Solutions At-A-Glance

Version: 13 October 2022

cyberark.com

CyberArk Defines Identity Security As

Centered on intelligent privilege controls, **Identity Security** seamlessly secures human and machine identities accessing workloads from hybrid to multi-cloud, and flexibly automates the identity lifecycle - all with a unified approach.

cyberark.com

Modern Identity Security Defined
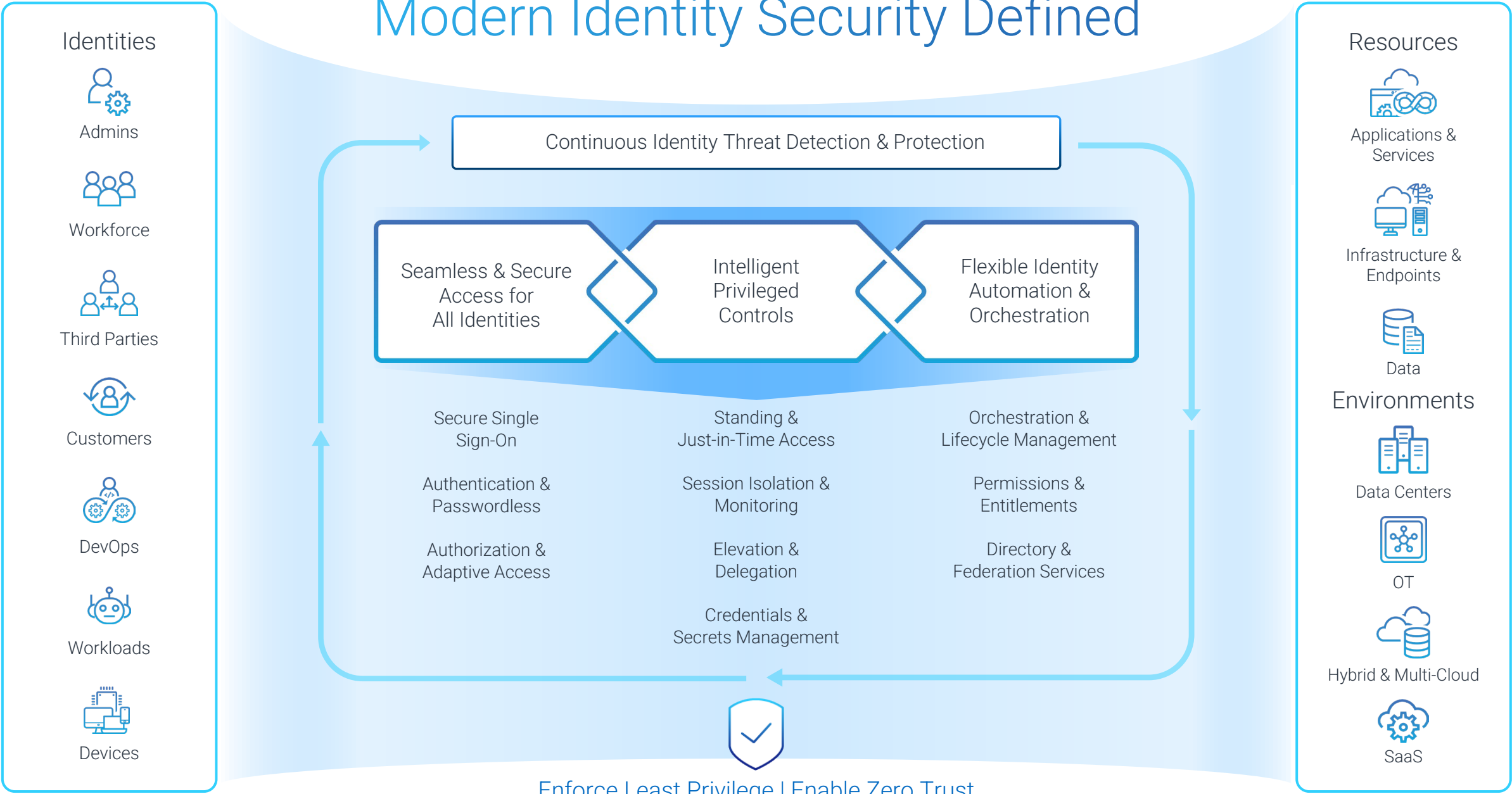
Identities

