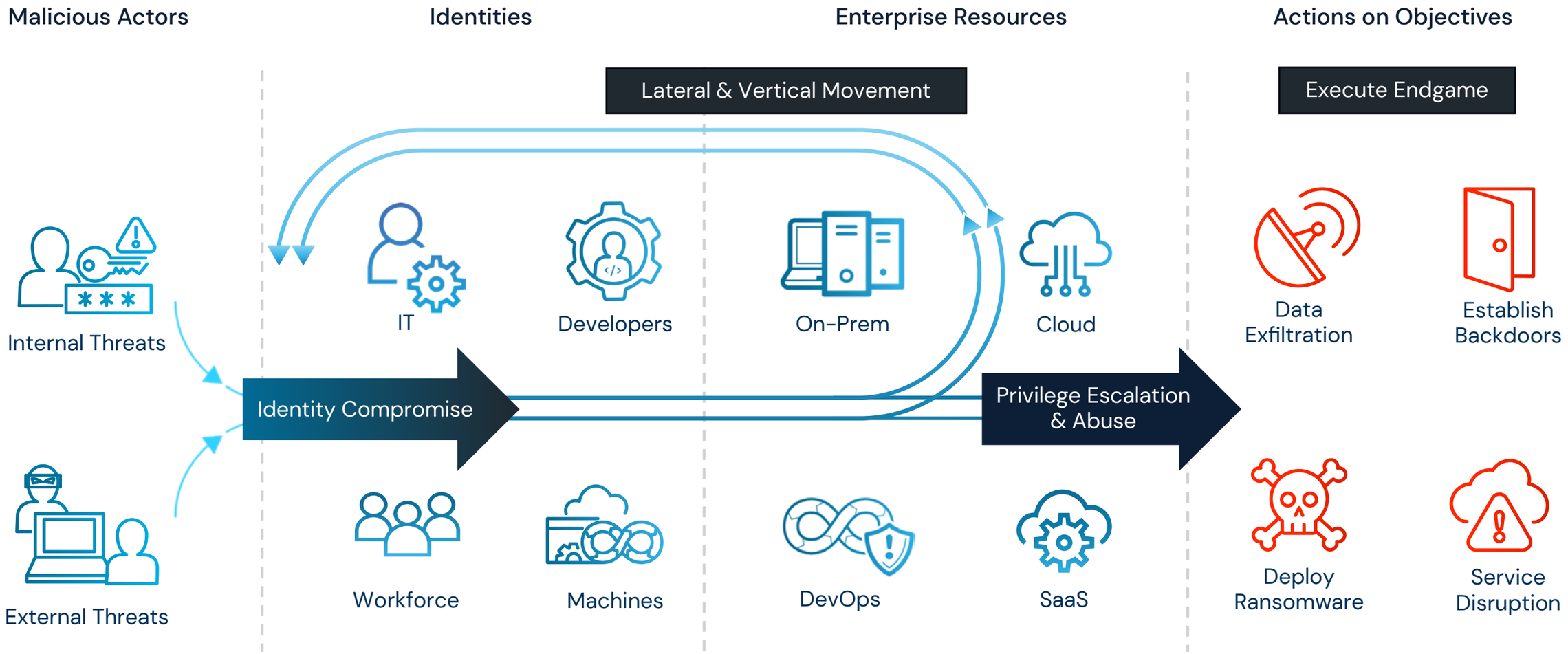
- Session monitoring and recording
- Full audit trail

Reimagine Your PAM Program With New Use Cases

From traditional on-premises servers to cloud-native applications, each layer of an IT infrastructure serves a unique purpose and presents its own set of security challenges.

Understanding the Attack Chain

Compromised identities and credentials remain a constant target in cyber attacks.



1 PAM Controls for System-Level Access to Long-Lived Systems

Many enterprises still directly manage much of the infrastructure on-premises, such as Linux and Windows servers, databases, and homegrown applications. This is especially true in highly regulated industries and verticals where low-latency computing is essential, like finance, energy and manufacturing. Even when organizations do move these established systems to the cloud, many take a 'lift-and-shift' approach. These systems still work well, so there's no need to re-architect them beyond moving them from on-premises servers to cloud-hosted virtual machines (VMs).

Whether long-lived systems exist on-premises or in the cloud, securing the privileged credentials and SSH keys that grant high-risk access to these workloads will always be essential. This is especially true of built-in accounts on servers and VMs, such as root accounts on Linux servers.

