



THE SECURITY GAP MOST ORGANIZATIONS DON'T KNOW THEY HAVE

Protecting Secrets, Applications, and AI with IBM HashiCorp Vault

Thursday, September 17, 2026

GENERATIVE AI

• DATA & ANALYTICS

• MIGRATION & MODERNIZATION

• SaaS DEVELOPMENT

TODAY'S CONVERSATION

WHAT WE'LL COVER

- ✓ Why secrets management has become a strategic security priority
- ✓ The people, process, and technology challenges behind secrets sprawl
- ✓ How cloud, hybrid environments, and AI are changing the risk landscape
- ✓ Where organizations should start: Crawl, Walk, Run
- ✓ Practical next steps for building a more secure foundation

MEET OUR SPEAKERS



Michael Wood

Global Field CTO
HashiCorp



Darren Mills

Chief Technology Officer
CleanSlate Technology Group



Hosted by **Branden Voegerl** • CleanSlate Technology Group

WHY SECRETS MANAGEMENT MATTERS NOW

The risk is growing because the environment is growing

Secrets now live across every layer of the modern stack:



Applications



Cloud platforms



CI/CD pipelines



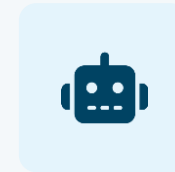
Infrastructure-as-Code



APIs



Databases



AI agents & automation

THE BUSINESS IMPACT

Secrets management is not just a technical issue



Security exposure

Every leaked credential is a direct path in.



Compliance readiness

Auditors expect control, rotation, and proof.



Developer productivity

Manual secret handling slows every team.



Incident response

Fast revocation limits blast radius.



Cloud modernization

Migrations stall without a secrets strategy.



AI adoption

Foundational control must precede scale.

PEOPLE - WHO OWNS SECRETS MANAGEMENT?

Secrets management requires shared ownership

No single team owns it end to end. These stakeholders share responsibility:



