Cryptographic Posture + Lifecycle Management

HashiCorp Vault

IBM **Guardium**

Cryptography Manager

Discover, assess and mitigate cryptographic risks across hybrid cloud, AI systems, and the post-quantum transition

Cryptography for modern, hybrid cloud environments

Cryptography is no longer just about encryption or secrets management. It has become a continuously changing operational lifecycle problem across hybrid cloud, AI systems, and post-quantum transition planning.

PQC-readiness starts here

IBM Guardium Cryptography Manager and HashiCorp Vault deliver a unified approach to cryptographic lifecycle management — discovering, assessing, governing, and automating cryptographic assets across hybrid & multi-cloud environments.

Security Lifecycle Managment

Vault
Secrets & crypto lifecycle managment

Vault Radar
Secret discovery & remediation

Boundary
Secure remote access

GCM
Crypto discovery & posture assesment

Traditional cryptography management	Cryptographic lifecycle management
Fragmented tools	Unified governance
Static certificates	Dynamic lifecycle
Point-in-time discovery	Continuous posture assessment
Manual rotation and renewal	Policy enforcement
Human-centric operations	Automation
Reactive PQC planning	Crypto-agility

Govern and Automate

IBM **Guardium Cryptography Manager**

- Discover cryptographic assets across hybrid and multi-cloud environments
- Assess cryptographic posture, policy compliance, and exposure
- Identify quantum-vulnerable algorithms and dependencies
- Prioritize remediation and crypto agility initiatives

Remediate and Govern

HashiCorp **Vault**

- Centralize management of secrets, keys, and certificates
- Automate key rotation, certificate renewal, and credential revocation
- Enforce policy-driven cryptographic lifecycle management
- Enable crypto-agility through automated lifecycle controls
- Secure non-human identities, workloads, and agentic systems

IBM Platinum Partner FOUR inc.

HashiCorp Vault

IBM Guardium Cryptography Manager

Cryptographic lifecycle management is becoming an operational requirement

Shorter certificate lifecycles are driving the need for automation

- The CA/Browser Forum has mandated certificate lifetimes to just 47 days by 2029, dramatically increasing the frequency of certificate issuance, renewal, and rotation.
- As certificate lifecycles continue to compress, automated and policy-driven CLM will become essential to reduce overhead, prevent outages, and maintain compliance at scale.

Preparing for 2029 post-quantum cryptography (PQC) transition requirements

- Threat actors are already executing "harvest now, decrypt later" attacks by capturing encrypted data today with the expectation that future quantum computing advances will be able to break widely used algorithms such.
- Organizations need continuous visibility into PQC exposure and cryptographic dependencies to prioritize remediation and prepare for the transition to quantum-safe cryptographic standards.

Age of agentic creates new asset lifecycle management and security requirements at scale

- Applications, services, and autonomous agents introduce new certificates, secrets, encryption keys, and cryptographic dependencies that must be securely issued, rotated, governed, and revoked.
- Manual lifecycle management and fragmented cryptographic governance models cannot scale to support the operational demands of modern AI-driven, hybrid, and multi-cloud environments.

Cryptographic management across complex enterprise environments requires discoverability, inventory, automation and remediation

Discover cryptographic risk
- Continuously inventory keys, certificates, secrets, and algorithms
- Identify weak or quantum-vulnerable cryptography
- Assess compliance and cryptographic posture

Automate lifecycle operations
- Automate rotation, renewal, and revocation
- Enforce policy-driven lifecycle management
- Reduce outages from expired certificates and unmanaged keys

Secure NHIs and AI systems
- Deliver short-lived credentials dynamically
- Secure workloads, APIs, and agentic systems
- Enforce least-privilege access at machine speed

Enable crypto-agility and PQC readiness
- Prioritize remediation efforts
- Support coordinated cryptographic modernization
- Prepare for quantum-safe transitions

FOUR inc.

IBM Platinum Partner