Foundational PAM best practices like automated credential rotation and least privilege access can reduce the risk of credential theft. Session isolation can further reduce risk by not allowing end users to directly connect to target resources, reducing the spread of malware, while recorded sessions are used in audits to demonstrate commands executed or keystrokes captured during privileged session. Sometimes, these controls may even be required to satisfy IT security compliance requirements or receive cyber insurance coverage.

Key Strategy

Good identity security programs need several layers. In addition to securing credentials, it's essential to apply additional PAM best practices like monitoring and isolating privileged sessions. This can help deter insider threats while preventing ransomware and other malware from ever reaching VMs.

2 PAM Controls for Operational Access to Workloads Running **ON** VMs

Most VMs are short-lived. This is one of the foundational value propositions of cloud computing; organizations can run workloads on rented VMs without spending time and money on infrastructure maintenance. While high-risk administration on specific VMs may sometimes be necessary organizations generally don't create dedicated system-level accounts (and the associated risk) for access to these short-lived machines.

PAM programs play an important role in securing access to ephemeral workloads. When access to specific, self-managed systems is needed, access can be elevated just-in-time to reduce the risk of credential theft, helping reduce standing privileges. Identity security teams and developer counterparts can tag workloads for a specific project using cloud service provider (CSP) tagging features, allowing end users to natively connect only to resources tagged with this attribute. IT and development teams can natively elevate access without the secure shell (SSH) Keys or passwords using attribute-based access control (ABAC). And since users don't have passwords with standing privileges, there is a significantly reduced risk of credential theft.

Key Strategy

The absence of credentials does not equate to the absence of trust. To embrace Zero Trust concepts for cloud access, embrace the 'never trust, always verify' paradigm. PAM Best practices like enforcement of least privilege and session isolation reduce trust. Meanwhile, the tried-and-true advice to implement adaptive multi-factor authentication (MFA) can help verify.

3 Access to Cloud Service Provider Services IN the Cloud

Protecting the most powerful access in the cloud is essential. And that includes the access engineers use to launch, configure and maintain the services powering their applications. Whether these engineers access this cloud management layer via web consoles or command line interfaces (CLIs), their access must be protected.

JIT elevation can help reduce the risk of credential theft in these scenarios. Many organizations are embracing the emerging security concept of Zero Standing Privileges (ZSP) to safeguard development teams without slowing them down. In this model, engineers can elevate access JIT only to roles scoped with just enough permissions for the job at hand (or, in other words, least privilege access).

Implementing ZSP provides meaningful, defense-in-depth risk reduction. First, developers do not have credentials with always-on access, so the risk of those credentials being stolen reduces substantially. Second, even if developers become malicious insiders or have their access compromised, their permissions are limited, reducing the blast radius of an attack.

Key Strategy

Empower developers with ZSP, instead of slowing them down. In an outage or critical situation ('critsit'), engineers need the ability to use their preferred tooling to request elevated entitlements and save the day. Integration with preferred development tooling is critical for these cases and any meaningful adoption of PAM controls. The same is true for session monitoring controls to deter internal threats and maintain audit trails for compliance purposes.

4 High-Risk Access to SaaS Apps

Risk isn't confined to infrastructure, networking devices, servers, and OT environments. It also exists in cloud-hosted web applications used by every workforce member, from software engineers to HR and finance administrators. Unfortunately, this access also presents a significant security risk, considering attackers can use it to gain access to sensitive data.

Organizations can protect this final layer of high-risk access in the cloud with web browser session protection and monitoring controls. Session protection can defend against session hijacking and cookie theft attacks. Just as with infrastructure or console access, monitoring high-risk sessions can provide a complete audit trail of user activity to satisfy compliance requirements and deter internal misuse.

Key Strategy

To get the cloud security recipe right, adjust controls according to the risk level of data in a SaaS application. For example, compromised access to apps containing IP or EHR data pose more risk than access to a training application. Just like with the PAM controls securing access to high-risk infrastructure, requiring step-up authentication to the most sensitive web apps is a simple best practice that can significantly reduce risk.

5 Take Your PAM Program Further with Access and Secrets Management

Humans aren't the only identities requiring privileged access in multi-cloud environments. Machine identities like serverless functions, application accounts and robotic process automation (RPA) bots also use credentials to authenticate autonomous processes. Expand the scope and benefit of your PAM programs by making full use of the full feature set of your PAM tools, especially secrets management for DevOps use cases, and CIEM for IaaS visibility. With a solid privileged access management foundation in place, security teams must now focus on expanding their identity security programs to encompass all facets of privileged access. That means securing human and non-human identities throughout the cycle of accessing critical assets — without slowing down development teams or delaying automation deployments.