Security



Infrastructure



DevOps



**Platform
Engineering**



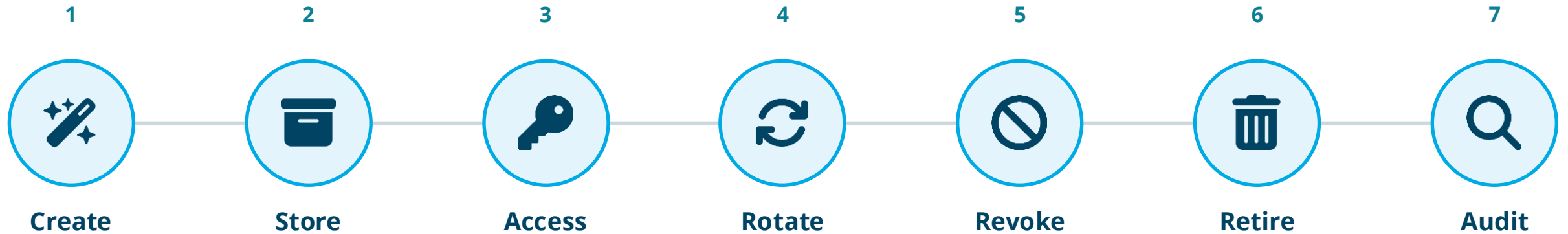
**Application
teams**



**Compliance /
Risk**

PROCESS - THE FULL SECRET LIFECYCLE

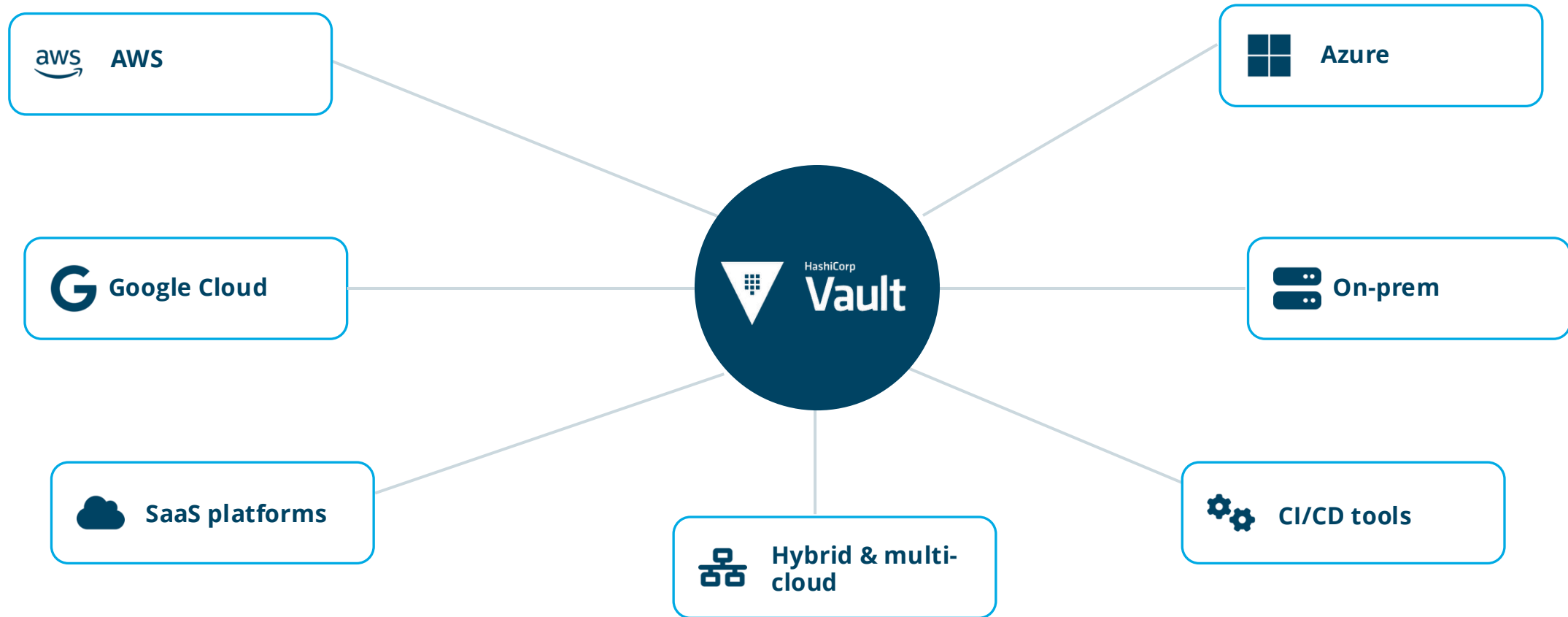
It is more than storing the secret securely



Ownership of the entire lifecycle, not just secure storage, is where most programs fall short.

TECHNOLOGY- WHY VAULT IN A CLOUD WORLD?

Cloud-native does not always mean centralized



AI & AUTOMATION CHANGE THE STAKES

AI increases the need for controlled access

As AI agents and automation reach more systems, control must be explicit and provable:



What can access
sensitive systems



When access
is granted



How long
access lasts



How access
is revoked



How activity
is audited

An example of core protections.

