Solution Brief

Building Secure Applications with HashiCorp Terraform and Posture Control by Zscaler

Business Challenge

Organizations around the world have made a monumental shift towards providing customers with an intuitive and sophisticated digital experience. They're now catering to every phase of consumer behavior, ranging from advertising and buying to after-sales support. The magnitude and scale of this digital transformation are made possible by shifting their infrastructure from conventional data centers to state-of-the-art infrastructure management from public cloud vendors.

DevOps teams are at the forefront of this transformation, leading the way with the rapid deployment of code and building infrastructure with modern CI/CD pipelines across multiple public cloud environments. Teams are often challenged with managing skill gaps widened due to complex multi-cloud environments that can slow down the pace of development. DevOps communities have simplified their routine tasks by widely adopting HashiCorp Terraform, an infrastructure-as-a-code (IaC) tool to provision, change, and version resources on any environment.

HashiCorp Terraform plays a pivotal role in the rapid development and deployment of new applications, but organizations are still struggling to assess and respond to various risks to their infrastructure. New threats and risks arising from misconfigurations in CI/CD pipelines, combined with the speed at which automation can multiply these issues, lead to exposure of attack surface and rapid risk proliferation. Cloud infrastructure development and management are opaque to the security team. This makes operations prone to misconfigurations introduced due to the skipping of established guardrails and the drift away from the intended state of the infrastructure.

An application can be made both continuously secure and reliable with closer collaboration between the DevOps and Security teams, a practice that would reinforce security at every stage of the development pipeline. Transparent security promotes expedited application deployment and makes the DevOps team an equal stakeholder in producing highly resilient and secure applications.

DevOps and Security Challenges

- Complex multi-cloud infrastructure with non-portable scripting
- Committed change impact not visible until deployed in production
- At loggerheads with the security team perpetually due to lack of visibility
- Resource strain and skill gaps leading to misconfigurations

Solution

Posture Control + HashiCorp

Securing the CI/CD pipeline for an enriched DevOps experience

Posture Control™by Zscaler and HashiCorp Terraform integration provides a comprehensive solution that enables DevOps and Security teams to secure infrastructure-as-code (IaC). The solution prevents misconfigurations, code leaks, environmental drift, and other cloud security issues, all in a single integrated platform. Each commit and pull request is scanned for changes that may lead to issues related to hard-coded secrets, access changes that may cause misconfigurations, storage that is shared widely beyond the scope of the content, and more. Near-to-real-time alerts and guided remediation is critical for expedited and informed remediation. The integration lays the foundation for a continuous security process that helps to detect potential IaC security vulnerabilities early in the development cycle and fix them before they go into production. This helps to improve the overall risk posture and maintain cloud compliance.

Benefits of Hashicorp Terraform and Posture Control integration

- Detect, track and fix misconfigurations in Terraform configurations earlier in CI/CD pipelines
- Resolve vulnerabilities and mitigate risk to enhance security and compliance of deployment
- Prioritize, contextualize and remediate cloud infrastructure risks

Posture Control integration for Terraform Cloud enables development teams to scan Terraform files — which are previews of potential infrastructure changes — and compare the output against best practice security policies for all major public cloud providers and Kubernetes. Policy violations in the Terraform pipelines can be prevented before the apply stage with Posture Control run tasks integration with Terraform Cloud. This helps to prevent out-of-compliance infrastructure from being provisioned and provides fast feedback on the issue, impact and suggests a fix to development teams about policy compliance.

Posture Control: Key Capabilities

Scans IaC configurations for errors
When IaC configurations contain misconfigurations and vulnerabilities, it is often due to well-intentioned developers that have poor awareness of enterprise security policies. A developer may open a port or change the visibility of the content storage directory to enable a testing scenario and propagate the change to the production environment. By integrating checks into the DevOps workflows, and regularly monitoring HashiCorp Terraform configurations and scanning Terraform cloud workspaces for misconfigurations, insecure default configurations, publicly accessible cloud storage, or unencrypted databases with Posture Control, the DevOps team can now identify and remediate potential violations before they are deployed in the production environments.