- Admins
- Workforce
- Third Parties
- Customers
- DevOps
- Workloads
- Devices

Resources

- Applications & Services
- Infrastructure & Endpoints
- Data

Environments

- Data Centers
- OT
- Hybrid & Multi-Cloud
- SaaS

Continuous Identity Threat Detection & Protection

Seamless & Secure Access for All Identities	Intelligent Privileged Controls	Flexible Identity Automation & Orchestration
Secure Single Sign-On	Standing & Just-in-Time Access	Orchestration & Lifecycle Management
Authentication & Passwordless	Session Isolation & Monitoring	Permissions & Entitlements
Authorization & Adaptive Access	Elevation & Delegation	Directory & Federation Services
	Credentials & Secrets Management	

Enforce Least Privilege | Enable Zero Trust

Workforce and Customer Access Overview

	ACCESS			
Product Name	CyberArk Identity		Workforce Password Management	Secure Web Sessions
Self-Hosted or SaaS	SaaS		SaaS	SaaS
Previous Names	iDaptive		Product launched in 2021	Product launched in 2021
Product Abbreviation	SSO	MFA	WPM	SWS
Product Full Name	Single Sign-On	Adaptive Multi Factor Authentication	Workforce Password Management	Secure Web Sessions
Primary Purpose	1. One-click access to cloud, mobile & legacy apps 2. One set of credentials to access all cloud and on-prem apps in one place 3. Self-service password reset 4. VPN-less access to internal applications	1. Adds an extra layer of protection before granting access to apps 2. Broadest choice of authentication factors, including passwordless 3. Architected for using OATH, FIDO & RADIUS standards 4. Provides step-up authentication based on risk assessment of user authentication. 5. Intuitive dashboard to investigate abnormal user authentication behavior.	1. Single console to store and manage credentials 2. Enable secure password sharing without involving IT 3. Protect access to credential stored in self-hosted Vault or Cloud 4. Track access activity, control password complexity and revoke access to credentials when no longer needed	1. Record, audit, and protect all user activity within web applications accessible through CyberArk Identity
Primary User	Head of Security, IAM			Power Users (e.g. HR Director, Financial Controller)
License Method	License based on number of users			# of users and storage credits
Global Competitor	Okta, Microsoft, RSA, Ping, OneLogin, ForgeRock, MicroFocus, IBM, Oracle		1Password, HitachiID, LastPass, Yukon	No competition

cyberark.com

Endpoint Privilege Manager Overview

	PRIVILEGE		
Product Name	Endpoint Privilege Manager		
Self-Hosted or SaaS	SaaS		
Previous Names	Endpoint Privilege Manager		Least Privilege Server Protection for *NIX
Product Abbreviation	EPM for Workstation	EPM for Servers	EPM For Linux
Product Full Name	EPM for Workstation	EPM for Servers	EPM For Linux
Primary Purpose	1. Remove Local Admin 2. Rotate/ Manage Local Admin Password (with CyberArk PAM) 3. Prevent Credential Theft 4. Restrict App Install/ Permission		1. Unix Command Control
Primary User	Windows, Mac and Linux Workstation Users	Windows Server Admin	Linux Admin
License Method	License based on Number of Workstations Minimum Order Quantity : 100 workstations	License based on Number of Servers Minimum Order Quantity : 25 servers	Number of Servers Minimum Order Quantity : 25 servers
Global Competitor	BeyondTrust, Delinea, CrowdStrike, IBM, MasterSAM, Thycotic, Wallix, Microsoft LAPS		

