Vault

HashiCorp
an IBM Company

Quick Reference for Prospecting

Vault is the market leading secrets management solution. Secrets are a set of credentials that grant authentication or authorization to a system. These include tokens, usernames and passwords, certificates, encryption keys and other sensitive data.

Enterprises often grapple with secrets sprawl, which means that they have lost control over where their secrets are located, creating risk of data exposure and breach. To ensure the security and auditability of secrets, it is imperative that enterprises understand who has access to secrets, who has been using them, and how to periodically rotate them.

Vault was built to address the secrets spawl challenge by enabling customers to secure, store and tightly control access to secrets. The product provides an extensive set of capabilities to standardize the workflow and manage the entire lifecycle of secrets management from acquisition, to rotation, to revocation, to auditing.

Vault is one of three products that enable the Security Lifecycle Management framework. This approach enables organizations' platform and security teams to have the systems in place to inspect and protect the sensitive elements of their environment.

Products in the Security Lifecycle Framework:

- **Vault:** machine authentication and authorization
- **Boundary:** human-to-machine access
- **Consul:** machine-to-machine access or service networking

Who to Sell to & Why

Target Customer Roles

- ***Decision Makers*:** Head of Platform Team, Chief Information / Technology Officer (CIO / CTO)
- ***Influencers:*** Chief Information Security Officer (CISO), Security Team, Compliance Team

Pain Points

- **Speed/efficiency** –
  - Tool sprawl, facilitating developer discovery/reuse/self-service
  - Policy enforcement and creating built-in, secure-by-default posture that extends to developer workflows
  - Reducing manual processes
  - Finding people with the right skills
- **Risk/GRC** –
  - Deciding on technologies and ensuring their integration, performance, and security
  - Providing visibility and evidence that security is improved and IT is within compliance for standards and control
  - Managing cloud costs
- **Deliver business value** –
  - Securing executive sponsorship and funding
  - Identifying the right actions and metrics to show improvements and aligning those to corporate goals

Seeking Use Cases

- Secrets management
- Certificate management
- Key management
- Data protection

What to Ask & Listen For

Prospecting Questions

- Do you have a sense of how many credentials are living in plain text across your estate?
- Do you have a challenge with secret sprawl?
- How often do you rotate secrets? What are the main challenges with secrets/credential rotation?
- How close are you to implementing a zero trust and least privileged architecture? Do your devs have more access than they should?
- When (not if) you get hacked, will an attacker be able to move laterally through your estate?
- How does your team execute audits? Are there challenges in this process?

Entry Points to Listen for

- "We don't have a good handle on secrets today. We don't track where they are and who has access to them."
- "We don't have a standardized way of rotating secrets. It's done manually/ad hoc."
- "I face a lot of pressure to ensure our policies are auditable and are compliant."
- "We have many disparate systems, and audit preparation requires manual effort."
- "Any tool I use for secrets management needs to integrate with CI/CD pipelines."
- "I'm concerned about cybersecurity threats, breaches and data privacy."

Leverage Help to Close a Deal

- Vault Sales Kit
- Sales Qs: #hashicorp-ama-sales
- Technical/product Qs: #hashicorp-ama-tech

How to Respond

Capabilities

- **Dynamic secrets:** Reduce risk with dynamic secrets that are generated on demand, so they can be configured to each unique application, machine or user for just-in-time, short-lived credentials
- **High availability (HA):** Enable multi-server model for HA for disaster recovery strategy
- **Secrets sync:** Consolidate credentials, reduce secrets sprawl across multiple cloud service providers, and automate secrets policies across services
- **Performance replication:** Deliver Vault cluster to multiple regions
- **Access control:** Granular policy and governance requirements with configurable multi-factor authentication
- **Proactively prevent secret sprawl:** Automate discovery of unmanaged secrets
- **Remediate risk and encrypt data seamlessly:** Manage certificate rotation and cryptographic keys, and leverage encryption as a service and transparent database encryption

Benefits

- **Reduce Risk:** Eliminate need for static, hard-coded credentials by centralizing secrets management, with over 100K edge devices supported
- **Improve Speed:** Spend 50% less time encrypting sensitive data with an automated and scalable process
- **Control Costs:** 0% unplanned downtime, enabling developers to programmatically consume and update secrets

IBM