How Reimagining your PAM Program Can Help Secure IT Admin Access

PAM capabilities delivered from the CyberArk Identity Security Platform provide end-to-end security for internal IT admins and third-party vendors, securing high-risk access used to maintain, migrate and scale systems on-premises or in the cloud.

CyberArk is the only vendor with an identity security platform that can offer customers the flexibility to provide standing access, just-in-time access or Zero Standing Privileges access depending on the identity type and the specific targets needed to be accessed

JIT access controls help prevent credential theft by replacing passwords with the temporary elevation of access to systems, applications or other high-risk areas. With ZSP security teams can take the JIT concept to take their PAM programs overall – to the next level. With ZSP, users are elevated just-in-time, with only the entitlements necessary for the task at hand.

Implementing ZSP enables security teams to:

- Reduce the risk of credential theft by preventing standing access.
- Enforce real-time least privilege in the cloud by granting only the relevant permissions a user needs and only when needed – for a given task.
- Reduces the potential impact of an account takeover; an attacker's options are extremely limited without admin-level access.
- Give users streamlined access through developer-friendly workflows and integrations. This greatly improves end-user adoption.
- Define customizable policies that reflect a wide range of use cases relevant to cloud users' jobs.

Reimagine Your PAM Program to Achieve Business Outcomes

1. Deliver Measurable Cyber Risk Reduction

Discover, onboard and securely manage high-risk accounts to prevent credential theft and identity compromise. Implement intelligent privilege controls and least privilege to reduce lateral movement and deter threats for all users, across on-premises and cloud infrastructure.

2. Enable Operational Efficiency

Secure both system and operational access – with unified support for PAM controls like credential management and access with Zero Standing Privileges. Leverage hundreds of integrations and native UX to accelerate adoption for IT, third-party vendor, developer and cloud ops users.

3. Satisfy Audit & Compliance

Achieve continuous compliance by proving adherence to industry best practices. Securely manage and rotate privileged credentials. Implement least privilege access and monitor user sessions for global regulations like SWIFT, SOC, ISO 27001.

4. Secure Digital Transformation

Secure native IT and developer access to every layer of a cloud environment – from lift-and-shift systems to elastic workloads and cloud-native services. Extend privilege controls to third-party vendors. Protect machine identities powering cloud-native apps with integrated secrets management.

PAM Best Practices for Hybrid and Multi-Cloud Environments

Today's PAM programs provides a centralized place to define and implement standard access management processes across the organization. This reduces the operational silos and inefficiencies resulting from diverse business units. Here are some best practices to secure privileged access in the cloud.

Meet Baseline Requirements

- Implement Zero Standing Privileges, replacing always-on access with configured policies based on roles, workload attributes, responsibilities and access needs.
- Maintain frictionless native access for users, by supporting existing developer workflows and integrating with existing tooling.
- Lock down cloud service provider (CSP) root and registration accounts, with credential vaulting, rotation, MFA and session isolation on all usage.
- Centralize secrets management and governance to a single hub, so developers can use their preferred tooling and the business can apply necessary industry and internal standards.
- Focus initially on meeting standards to remain compliant with industry regulations.

Standardize Audit and Reporting

- Build a proactive strategy to get ahead of auditors' required evidence, artifacts and reports – centered on continuous visibility for all identities' access.
- Define models permitting a "critical situation" level of access, to ensure on-call cloud engineering teams can quickly solve problems without waiting for approvals.
- Monitor high-risk access to cloud workloads and services, storing audit trails in the same place as web apps or on-prem session logs, to streamline processes.

Encourage Continuous Improvement

- Ensure all new cloud environments have secure access policies in place, with correctly configured roles and identity settings – offsetting the need to fix issues once they are provisioned.
- Use automation to enforce industry and internal standards for human and service-to-service access.
- Automate compliance and audit reporting processes to reduce manual work and improve efficiency.

Intelligent Privilege Controls for All Identities and Environments

Intelligent privilege controls help organizations to secure all identities. Continuous monitoring and analysis of every identity allow organizations to detect and respond to unusual behavior. Below are five critical intelligent privilege controls.

Access with Zero Standing Privileges and Just-in-Time Access

Reducing standing privileges is essential to preventing both identity compromise and lateral movement. Implementing ZSP positions organizations to grant users elevated access privileges in real-time, only when they are needed, and then revoke access once the task is completed.

