Secrets Replicator for CyberArk Secrets Hub and Azure Key Vault

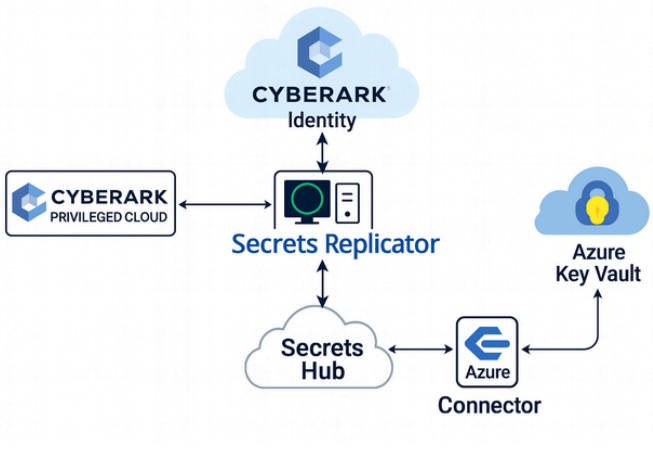
Enterprise-grade privileged access continuity solution for identity resilience and compliance

Addressing critical gaps in privileged access continuity

Identity leaders face an inherent paradox: the security controls protecting critical credentials can become barriers during the incidents when those credentials are most urgently needed. When CyberArk environments become inaccessible during underlying infrastructure outages or security incidents, identity teams must resort to manual break-glass procedures that introduce delays, human error potential, and audit trail gaps. For identity programs governed by strict compliance mandates, these procedural gaps represent material risk exposure.

Introducing Secrets Replicator: Strategic privileged access resilience

Secrets Replicator addresses these challenges through automated, policy-driven credential replication that maintains privileged access availability independent of primary PAM infrastructure status. The solution integrates natively with CyberArk Secrets Hub and Azure Key Vault to establish a continuous synchronization framework that ensures critical privileged credentials remain accessible through an alternate, secure access path.



Strategic Implementation and Architecture

Secrets Replicator represents a paradigm shift from reactive break-glass procedures to proactive privileged access resilience. The solution operates through CTI's automation framework, enabling identity programs to move beyond traditional disaster recovery toward comprehensive resilience strategies.

CTI Global
Identity & Access Management
(215) 300-3657
sales@cticorp.com
www.cticorp.com

Key implementation benefits:

- **Preserves existing governance controls** while extending credential availability through independent access paths
- **Automated orchestration** manages secure credential replication across hybrid environments
- **Proactive resilience** replaces manual procedures with tested, automated capabilities
- **Comprehensive failure coverage** addresses the full spectrum of potential system failure scenarios

Technical requirements

- CyberArk Secrets Hub with API access
- Azure Key Vault with appropriate access policies
- CTI automation framework for orchestration and monitoring

Quantifiable business outcomes

Implementation metrics demonstrate significant operational improvements that directly impact recovery time objectives and business continuity postures:

- **95% reduction** in credential provisioning time during disaster scenarios
- **300+ privileged accounts** onboarded in minutes rather than days
- **100% successful validation** of disaster recovery procedures
- **Reduced RTOs** through automated credential availability
- **Strengthened compliance posture** with comprehensive audit trails

Ready to transform privileged access disaster recovery from risk to resilience?

Schedule time to talk with CTI and evaluate how Secrets Replicator can strengthen your privileged access management program's resilience posture and compliance alignment while seamlessly integrating with your existing identity governance framework.