cyberark.com

Privilege Cloud Overview

	PRIVILEGE					
Product Name	Privilege Cloud (Priv. Cloud)					
Self-Hosted or SaaS	SaaS					
Previous Names	Privilege Cloud					
Product Abbreviation	EPV	ISP	CPM	PSM	PSMP	ISI [NEW]
Product Full Name	Enterprise Password Vault (Part of SaaS)	Identity Security Platform Unified UI (Part of SaaS)	Central Policy Manager (Part of Cloud Connector)	Privilege Session Manager for Windows (Part of Cloud Connector)	Privilege Session Manager for SSH (Additional Connector)	Identity Security Intelligence [NEW]
Primary Purpose	Securely store 1. Password 2. Recordings 3. Audit Trails	1. ISP Main login page	Validate & Rotation of 1. Passwords 2. SSH Keys Scan for new accounts on 1. Windows 2. Linux	1. Windows Jump Host 2. Transparent Login 3. Session Recording 4. Live Monitoring 5. Session Suspend 6. Win Remote APP 7. HTML5 RDP	1. Unix Jump Host 2. Transparent Login 3. Session Recording 4. Command Restriction 5. Session Suspend	1. Built-in reports/dashboard that help risk visualization and breach investigations 2. Predictive risk analytics 3. Threat intelligence 4. Automated response & remediation
Primary User	Infra Admin, Windows Admin, DBA, Network Admin, Linux/ Unix Admin, Cloud Admin					Infra Admin, SOC Team, Auditor
License Method	License based on Number of Named Users | Number of 3rd Party Users Minimum Order Quantity : 25 Users					
Global Competitor	BeyondTrust, Delinea					
C3 Alliance Partner	SIEM: Splunk, ArcSight, LogRhythm | Identity Management: SailPoint | Vulnerability Scanning: Tenable					

PAM Self-Hosted Overview

	PRIVILEGE					
Product Name	Privileged Access Manager Self-Hosted					
Self-Hosted or SaaS	Self-Hosted. On Premise					
Previous Names	Core PAS (Privileged Access Security)					
Product Abbreviation	EPV	PVWA	CPM	PSM	PSMP	PTA
Product Full Name	Enterprise Password Vault	Password Vault Web Access	Central Policy Manager	Privilege Session Manager for Windows	Privilege Session Manager for SSH	Privileged Threat Analytics
Primary Purpose	Securely store 1. Password 2. Recordings 3. Audit Trails	1. Main login page	Validate & Rotation of 1. Passwords 2. SSH Keys Scan for new accounts on 1. Windows 2. Linux	1. Windows Jump Host 2. Transparent Login 3. Session Recording 4. Live Monitoring 5. Session Suspend 6. Win Remote APP 7. HTML5 RDP	1. Unix Jump Host 2. Transparent Login 3. Session Recording 4. Command Restriction 5. Session Suspend	Detect & Alert 1. High-risk sessions 2. PAS bypass attempt 3. Privileged Account Theft Auto-onboard 1. Privileged Accounts 2. IaaS Accounts
Primary User	Infra Admin, Windows Admin, DBA, Network Admin, Linux/ Unix Admin, Cloud Admin, SOC Team, Auditor					
License Method	License based on Number of Named Users | Number of 3rd Party Users Minimum Order Quantity : 25 Users					
Global Competitor	BeyondTrust, Delinea					
C3 Alliance Partner	SIEM: Splunk, ArcSight, LogRhythm | Identity Management: SailPoint | Vulnerability Scanning: Tenable					

