**Summary:** To align our marketing and sales strategies, FY26 will introduce a refreshed approach to ensure consistent messaging and positioning across Product Marketing, Integrated Campaigns, and Sales Plays.

The focus for FY26 will prioritize presenting solutions as the entry point for customer conversations, emphasizing our top-down value proposition and the differentiated value we deliver as a platform service provider. This shift moves beyond single-product discussions, aiming to elevate the quality of account-level conversations. The ultimate goal is to ensure our GTM activities effectively nurture customers toward understanding and leveraging the comprehensive solutions we offer.

There is one overarching MPF for Infrastructure Cloud and three Value Pillars:Accelerate Innovation and Efficiency, Strengthen Security and Governance and Optimize Cloud Operations and ROI. This MPF represents the double click into the Strengthen Security and Governance Value Pillar and presents three Discussion topics that allow for deeper conversations with TDM, BDM, and Practitioners.

| **Created:** Nov 26, 2024  **Owner:** Jackson Connell | **Supporting Links**  [MPF Accelerate Innovation and Efficiency](https://docs.google.com/document/d/1KjG263IzHASWF8tIxkKVVOKOoTIdcOtmoIU9tJTHdr4/edit?usp=sharing)  [MPF Strengthen Security and Governance](https://docs.google.com/document/d/1DUDIGxNkr2W0nqjupMVtg3UdlnAbl4GVvycoUmd4_3c/edit?usp=drive_link)[(this doc)](https://docs.google.com/document/d/1KjG263IzHASWF8tIxkKVVOKOoTIdcOtmoIU9tJTHdr4/edit?usp=sharing)  [MPF Optimize Cloud Operations and ROI](https://docs.google.com/document/d/1-shVUKk_bakgjfwUO_QadraflzWPoY38ShRNcyy5CG4/edit?usp=drive_link)  Campaign Briefs:  [BDM](https://docs.google.com/document/d/1rgoPFxaKNhPjiv9l1g9CFPt7GJGDyif2CE8xD3LEPvc/edit?usp=sharing); [TDM](https://docs.google.com/document/d/1hn_zFPpzbCHt5LYE5U2cZg8wTPOwmLqA_4zp9kDTzuM/edit?usp=sharing);  [Practitioner](https://docs.google.com/document/d/1ZpEwD93Og2x53Op-YfhFFmF42oAAOSgzxoHJSS2DK30/edit?usp=sharing) |
| --- | --- |

## FY26 Messaging and Positioning Framework - **Strengthen Security and Governance**

| **Risk: Strengthen Security and Governance** | | | | |
| --- | --- | --- | --- | --- |
| **Brand Promise** | HashiCorp will unify, secure, and govern your entire digital estate, delivering scalable solutions to mitigate cybersecurity, compliance, and business risk across hybrid and multi-cloud environments. | | | |
| **Mission** | To empower organizations to navigate the complexities of hybrid and multi-cloud environments securely through unified, automated solutions that strengthen security, ensure compliance, and safeguard sensitive data, enabling businesses to innovate faster and with confidence. | | | |
| **Positioning Statement** | For C-suites managing the complexities of hybrid and multi-cloud adoption, HashiCorp delivers comprehensive solutions to reduce business risk, streamline compliance, and scale operations with confidence. | | | |
| **Tone of Voice** | Professional and business oriented | | | |
| **Elevator Pitch** | In today’s complex hybrid and multi-cloud environments, HashiCorp reduces business risk and ensures compliance by securing sensitive data across all digital assets. With centralized visibility, automated policies, and secure access, we empower businesses to mitigate threats, streamline compliance, and innovate at scale. | | | |
| **Discussion Pillars**  **Strengthen Security and Governance** | Emphasizing security, compliance, and risk mitigation, these pillars address key scenarios and use cases, aligning with HashiCorp’s mission to deliver secure, scalable, and unified solutions for hybrid and multi-cloud environments. They guide organizations in navigating complex digital estates with confidence and agility. | | | |

