

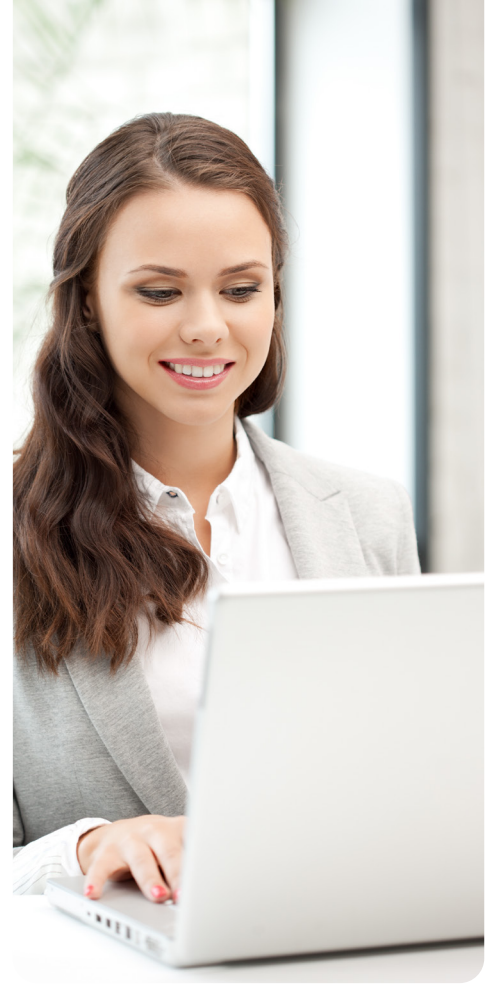
Privileged Access Management (PAM) as a service

Overview

In today's hyperconnected digital landscape, privileged access is the #1 attack vector. From ransomware actors to nation-state threats, adversaries relentlessly target privileged accounts—the keys to an enterprise's crown jewels. Mismanagement of these credentials doesn't just open the door to cyberattacks—it magnifies regulatory exposure, increases downtime risk and erodes stakeholder trust. Privileged Access Management (PAM) has therefore become a cornerstone of any mature cybersecurity and zero trust strategy.

Recognizing the criticality and complexity of modern PAM, HCLTech and CyberArk jointly offer a comprehensive PAM as a Service (PAMaaS) solution that transforms how enterprises secure and manage privileged identities across their entire IT estate—from on-prem infrastructure to multicloud environments and DevOps pipelines.

At the heart of this offering is CyberArk's Privilege Cloud, a Gartner and Forrester-recognized SaaS platform that simplifies PAM while delivering unmatched security depth. Augmented by HCLTech's global cybersecurity services expertise the solution is not just with ; it's a strategic managed service that combines intelligent automation, zero trust enforcement and continuous compliance.



Business challenges

1 Increased risk of cyberattacks and data breaches

Without PAM, organizations are highly vulnerable to attacks involving compromised privileged credentials. Gartner has highlighted that many high-profile breaches are directly linked to privilege abuse.

2 Compliance failures

Many industries require strict access controls to meet regulatory standards (e.g., GDPR, HIPAA, SOX). Without PAM, tracking and auditing privileged access becomes difficult, leading to non-compliance and potential fines.

3 Financial losses

Data breaches and compliance violations can result in massive financial penalties, lawsuits and remediation costs. The Target breach in 2024, caused by poor PAM practices like Santander Bank Breach, Snowflake Cloud Breach, AT&T Exposures, etc. led to multi-million dollars in settlements.

4 Operational inefficiencies

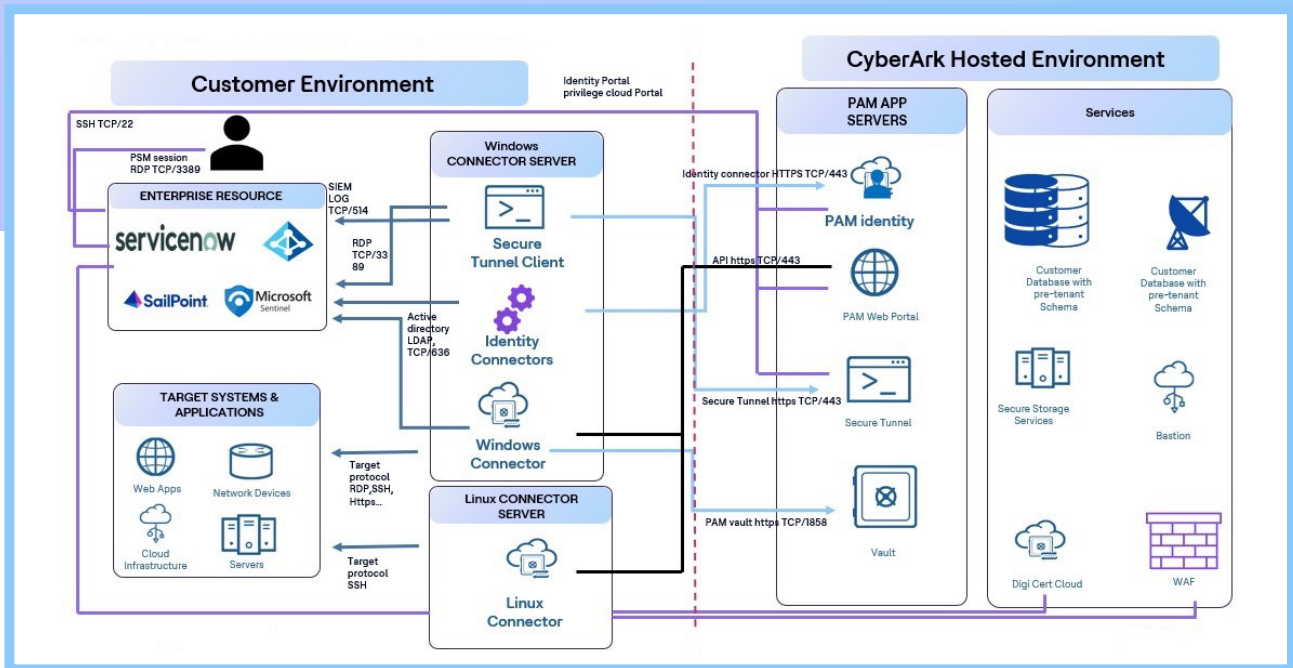
Manual management of privileged accounts is time-consuming and error-prone. It can lead to delays in provisioning/de-provisioning access, misconfigurations and reduced productivity.