Agent Trust

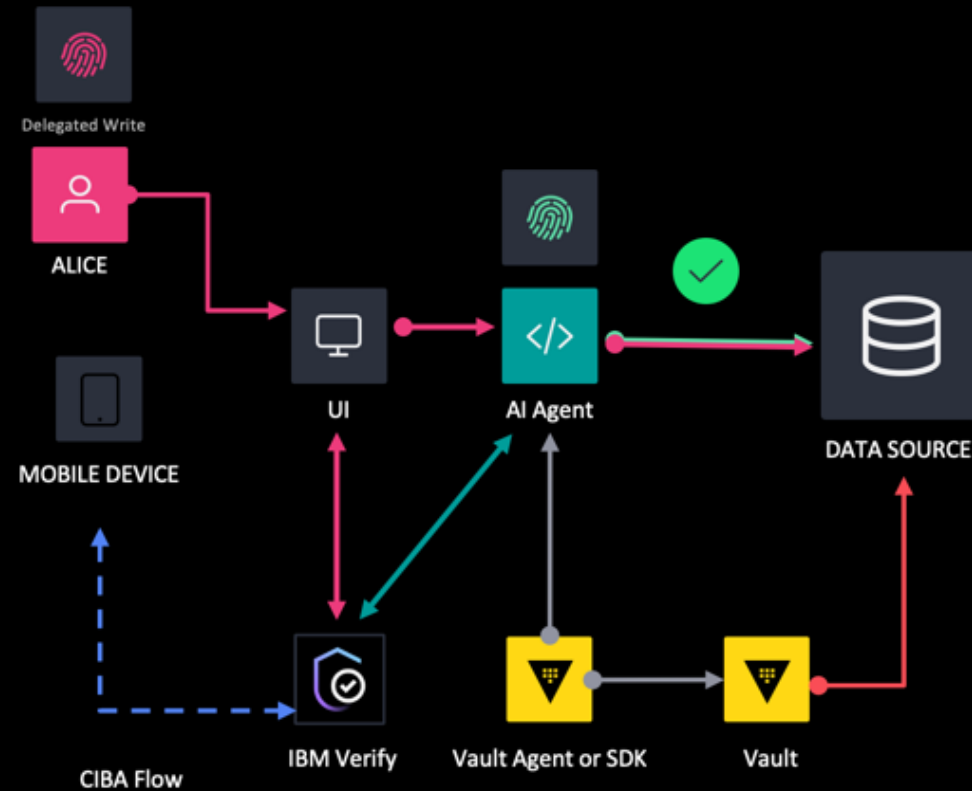
Use-case

Agents require elevated privileges for actions such as banking operations, agentic shopping, document authoring, HR functions (onboarding/offboarding employees).

Implementation pattern

- User context required
- User consent and delegation required
- OAuth2.0 CIBA authorization code flow with user consent, optionally using RAR for task specific fine-grained permissions
- JWT token containing user context, session ID, and delegation claims
- Explicit Token TTL and revocation on session termination
- Vault creates dynamic credentials in data sources for user content access

Agentic Runtime Security: Personalized Personalized and privileged agents



CRAWL

CRAWL

WALK

RUN

Build visibility and control

- ✓ Inventory secrets across the environment
- ✓ Centralize high-value secrets
- ✓ Establish clear ownership
- ✓ Implement identity-based access
- ✓ Eliminate hard-coded credentials
- ✓ Establish basic policies
- ✓ Start audit visibility



Reactive → Controlled

Establish visibility and basic control — know what you have and who owns it.

WALK

CRAWL



WALK



RUN

Reduce manual effort and improve consistency

FOCUS AREAS

- ✓ Centralized management
- ✓ Automated rotation
- ✓ Faster revocation
- ✓ Application onboarding
- ✓ Policy enforcement
- ✓ Incident reduction

METRICS TO WATCH

- 1 % of secrets centrally managed
- 2 % automatically rotated
- 3 Hard-coded secrets discovered
- 4 Time to revoke credentials
- 5 Applications onboarded
- 6 Long-lived credentials reduced



Repeatable & Consistent

Automation and secure defaults replace trusting people to do it manually.

RUN

CRAWL



WALK



RUN

Move toward dynamic, policy-driven access



Dynamic secrets



Short-lived credentials



Automated rotation



Policy-based access



Identity-driven controls



Strong auditability



Secure AI & automation patterns



Dynamic & AI-Ready

Access is granted, proven, and revoked automatically, the foundation for AI.



RAPID FIRE QUESTIONS



CleanSlate
TECHNOLOGY GROUP

AUDIENCE Q&A

What questions do you have for Michael and Darren?



CleanSlate
TECHNOLOGY GROUP

LET'S CONTINUE THE CONVERSATION

CleanSlate can help you assess:

- Where secrets live today
- Current risk and exposure
- Ownership and governance gaps
- Automation opportunities
- Readiness for Vault adoption
- Next steps for secure modernization



IBMSalesLead@cleanslatetg.com

Scan or email to schedule a follow-up assessment.