## 

| **Ideal Customer Profile** | |
| --- | --- |
| **Firmographics:** | **Industries:** Financial Services, Healthcare, Government, Technology, Retail, Energy  **Company Size**: Large enterprises & highly regulated industries (5,000+ employees)  **Cloud Maturity:** Hybrid and multi-cloud deployments, high compliance requirements |
| **Key Buying Personas:** | **BDM:** CISO, CIO, Head of Risk & Compliance  **TDM:** Head of Cloud Security, Security Architect, DevSecOps Lead  **Practitioner:** Security Engineers, Compliance Analysts, Cloud Security Teams |
| **Common Business Challenges:** | * Security and compliance gaps due to rapid cloud expansion * Mismanaged secrets and lack of centralized access controls * Audit complexity and difficulty enforcing policy as code * Difficulty securing multi-cloud & hybrid environments |
| **Buying Triggers:** | * Security breaches or compliance audit failures * Adoption of Zero Trust Architecture (ZTA) mandates * Need for secrets management & dynamic access controls * Regulatory pressures (PCI-DSS, SOC 2, GDPR, HIPAA, FedRAMP) |
| **Solution Fit Criteria:** | * Teams looking to standardize security automation * Organizations needing centralized policy enforcement across clouds * Companies struggling with identity & access management (IAM) at scale * Businesses wanting to reduce cyber risk & security debt |