Our solution

HCLTech and CyberArk have partnered to deliver a robust Privileged Access Management (PAM) solution that addresses the increasing risks of credential theft, compliance failures and operational inefficiencies. This solution helps enterprises secure privileged access across on-prem, cloud or hybrid environments while enabling Zero Trust and regulatory alignment. Below are the key capabilities:

- Secure storage and automated rotation of passwords and SSH keys to prevent unauthorized access.
- Isolate privileged sessions and record activities for real-time monitoring and forensic analysis
- Implement zero standing privileges and enforce the principle of least privilege across endpoints, servers and cloud workloads.
- Grant temporary privileged access based on contextual risk, reducing the attack surface.
- Detect anomalous behavior and apply adaptive access policies using integrated threat intelligence.
- Secure secrets and credentials used in cloud platforms (AWS, Azure, GCP) and DevOps pipelines (Terraform, Jenkins, Kubernetes).
- Generate detailed audit logs and reports to meet GDPR, HIPAA, SOX and other regulatory requirements.
- HCLTech provides end-to-end PAM implementation, consulting, operations and continuous improvement, ensuring scalability and resilience.



HCLTech offers a proven roadmap to implement PAM, with expert consultation, seamless implementation and managed services. The various phases involved in the process are as follows:

Consulting & Advisory Services	Professional Services	Managed Services
<ul style="list-style-type: none"> • Understand as-is PAM processes and deployment • Review security controls • Perform a detailed assessment of the as-is PAM configuration and deployment • Identify gaps, risks, observations and provide recommendations to mitigate the same 	<ul style="list-style-type: none"> • Define use cases • Draft architecture as per the requirement • Perform implementation (basis on approved design) • Configure the application • Perform integrations, SIT/UAT • Training & handover 	<ul style="list-style-type: none"> • PAM Maintenance and Administration • Service requests (SR) • Proactive recommendations • Incident management • Reporting • Knowledge management • Problem management

Value delivered

Reduced operational overhead & predictable costs

By moving to a fully managed, cloud-based model (PAMaaS), organizations eliminate the need for upfront investments in infrastructure and ongoing IT maintenance. This transition shifts CapEx to a predictable Opex model while freeing internal resources for more strategic initiatives.

Accelerated time to value

Traditional on-prem PAM deployments can extend over weeks or months. PAMaaS enables rapid implementation—often in days or hours—helping businesses quickly fortify privileged access controls and meet urgent compliance demands.

Enhanced security posture

Centralized control over privileged access, strict enforcement of the principle of least privilege, session recording, and advanced monitoring significantly elevate defense against credential theft, misuse, and lateral movement.

Scalability & flexibility

Cloud native PAM scales effortlessly to accommodate organizational growth, supports integrations with hybrid environments, and adapts to evolving security and operational needs.

Faster breach containment & threat response

PAMaaS solutions aid in the rapid detection and containment of suspicious activity by restricting access within tight time windows and providing comprehensive oversight.

Benefits

Reduced attack surface and risk exposure

Monitor who accessed what, when and how—capturing session histories and behavioral alerts in real time to strengthen forensic readiness and oversight.

Elevated productivity and operational efficiency

Automation of privileged workflows (e.g., password rotation, approvals), self-service access and unified dashboards streamline operations and reduce admin burden.

Stronger compliance and governance

PAM inherently supports regulations like HIPAA, SOX, PCI DSS and GDPR through comprehensive access control, rotation, session logs and consistent policy enforcement.

Better cyber insurance positioning

Demonstrable control and visibility over privileged access—core insurance requirements—can lower premiums and increase coverage eligibility.

Reduced Attack Surface & Risk Exposure

Enforcing least privilege and JIT access dramatically shrinks the window of opportunity for misuse, insider threats and external breaches.

Future-proofed security strategy

With built-in automation, analytics and adaptability, PAMaaS aligns with emerging needs like zero-trust frameworks, DevOps integration and hybrid cloud security postures.

Why HCLTech?

800+

Active client engagements

8000+

Cybersecurity professionals

28+

Years of mature security practice

50+

Collaborative partner alliances

10

CSFCs & 40+ GDCs

Recognized by

Everest, ISG, Avasant, IDC, Forrester and Gartner

HCLTech | Supercharging
Progress™

hcltech.com