CYBERARK® | HYDDEN

www.hydden.com

SOLUTION BRIEF

ACCELERATE PAM & IGA DEPLOYMENTS THROUGH CONTINUOUS DISCOVERY

Continuously discover all identities across hybrid environments, automatically identify high-risk accounts, and streamline onboarding applications and identity data to CyberArk's PAM and IGA solutions.

THE CHALLENGE

Identity visibility gaps persist across large enterprises with complex, hybrid infrastructure. High-risk identities reside outside Active Directory in systems that lack standard connection paths. Many applications remain disconnected from core PAM and IGA processes due to brittle, script-based connection paths, inhibiting regulatory compliance adherence.

THE SOLUTION

Hydden strengthens CyberArk by continuously discovering identity data across any system, validating quality, and automating workflows through CyberArk's PAM and IGA. Unmanaged privileged accounts are automatically onboarded to EPV/Privilege Cloud Safes and CyberArk Modern IGA benefits from continuous data quality checks ensuring trustworthy audit-ready evidence.

HOW HYDDEN ENHANCES CYBERARK PAM & IGA

1 DISCOVER EVERY ACCOUNT

Continuously discovers all identity data across your entire infrastructure, utilizing Hydden's Universal Collector for maintaining connections to non-standard systems

→

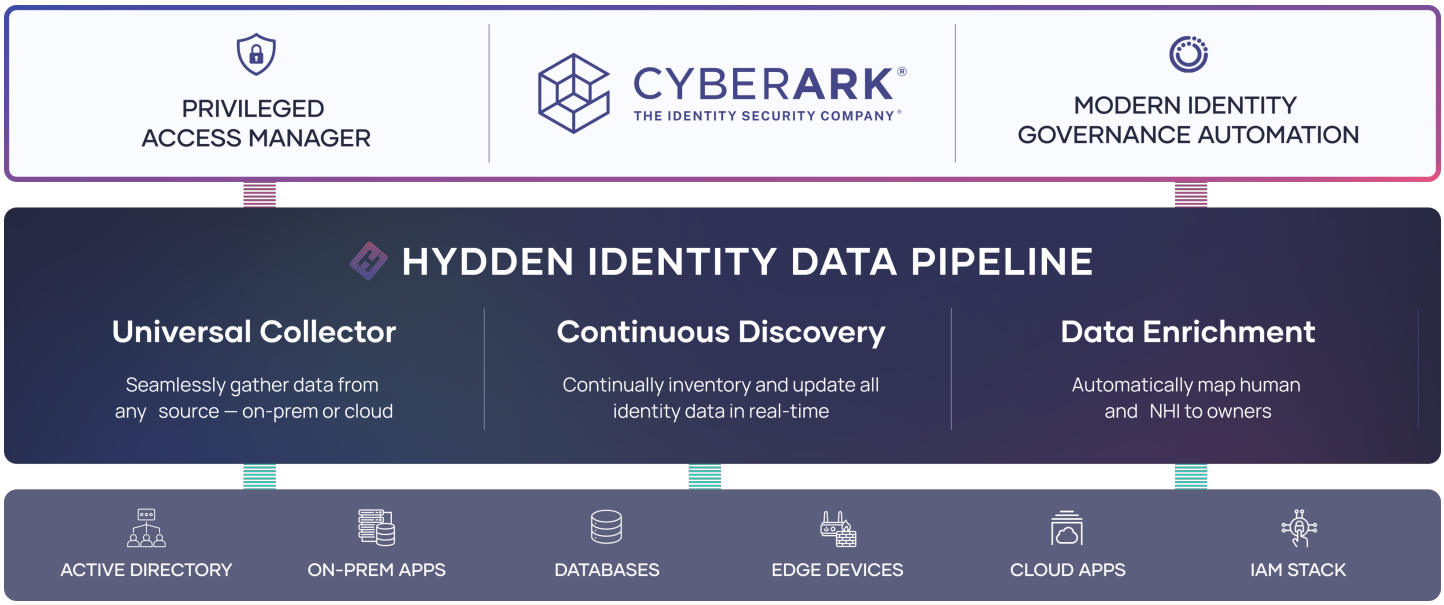
2 ANALYZE & ENRICH IDENTITY DATA

Maps relationships, detects threats, proactively resolves hygiene risks, auto-classifies privileged accounts, and maintains data collection integrity

→

3 OPERATIONALIZE CYBERARK

Auto-vault every unmanaged privileged identity into existing Safes + continuously validate identity data extraction from apps so CyberArk's IGA



COMPLETE PAM COVERAGE

- **Manage every privileged account:** Discover human and machine accounts across legacy/custom apps, databases, endpoints, and devices—beyond AD.
- **Auto-onboard to Safes:** Push unmanaged credentials (passwords, SSH keys, certs, tokens) into EPV/Privilege Cloud for rotation and policy control.
- **Risk-informed hardening & JIT:** Surface hygiene gaps (stale creds, shared/local admins, MFA gaps) to inform CyberArk policies and JIT decisions.
- **Endpoint least-privilege:** Identify and vault local admin accounts on Windows, Mac, & Linux.
- **Context for action:** Enrich with ownership, usage and risk to prioritize remediation of critical and risky accounts.

ACCELERATE IGA DEPLOYMENT

- **Broaden access review coverage:** Bring accounts from non-standard and custom systems into certification campaigns.
- **Continuous data assurance:** Source ↔ IGA parity checks for deltas, duplicates, and historical replay makes the data provably trustworthy.
- **Minimize app owner intervention:** Guarantee integrity of data collection by auto-adjusting connections when fields/APIs change to ensure IGA policies work with quality identity information.
- **Owner mapping for machine accounts:** Link service and machine accounts to human owners for reliable de-provisioning and separation of duties.
- **Audit-ready evidence:** Dated proof of completeness and accuracy for regulators.

PROVEN BUSINESS IMPACT

Save security engineering time by onboarding apps and entitlements in hours not weeks

Reduce need for app owners & engineers to maintain brittle script-based connections

Provide evidence to auditors that every enterprise app is secured with validated data sent to PAM & IGA

WHY HYDDEN + CYBERARK

The integrated CyberArk-Hydden solution provides complete coverage of critical privileged accounts – both human and machine – across cloud, on-premises, SaaS applications, databases, containers, and edge devices. Security teams can quickly remediate risks by automatically adding discovered accounts into CyberArk's Privileged Access Manager, leveraging existing vault investments to secure the privileged identity attack surface. IGA teams can rapidly scale CyberArk's Modern IGA to every critical account—adding contextual information like ownership, usage patterns, and hygiene status so reviewers understand risk at a glance.