## 

| **Risk: TDM | Strengthen Security and Governance** | | | | |
| --- | --- | --- | --- | --- |
| **TDM Mix &  Messaging One-Liner** | **TDM Titles:**  Key audiences and their titles are identified further below and for a full list of TDM titles refer to [this](https://docs.google.com/spreadsheets/d/19qIyfqBJgjSWxv6Vey2Ol7hTGyTpUd3-Z_D_OB-aRao/edit?gid=144271512#gid=144271512)  **OneLiner:** Unify your security and compliance architecture across complex multi-cloud and on-prem environments to reduce risk, streamline governance, and enable scalability. | | **Problem Statement:** Managing security and compliance at scale across distributed, ephemeral, and multi-cloud environments has become increasingly complex, creating gaps in governance and exposing the organization to heightened risk. **Solution Overview:** HashiCorp delivers a central control plane that enables seamless security and compliance governance across all environments, helping mitigate risks, enforce policies, and protect sensitive data throughout your hybrid cloud estate. | |
| **Discussion Pillars** | **Proactive  Risk Management** | **Enhanced Compliance Posture** | | **Advanced Zero  Trust Cloud Practices** |
| **Pillar Focus** | Reduce risks across public cloud, private cloud, and on-premise environments by establishing secure access, reducing manual processes with automated policies and workflows, and centralizing visibility. | Maintain consistent governance and compliance across hybrid and multi-cloud environments through automation, including automated workflows, and policy standardization. | | Implement advanced zero trust best practices across your cloud estate with a focus on trusting nothing and authenticating everything, plus ensure data is protected should a breach occur.  - Leverage identity based security and access to ensure a stronger security posture.  - Protect sensitive data across all environments with advanced encryption, key lifecycle management, and automated discovery of vulnerabilities. |
| **Market Drivers** | Many organizations only discover their security gaps after a breach occurs, leading to costly damages and reputational harm. Instead of mitigating risks proactively, companies are stuck in a reactive security posture, increasing their exposure to financial and operational disruption.   * Comply with SEC Cybersecurity reporting mandates for public companies: With growing regulatory pressure, publicly traded companies must demonstrate cybersecurity preparedness or face material financial and legal consequences. * Reduce the cost of breaches by preventing misconfigurations: Security missteps, such as mismanaged credentials and open access policies, continue to be the leading cause of breaches, costing organizations millions annually. | Organizations struggle to maintain compliance across their cloud environments, often due to a lack of visibility and standardized governance controls. Unclear policies lead to audit failures, fines, and operational disruptions.   * Meet compliance mandates and pass annual audits with confidence: Regulations such as SOC 2, GDPR, HIPAA, and PCI DSS require continuous monitoring and policy enforcement across hybrid and multi-cloud environments. * Reduce the risk of non-compliance penalties: Without centralized governance and automated policy enforcement, organizations risk fines and reputational damage from regulatory non-compliance. | | Many enterprises still rely on legacy security models that were designed for traditional, perimeter-based architectures rather than dynamic, cloud-native environments. This reliance on outdated security practices creates a roadblock to cloud adoption and increases attack surfaces.   * Overcome firewall dependency—adopt identity-driven security: Cloud-based infrastructure requires a shift from perimeter-based security to Zero Trust models, where access is dynamically verified based on identity and least-privilege principles. * Address security challenges from cloud sprawl and hybrid adoption: Organizations struggle with securing multi-cloud and hybrid environments, where inconsistent security controls leave gaps in visibility and enforcement. |
| **Pillar Why-it-Matters** | As cloud environments expand, organizations face increased vulnerabilities and governance complexities. This pillar mitigates risks by addressing security gaps, automating remediation, and enforcing consistent governance across all environments. | Meeting regulatory and compliance requirements is essential for avoiding fines and maintaining customer trust. By standardizing policies and automating compliance workflows, this pillar reduces overhead while ensuring adherence to regulations. | | As hybrid cloud estate threat surfaces continue to grow and sensitive data becomes a prime target for attackers, organizations need proactive security measures and robust encryption to ensure data integrity and confidentiality. |
| **Piller Key TDM Audiences** | CIO, CISO, VP of Infrastructure, Head of Cloud Operations | CIO, Head of Platform Team, VP of Infrastructure, Head of Cloud Operations, CISO | | Head of Platform Team, VP of Infrastructure, Head of Cloud Operations, CISO |
| **Scenario 1**  **Scenario Outcome**  **& Use Cases** | **Mitigate Risk Within Complex Cloud Environments**  Reduce risk across public cloud, private cloud, and on-premise environments  **Prioritization Rating: 0**  **Outcome:** Reduce data breach risks by 40%\* through centralized policy enforcement and automated secrets rotation.  **1. Centralized Visibility & Control** - Address the primary areas of risk in hybrid cloud development pipelines with a single system of record for security and infrastructure and Centralized Policy as Code to enforce consistent security and governance.  **Product - Vault, Terraform**  **2. Vulnerability and Patch Management** - Identify, prioritize, and mitigate vulnerabilities quickly and through automation for CI/CD pipelines across any infrastructure.  **Product - Terraform, Packer**  **3. Machine Identity & Trust** - Replace human tasks with centralized, automated secrets and identity management to eliminate risk and standardize lifecycle management for machine identities.  **Product - Vault, Terraform**  **4. Secure Human Access** - Authenticate and authorize users to development pipelines while ensuring least privileged access to sensitive systems and proper governance of human identities  **Product - Vault, Boundary, Terraform**  **Partner -** Automated scanning of application code within a development pipeline with PANW Prisma Cloud Code Scanning  Pre-written Sentinel policies for AWS across security, compliance, and operational efficiency  **Product - Terraform** | **Advance Governance Practices**  Enhance governance and compliance across all cloud environments  **Prioritization Rating: 0**  **Outcome:** Achieve 100%\* audit success with pre-built compliance workflows and policy-as-code governance.  **1. Centralized Control & Visibility** - Maintain compliance within all cloud environments through policy as code guardrails both pre and post deployment, and gain greater visibility through a single system of record for security and infrastructure  **Product - Vault, Terraform**  **2. Compliance Readiness** - Automated compliance audits with logging and monitoring of secrets access, activity history, and session recording.  **Product - Vault, Radar, Boundary, Terraform, Consul**  **3. Automated Secrets Lifecycle Management** - Dynamic secrets and automated secrets rotation based on least-privilege access  **Product - Vault, Radar, Boundary, Terraform**  **4. Shift Compliance Requirements Left -** Leverage Secure and Compliant Images, Modules and Registries that are prebuilt to be compliant.  **Product - Vault, Terraform, Packer, Waypoint**  **5. Monitor User Compliance** - Actively monitor all users and sessions to ensure proper compliance and terminate access when suspicious activity is reported. **Vault, Boundary, Consul, Terraform**  **6. Vulnerability and Patch Management** - Identity, prioritize, and mitigate vulnerabilities  **Product - Vault, Terraform, Packer**  **Partner -** Simplify policy adoption with pre-written Sentinel policies for AWS  **Product - Terraform** | | **Leverage Identity-based Access Controls**  Connect machines, people, and networks using trusted identities  **Prioritization Rating:1**  **Outcome:** Improve secure access efficiency by 25% through automated machine-to-machine identity verification.  **1. Dynamic and Ephemeral Credentials** - Keep up with a dynamic and ephemeral environment by instituting identity-based controls to generate, rotate, or revoke secrets on demand or automatically.  **Product** **-** **Vault**  **2. Machine Identity & Trust** - Authenticate and authorize every machine-to-machine access request based on fine-grained identity and access controls and MFA governance.  **Product - Vault, Terraform**  **3. Secure Human Access** - Ensure the right roles gain access to the right services and least privilege and MFA access is enforced.  **Product - Vault, Boundary, Terraform**  **4. Application and Service Authentication** - Discover, schedule and securely connect any service across any runtime with identity-based service networking.  **Product - Vault, Consul, Nomad**  **Partners -**Dynamic secrets generate just-in-time, short-lived credentials for AWS, Azure and Google Cloud to access resources securely  **Partners -** Use our trusted partners (Okta, Duo, PingID, Auth0 etc.) for authentication, SSO, and context-based access controls as well as multi-factor governance based granular access. |
| **Scenario 2**  **Scenario Outcome**  **& Use Cases** | **Detect & Respond to Threats Efficiently**  Identify suspicious activity across cloud environments and automatically remediate potential threats.  **Prioritization Rating: 3**  **Outcome:** Decrease response time to security incidents by 30% through predefined workflows and drift detection alerts.  **1. Centralized Visibility & Control** - Address the primary areas of risk within a cloud environment with a single system of record for security and infrastructure  **Product - Vault, Terraform**  **2. Continuous Security Monitoring** - Automatically scan code repositories, monitor privileged access sessions, and service registries  **Product - Vault, HCP Vault Radar, Terraform**  **3. Streamlined Remediation Workflows** - Leverage pre-defined developer templates as well as workflows for both reactive and proactive threat remediation  **Product - Vault, Terraform, Waypoint**  **4. Enforce Policy At Scale** - Integrate policy as code directly into standardized images and workflows  **Product - Vault, Terraform, Packer**  **5. Privileged Session Monitoring** - Actively monitor all users and sessions, track activity history, and prevent tampering of session recording policies  **Product - Boundary**  **6. Drift Detection And Alerts** - Continuously monitor for infrastructure changes against expected state  **Product - Terraform** | **Adopt Holistic Secrets governance**  End-to-end holistic management of secrets to govern and comply with application, identity, and sensitive data regulations.  **Prioritization Rating: 1**  **Outcome:** Enhance compliance readiness by 50% through automated secrets lifecycle management and centralized logging.  **1. Dynamic Secrets For Least Privileged Access** - Ease compliance and management of secrets by generating/expiring them on demand and Just In Time (JIT) for today’s ephemeral environments.  **Product - Vault**  **2. Secrets Rotation And Expiration Policies** - Govern secrets easily with the right level of policies, and protect them automatically by rotating or revoking them on demand or upon lease end.  **Product - Vault,** **Terraform**  **3. Audit Logging And Monitoring Of Secrets Access** - Support compliance needs with customizable audit log filtering  **Product - Vault, Boundary**  **4. Integration With Identity Providers** - Use any trusted identity provider for authentication, SSO, and context-based access controls as well as multi-factor governance based granular access.  **Product - Vault, Boundary, Consul, Terraform**  **Partner** - Centralize the management and policy of secrets with secret sync, allowing users to sync secrets to various destinations, including secrets managers from AWS, Google Cloud, Microsoft Azure, GitHub and Vercel.  **Product - Vault** | | **Secure Sensitive Data Across All Environments**  Protect your data with future-proof encryption and secrets management.  **Prioritization Rating: 2**  **Outcome:** Reduce data theft risks by 35% with persistent encryption for data in motion and at rest.  **1 - Advanced data encryption and protection -** Secure your data across any environment with transparent encryption, format preservation, data masking and tokenization, and also prepare for the future with quantum safe encryption mechanisms.  **Product - Vault**  **2 - Data protection as a service**  Speed up your data protection with encryption as a service and encryption that includes fine grained permissions for specific users and applications that access or require that security**.**  **Product: Vault, Boundary**  **3** - **Lifecycle management of sensitive data** - Automate and dynamically create keys and certificates and manage the lifecycle of your most important data.  **Product - Vault, Terraform**  **4. Automated Secrets Discovery And Remediation** - Detect unmanaged and leaked secrets and remediate via seamless integrations and predefined workflows  **Product - HCP Vault Radar**  5. **Partner** - Centralize the management and policy of secrets with secret sync, allowing users to sync secrets to various destinations, including Secrets sync which lets users manage multiple external secrets managers, including secrets managers from AWS, Google Cloud, Microsoft Azure, GitHub and Vercel.  **Product - Vault** |

