ARCTIQ

Architect Transformation

Arctiq Acceleration Program (AAP) for HashiCorp Boundary and Vault

Platform Engineering

Elevating Security with HashiCorp Boundary and Vault Integration

HashiCorp

HashiCorp Boundary stands as a robust solution, offering both security and flexibility in managing access to critical systems while adhering to the principle of least privilege. Its centralized and structured approach enhances security measures and effectively reduces the potential attack surface. Embodying the principles of Zero Trust Security, HashiCorp Boundary operates on a "Trust Nothing. Authenticate and Authorize Everything" basis, providing a Privileged Access Management (PAM) solution that ensures comprehensive security measures. The integration of HashiCorp Boundary and Vault is pivotal in realizing the core principle of Zero Trust Security, fortifying access control measures and bolstering overall security protocols. Arctiq leverages this integration to elevate security standards for our clients, ensuring robust protection for their critical systems and data assets.

Is AAP right for you?

Overcoming the Learning Curve

Boundary, though powerful, presents a steep initial learning curve for teams as they familiarize themselves with this relatively new technology.

Strategic Deployment in Complex Networks

Deploying Boundary within intricate network architectures demands meticulous planning and configuration adjustments to ensure seamless integration and optimal performance.

Navigating Complex Integrations

Integrating Boundary with existing identity and access management (IAM) systems, infrastructure, and applications poses a complex challenge, requiring careful coordination and expertise to achieve cohesive integration.

Securing Critical Systems with PAM Tools

Privileged Access Management (PAM) tools play a crucial role in the security ecosystem, ensuring access to critical systems is tightly controlled and monitored, safeguarding against potential breaches and unauthorized access.

Common Challenges

- Limited scalability and increased attack surface
- Secrets are often sprawled, shared over collaboration tools and may be saved in log files
- Challenges with traditional privileged access workflow
- Remote user access often relies on static credentials for accessing resources
- Modern Infrastructure is highly scalable requiring dynamic credentials accessing applications

HashiCorp Boundary

HashiCorp Vault

Your Zero Trust Maturity Journey with Arctiq

Arctiq Acceleration Program is a service package developed to be a guide for your ZeroTrust Maturity journey. Our approach is specifically designed to assess and progress yourenvironment and your organization's skill maturity utilizing a Minimum Viable Product (MVP) methodology. This approach enables guided adoption of HashiCorp Boundary and Vault enhancing the probability of successfully implementing and operationalizing this PAM solution across the entire organization.

Arctiq Starter Package Program Overview

Duration
4-8 weeks*

Phase 1

Discovery and Interviews

- Review existing architecture and design
- Validate use cases
- Migration pattern from current PAM methods
- Recommend best practices

Phase 2

Deployment

- Generate IaC assets for Boundary and Vault
- Configure Vault/Boundary per use cases
- Create reusable assets and patterns

Phase 3

Configuration & Hand-Off

- Onboarding teams, users, and private hosts on Boundary
- Knowledge transfer
- Project documentation, review, and walkthrough

*Exact timeline and pricing will be determined based on availability, readiness, and scope

Business Impact

- Enhanced security and compliance
- Improved operational efficiency
- Cost savings and resource optimization
- Scalability and flexibility
- Reduced operational risks
- Robust security measures increase customer trust

Use Cases

Zero Trust Access

- On demand access
- Continuous authentication
- Admin-defined authorization
- Authentication of user access and actions in a granular manner

Multi-cloud Access

- Centralized layer of identity-based authentication and authorization
- Simplified management of different access workflows by streamlining access across different platforms

Single Sign-On (SSO) with Integrated Secrets Management

- Boundary supports SSO with trusted identity providers like Azure Active Directory, Auth0, and Okta
- Once authenticated, users can create sessions with integrated credential management from HashiCorp Vault without the need for re-authentication

Session Monitoring /Recording

- Security administrators can track user access and actions
- Session logs accessible via the Boundary administrator UI and integrated with BI and SIEM tools
- Session recordings on targets for later review using a browser-based session player is available for admins

Partner with Arctiq to harness the power of the AAP for seamless integration and optimization of HashiCorp Boundary and Vault.

Book a consultation