cyberark.com

Vendor Privileged Access Manager Overview

	PRIVILEGE
Product Name	Vendor Privileged Access Manager
Self-Hosted or SaaS	SaaS
Previous Names	Alero, Remote Access
Product Abbreviation	VPAM
Product Full Name	Vendor Privileged Access Manager
Primary Purpose	1. Remote Vendor Access to CyberArk PAM 2. JIT (Just-in-Time) External User Remote Access with Multi-Factor Authentication (MFA) 3. Record and monitor, gain full visibility into vendor activities, with complete reporting, auditing and remediation capabilities 4. Offline Access, securely provide access credentials to authorized third parties in air-gapped and other offline environment 5. Dual control approval via mobile app. 6. MUST integrate with PAM Self-Hosted or Privilege Cloud
Primary User	3rd Party Vendor, Infra Admin, Windows/Linux Admin, Network Admin
License Method	License based on Number of Remote/ External/ 3rd Party Users
Global Competitor	BeyondTrust, Centrify, Okta, Proofpoint, Delinea, Wallix, ZScaler

cyberark.com

Dynamic Privileged Access Overview

	PRIVILEGE
Product Name	Dynamic Privileged Access [NEW]
Self-Hosted or SaaS	SaaS
2022 Name	Anticipated Launch in 2023
Product Abbreviation	DPA [NEW]
Product Full Name	Dynamic Privileged Access [NEW]
Primary Purpose	1. Reduce risk of standing access by providing Just-in-Time (JIT) access to specific VMs in the cloud and specific servers on-premises 2. Extend PAM coverage across hybrid + multi-cloud environments to accelerate Zero Trust initiatives 3. Windows and Linux instances on AWS/ Azure/ GCP 4. Attribute Based Access Control (ABAC) policies 5. Agent-less SaaS solution 6. Full audit trail and session isolation 7. Born in the cloud SaaS solution with no vaulting, account onboarding or management required 8. DPA is currently available for Linux Virtual Machines in AWS and Azure and Windows on prem machines
Primary User	Head of PAM/ IAM, Security Architect, Head of Cloud Security
License Method	License based on Number of Users
Global Competitor	Okta, Remediant/ Saviynt, Delinea, BeyondTrust, Azure PIM

cyberark.com

Secrets Management Overview

	DevSecOps						
Product Family	Credential Providers			Conjur			Secrets Hub [NEW]
Product Name	Credential Provider	Application Server Credential Provider	Central Credential Provider	Conjur Enterprise	Conjur OSS	Conjur **Cloud [NEW]**	Secrets Hub [NEW]
Self-Hosted or SaaS	Self-Hosted (supports PAM Self-Hosted & Privilege Cloud)				Self-Hosted	SaaS	SaaS
Previous Names	AAM (Application Access Manager)					Controlled Availability in 2022	
Product Abbreviation	CP	ASCP	CCP	Conjur Ent.	Conjur OSS	Conjur Cloud [NEW]	SH [NEW]
Product Full Name	Credential Provider	Application Server Credential Provider	Central Credential Provider	Conjur Secrets Manager Enterprise	Conjur Open Source Suite	Conjur Cloud [NEW]	Secrets Hub [NEW]
Primary Purpose	Agent-based secret retrieval on bare-metal server or VM: 1. C3 Solutions 2. Scripts 3. Home-grown apps	Agent-based application server secret retrieval: 1. JBoss 2. Tomcat 3. WebLogic 4. WebSphere	Agentless secret retrieval via web services or REST API: 1. C3 Solutions 2. DevOps tools 3. IoT	Secret retrieval by containers (OpenShift, Kubernetes), cloud workloads and DevOps tools	Open-source version of Conjur Enterprise, with no web UI, HA, DR, followers for caching & auto-scaling, HSM or SIEM support etc.	Secret retrieval by containers (OpenShift, Kubernetes), cloud workloads and DevOps tools	Sync secrets to cloud service provider like AWS Secrets Manager, from Privilege Cloud with centralized control
Primary User	Developer, Network Admin, Security Architect	DBA, Security Architect	Developer, DevOps, Security Architect	Developer, DevOps, Security, Cloud Architect	Developer, DevOps	Developer, DevOps, Security, Cloud Architect	Developer, DevOps, Security, Cloud Architect
License Method	• C3 Integration (CP/CCP/Conjur): Number of integration units / RPA bots • Home Grown Apps (CP/ASCP/CCP): No of calling systems • Conjur T1: No of regions (5 container clusters, 15 cloud a/c & 20 ISV Conjur) • Get-Started Package: 20 ISV/RPA, 20 calling systems, 1 region of Conjur T1 • IoT (Phosphorous): No of devices (per 10K devices)				Open source, Free to use	TBA	TBA
Global Competitor	HashiCorp						No competition
C3 Alliance Partner	RPA: Blue Prism, UiPath, AA	Redhat (JBoss), IBM (WebSphere)	IoT: Phosphorus	Container: RedHat OpenShift, docker, Pivotal; CI/CD: CloudBees Jenkins, RedHat Ansible, Puppet; Cloud: AWS, Microsoft, Google			AWS