## 

| **Risk: BDM | Strengthen Security and Governance** | | | | |
| --- | --- | --- | --- | --- |
| **BDM Mix &**  **Messaging One-Liner** | **BDM Titles:** Key audiences and their titles are identified further below and for a full list of BDM titles refer to [this](https://docs.google.com/spreadsheets/d/19qIyfqBJgjSWxv6Vey2Ol7hTGyTpUd3-Z_D_OB-aRao/edit?gid=1757921089#gid=1757921089)  **OneLiner:** Reduce business risk from insecure cloud environments while ensuring compliance. | | **Problem Statement:** Leveraging the cloud has become a necessity, but it often introduces additional risk to the business and can complicate critical compliance initiatives.  **Solution Overview:** HashiCorp can make your cloud environment more secure and simplifies compliance management, reducing business risk and ensuring your operations meet critical regulatory standards across all cloud and on-prem environments. | |
| **Discussion Pillars** | **Risk Management** | **Compliance Posture** | | **Data Protection** |
| **Pillar Focus** | Reduce risks across public cloud, private cloud, and on-premise environments by establishing centralized visibility, automated policies, and secure access. | Maintain consistent governance and compliance across hybrid and multi-cloud environments through automation and policy standardization. | | Protect sensitive data across all environments with advanced encryption, key lifecycle management, and automated discovery of vulnerabilities. |
| **Pillar Why-it-Matters** | As cloud environments expand, organizations face increased vulnerabilities and governance complexities. This pillar mitigates risks by addressing security gaps, automating remediation, and enforcing consistent governance across all environments. | Meeting regulatory and compliance requirements is essential for avoiding fines and maintaining customer trust. By standardizing policies and automating compliance workflows, this pillar reduces overhead while ensuring adherence to regulations. | | As sensitive data becomes a prime target for attackers, organizations need robust encryption and proactive security measures to ensure data integrity and confidentiality. |
| **Piller Key BDM Audiences** | CIO | COO, CIO, CEO | | CIO |
| **Scenario 1**  **Scenario Outcome** | **Mitigate Risk Within Complex Cloud Environments**  Proactively reduce risk across public cloud, private cloud, and on-premise environments with automated access, secrets management, and consistent governance.  **Outcome:** Reduce data breach risks by 40%\* through centralized policy enforcement and automated secrets rotation.  **Prioritization Rating: 0** | **Improve and Optimize Compliance Posture**  Streamline governance and compliance across all cloud environments with robust policy management and advanced monitoring capabilities.  **Outcome:** Achieve 100%\* audit success with pre-built compliance workflows and policy-as-code governance.  **Prioritization Rating: 0** | | **Safeguard your Digital Assets**  Protect your data with future-proof encryption and secrets management.  **Outcome:** Reduce data theft risks by 35%\* with persistent encryption for data in motion and at rest.  **Prioritization Rating: 1** |
| **Scenario 2**  **Scenario Outcome**  **& Use Cases** | **Proactive Threat Management**  Identify suspicious activity across cloud environments with continuous monitoring and efficiently remediate threats with scalable policy enforcement.  **Outcome:** Decrease response time to security incidents by 30% through pre-defined workflows and drift detection alerts.  **Prioritization Rating: 3** | **Streamline Secrets Management**  End-to-end holistic secrets management to maintain compliance and protect applications, identities, and sensitive data  **Outcome:** Enhance compliance readiness by 50% through automated secrets lifecycle management and centralized logging.  **Prioritization Rating: 2** | | **Identity-based Access Controls**  Securely connect machines, people, and networks using trusted identities, precise access controls and multi-factor authentication.  **Outcome:** Improve secure access efficiency by 25% through automated machine-to-machine identity verification.  **Prioritization Rating: 2** |