This reduces the risk of credential theft and the potential impact of an account takeover. Taking the JIT concept to the next level, ZSP enables organizations to reduce the risk of credential theft and the potential impact of an account takeover by significantly limiting an attacker's options. In particular, control of TEA (time, entitlements, approvals) settings for access to cloud services can notably reduce the attack surface.

Session Isolation and Monitoring

Establish secure, isolated remote privileged sessions while monitoring and recording all activity during that session. End users should not directly connect to a target system, reducing the risk of spreading malware. Securely and centrally store recorded sessions to maintain compliance.

Secure Remote Access to Privileged Access Management

Enable the digital business with secure third-party access to critical internal infrastructure and resources with full session isolation, monitoring and audit capabilities. Provide Zero Trust third-party privileged access with JIT provisioning for a more secure, isolated session.

Endpoint Least Privilege

Organizations can manage and secure endpoints with controls that enable continuous least privilege and consider variables such as an application's context, parameters and attributes to allow or block certain scripts, applications or operations. This can significantly reduce an organization's attack surface and ability to meet various regulatory requirements.

Credentials and Secrets Management

Credential management includes password/key rotation, enforcing password policies and consistently validating the authenticity of the entity requesting the access. Secrets management allows organizations to enforce similar security policies for non-human (machine) identities.

Improving Compliance Programs

An effective PAM program can help organizations satisfy certain security related regulatory requirements. Here are examples of sources of regulatory requirements, some of which may be satisfied with an effective PAM program.

Security Regulations Applicable to Any Industry

- SOC 3
- NIST SP 800-207 Zero Trust Architecture
- ISO/IEC 27001
- Payment Card Industry Data Security (PCI DSS)
- Sarbanes-Oxley Act Financial Fraud Controls (SOX)
- Cybersecurity Maturity Model Certification (CMMC)
- EU General Data Protection Regulation (GDPR)

Financial Sector Regulations

- SWIFT Customer Security Controls Framework
- Digital Operational Resiliency Act (DORA)
- MAS Technology Risk Management Guidelines (MAS)
- Gramm-Leach-Bliley Act (GLBA)
- SEC Deadlines and the Role of Automation
- Internal Revenue Services (IRS) 1075

Healthcare Industry Security Regulations

- Health Insurance Portability and Accountability Act (HIPPA)
- Health Information Technology for Economic and Clinical Health Act (HITECH)
- German Federal Data Protection Act or Patientendaten-Schutz-Gesetz (PDSG)

Critical Infrastructure Security Regulations

- EU Network and Information Systems (NIS2) Directive
- German Critical Infrastructure Regulation
- French Military Programming Law
- Australian Critical Infrastructure Security Act
- Singapore Cybersecurity Act

CyberArk Blueprint

The CyberArk Blueprint is a best practices framework that helps customers plan and implement an effective PAM program. It helps customers identify high-value, high-risk targets and prioritize PAM efforts and coverage to align investments with potential risk-reduction benefits.

The CyberArk Blueprint takes an "assume breach" approach to PAM, defending against the tactics attackers typically employ to penetrate systems, traverse networks and wreak havoc. These are the three guiding principles of the CyberArk Blueprint that help customers secure their environment and contain threats:

- **Prevent credential theft:** Whether it is administrative account passwords or SSH keys used to secure application traffic, safeguarding credentials is the first step in securing your environment.
- **Stop lateral and vertical movement:** Prevent bad actors from jumping from lower-value targets like workstations to your most critical assets like servers through proper enforcement of credential boundaries, credential randomization and the like.
- **Limit privilege escalation and abuse:** Enforce the principle of least privilege to contain attackers, shrink implicit trust zones and minimize the blast radius.

Summary

As organizations plan to move workloads and applications into the cloud, new challenges arise due to the scalability and flexibility of cloud computing. The shared responsibility for security and the highly elastic cloud environments requires more dynamic protections and controls. Improving the efficiency of your PAM program can help you secure the use of shared and privileged accounts with credential management and session isolation and monitoring; elastic cloud workloads, which are dynamic and ephemeral. Take the next step and modernize your PAM program to maximize the value of your PAM deployments and build a cyber resilient organization.

Learn more about how **CyberArk Blueprint** helps organizations reimagine an effective PAM program.

Contact us to schedule a meeting to discuss your organization's needs.

Request A Demo

CyberArk is the global leader in identity security. Centered on intelligent privilege controls, 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. To learn more about CyberArk, visit www.cyberark.com, read the CyberArk blogs or follow us on Twitter via @CyberArk, LinkedIn or Facebook.

CYBERARK®
The Identity Security Company™