Cloud Privilege Security Overview

	PRIVILEGE	
Product Name	Cloud Entitlements Manager	Secure Cloud Access [NEW]
Self-Hosted or SaaS	SaaS	
Previous Names	Cloud Entitlements Manager	Anticipated launch in 2023
Product Abbreviation	CEM	SCA [NEW]
Product Full Name	Cloud Entitlements Manager	Secure Cloud Access [NEW]
Primary Purpose	1. Continuous, AI-powered detection and remediation of hidden, misconfigured and unused permissions for all cloud identities 2. Support major cloud platforms – AWS, Azure and Google Cloud Platform 3. Onboard cloud workspaces 4. Automatically analyze permissions 5. Assess analytics and implement CEM recommendations	1. Provisions Just-in-Time, least privilege access to cloud services via the AWS, Azure and GCP cloud console 2. Remove standing access 3. Session protection and monitoring. All activity recorded 4. Full integration with CyberArk Identity
Primary User	Cloud Security Architect | Cloud Team | Security Team | Security Architect	
License Method	License based on Number of Cloud workspaces	TBA
Global Competitor	Microsoft, Sailpoint, Palo Alto, Crowdstrike, Cloudknox, AWS	Microsoft Azure

cyberark.com

Identity Management Overview

	ACCESS			
Product Name	CyberArk Identity		Identity Flows [NEW]	Identity Compliance [NEW]
Self-Hosted or SaaS	SaaS		SaaS	SaaS
Previous Names	iDaptive		Anticipated launch in 2022	Product Launched in 2022
Product Abbreviation	LCM	DS	Identity Flows [NEW]	Identity Compliance [NEW]
Product Full Name	LifeCycle Management	Directory Services	Identity Flows [NEW]	Identity Compliance [NEW]
Primary Purpose	1. Provision access to apps from a central admin point & with right access based on roles/ groups 2. Automate licensing & entitlement management; manage device authorization 3. Leverage HR systems as the single source of truth	1. Centrally manage users at scale 2. Integrate with a variety of popular on-premises and cloud-based directory services, including Microsoft Active Directory, Azure AD, LDAP directories, and more	1. Automates identity management tasks through no-code app integrations and workflows for identity data, processes, and events 2. Keep identity data in sync between systems and use event triggers to take provisioning or deprovisioning actions into any configured applications	1. Automates the discovery, certification, and reporting of access rights 2. Easily find and view all the resources and entitlements to user 3. Access certification, with continuous and risk-aware access review 4. Application, role, and policy compliance management and orchestration 5. Continuous compliance with adaptable workflows, analytics, reporting and dashboards
Primary User	Security, IAM			
License Method	License based on Number of users			
Global Competitor	Okta, Microsoft, RSA, Ping, OneLogin, ForgeRock, MicroFocus, IBM, Oracle			

cyberark.com

What's Next?

Where to find out more?

Who to contact?

Please reach out to your local CyberArk Channel Account Manager for more information

cyberark.com