## 

| **Risk: Practitioner | Strengthen Security and Governance** | | | | |
| --- | --- | --- | --- | --- |
| **Prac Mix &   Messaging One-Liner** | **Practitioner Titles:** Key audiences and their titles are identified further below and for a full list of Practitioner titles refer to [this](https://docs.google.com/spreadsheets/d/19qIyfqBJgjSWxv6Vey2Ol7hTGyTpUd3-Z_D_OB-aRao/edit?gid=1487225902#gid=1487225902)  **OneLiner:** Enable faster and more secure deployments while streamlining compliance requirements within distributed and ephemeral cloud environments. | | **Problem Statement:** Platform engineers are struggling to meet strict security and compliance requirements while delivering an integrated platform that enables developers to innovate and deliver business value.  **Solution Overview:** HashiCorp provides platform engineers with a unified control plane to simplify risk mitigation, automate compliance workflows, and maintain governance at scale. | |
| **Discussion Pillars** | **Risk Management** | **Compliance Posture** | | **Data Protection** |
| **Pillar Focus** | Streamline security and governance workflows across public cloud, private cloud, and on-premise environments. | Simplify governance and compliance at scale, across hybrid and multi-cloud environments through automation and policy standardization. | | Protect sensitive data across all environments with advanced encryption, key lifecycle management, and automated discovery of leaked secrets. |
| **Pillar Why-it-Matters** | As cloud environments expand, organizations face increased security and governance complexities. This pillar mitigates risks by addressing security gaps, automating remediation, and enforcing consistent governance across all environments. | Meeting regulatory and compliance standards is a requirement for platform teams. By standardizing policies and automating workflows, this pillar simplifies achieving and maintaining compliance. | | As sensitive data becomes a prime target for attackers, organizations need robust encryption and proactive security measures to ensure data integrity and confidentiality. |
| **Piller Key Audiences** | Cloud Engineer, Infrastructure Engineer, Platform Engineer | Cloud Engineer, Infrastructure Engineer, Platform Engineer | | Cloud Engineer, Infrastructure Engineer, Platform Engineer |
| **Scenario 1**  **Scenario Outcome** | **Efficient Risk Management in Complex Environments**  Reduce security risks across all environments with centralized policy as code, simplified access controls, and proactive vulnerability management  **Outcome:** Reduce data breach risks by 40%\* and free up resources through centralized policy enforcement and automated secrets rotation.  **Prioritization Rating: 2** | **Improve Compliance Posture**  Maintain governance and compliance across cloud environments with centralized policy as code, automated audit logging, and robust secrets lifecycle management.  **Outcome:** Achieve 100%\* audit success with pre-built compliance workflows and policy-as-code governance.  **Prioritization Rating: 0** | | **Secure Sensitive Data Across All Environments**  Protect your cloud environments with advanced encryption as a service, RBAC for sensitive systems, and automated secrets discovery.  **Outcome:** Reduce data theft risks by 35%\* with persistent encryption for data in motion and at rest.  **Prioritization Rating: 1** |
| **Scenario 2**  **Scenario Outcome**  **& Use Cases** | **Threat Detection and Incident Response**  Identify suspicious behavior and insecure infrastructure across your environment to streamline risk mitigation.  **Outcome:** Decrease response time to security incidents by 30% through pre-defined workflows and drift detection alerts.  **Prioritization Rating: 3** | **Centralized Secrets Management**  End-to-end secrets management including dynamic secrets, rotation, and revocation to protect applications, identities, and sensitive data  **Outcome:** Enhance compliance readiness by 50% through automated secrets lifecycle management and centralized logging.  **Prioritization Rating: 0** | | **Identity-based Access Controls**  Enable secure connections between machines, people, and networks using trusted identities, seamlessly integrated into your workflows.  **Outcome:** Improve secure access efficiency by 25% through automated machine-to-machine identity verification.  **Prioritization Rating: 0** |

| Source Information | | | | |
| --- | --- | --- | --- | --- |
|  | **Reduce data breach risks by 40% through centralized policy enforcement and automated secrets rotation**   * Industry averages for risk reduction when adopting centralized policy management and automated secrets management.. For example:   + Data from [IBM’s Cost of a Data Breach Report 2023](https://www.ibm.com/reports/data-breach) shows significant savings in breach costs when automated governance and access controls are deployed.   + Customer case studies from HashiCorp (e.g., Vault implementation impact on breach prevention).   **Decrease response time to security incidents by 30% through pre-defined workflows and drift detection alerts**   * [Gartner](https://www.computerweekly.com/opinion/Gartner-Navigating-Incident-Response-in-the-cloud) and [Forrester](https://www.forrester.com/report/best-practices-for-automating-security-operations-workflows/RES179705) research on incident response improvements when leveraging automation and continuous monitoring. * HashiCorp Vault and Terraform’s ability to enforce dynamic, automated remediation workflows. | **Achieve 100% audit compliance with pre-built compliance workflows and policy-as-code governance**   * Direct from customer case studies (e.g., HashiCorp’s work with financial services and healthcare customers achieving audit compliance via Terraform Sentinel and Vault's logging). * NIST compliance reports and pre-built compliance modules provided by HashiCorp Terraform and Vault.   **Enhance compliance readiness by 50% through automated secrets lifecycle management and centralized logging**   * [Industry analysis](https://delinea.com/resources/cyberedge-2024-cyberthreat-defense-report) on lifecycle management for secrets (e.g., Secretless apps and DevSecOps approaches). * Vault customer evidence showcasing automated rotation and dynamic secrets reducing audit times. | | **Reduce data theft risks by 35% with persistent encryption for data in transit and at rest**   * Research from the [Ponemon Institute](https://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf) and encryption technology reports highlight the role of pervasive encryption in reducing unauthorized data access. * HashiCorp Vault’s encryption-as-a-service use cases (protecting sensitive data across multi-cloud environments).   **Improve secure access efficiency by 25% through automated machine-to-machine identity verification**   * HashiCorp customer implementations (e.g., Nomad and Consul for service-to-service authentication). * [Forrester analysis](https://www.appviewx.com/2023-forrester-survey-secure-a-zero-trust-future-with-an-integrated-human-machine-identity-security-approach/) on reducing downtime through machine identity automation. |

## Competitive Analysis

| **Competitive Battle Cards** | |
| --- | --- |
| [Terraform CE](https://hashicorp.highspot.com/items/61d37eae550295ea581553e9?lfrm=rhp.16#1) |  |
| [OpenTofu](https://hashicorp.highspot.com/items/65f8c5b092bc534193bdb69f?lfrm=shp.0#1) |  |
| [Vault CE](https://drive.google.com/file/d/1BTRpL-6E5DiQIU32pmxp2VUn_c6IW9lt/view) | |
| [CyberArk](https://hashicorp.highspot.com/items/6414916e8d89f3f2890c80a5?lfrm=rhp.0#1) | |
|  | |