Enforces guardrails to counter drift

Terraform configurations ensure that the cloud infrastructure is deployed in a uniform and consistent way across the multi-cloud environment in various stages of production. However, sometimes application owners need to make modifications to their applications in a method that does not conform to the established practices. Such changes are often a response to urgent production situations or a user inadvertently making changes directly to the infrastructure. The observed phenomenon of a gap between the desired and the intended state of the production configuration is known as drift. If left unchecked, it leads to an infrastructure exposed to attacks and renders the infrastructure out of compliance. With Posture Control, organizations benefit from the convergence of IaC scanning and CSPM to help identify and remediate drifts as they are observed in all the stages of the CI/CD pipeline.

Enhances team collaboration

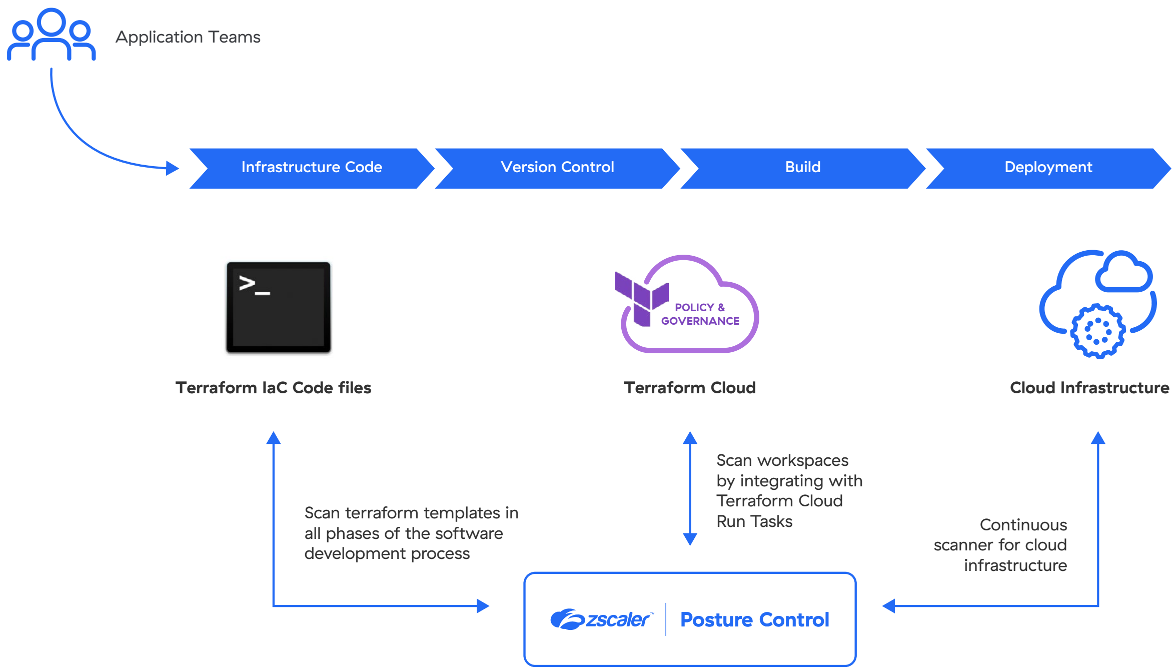
DevOps and Security teams often are not on the same page with security. Frequently, the cause is a lack of visibility in each other's domain. The DevOps team is focused on rapid and agile development powered by HashiCorp Terraform automation, while the security team is concerned with the threats and risks to the application and services infrastructure arising from the misconfigurations and vulnerabilities in the system. Posture Control breaks the silos between these teams with a continuous unified assessment and analysis of the risks and threats to the application environment.

Secures hard-coded credentials

Sensitive data such as secret keys, private keys, SSH keys, access/secret keys, and API keys are often found hardcoded in IaC configurations. The exposed credentials can propagate rapidly with the IaC code committed to public repositories and can pose a great risk for the organizations. HashiCorp Terraform configurations are also susceptible to this type of DevOps user error. The best approach to prevent such hard-coded secrets from leaking into the version control system is by scanning commits with Posture Control before they are merged into the main branch and by highlighting the violations for appropriate remediation.

Posture Control and HashiCorp Terraform integration provides a comprehensive solution that enables DevOps and Security teams to secure infrastructure-as-code (IaC).

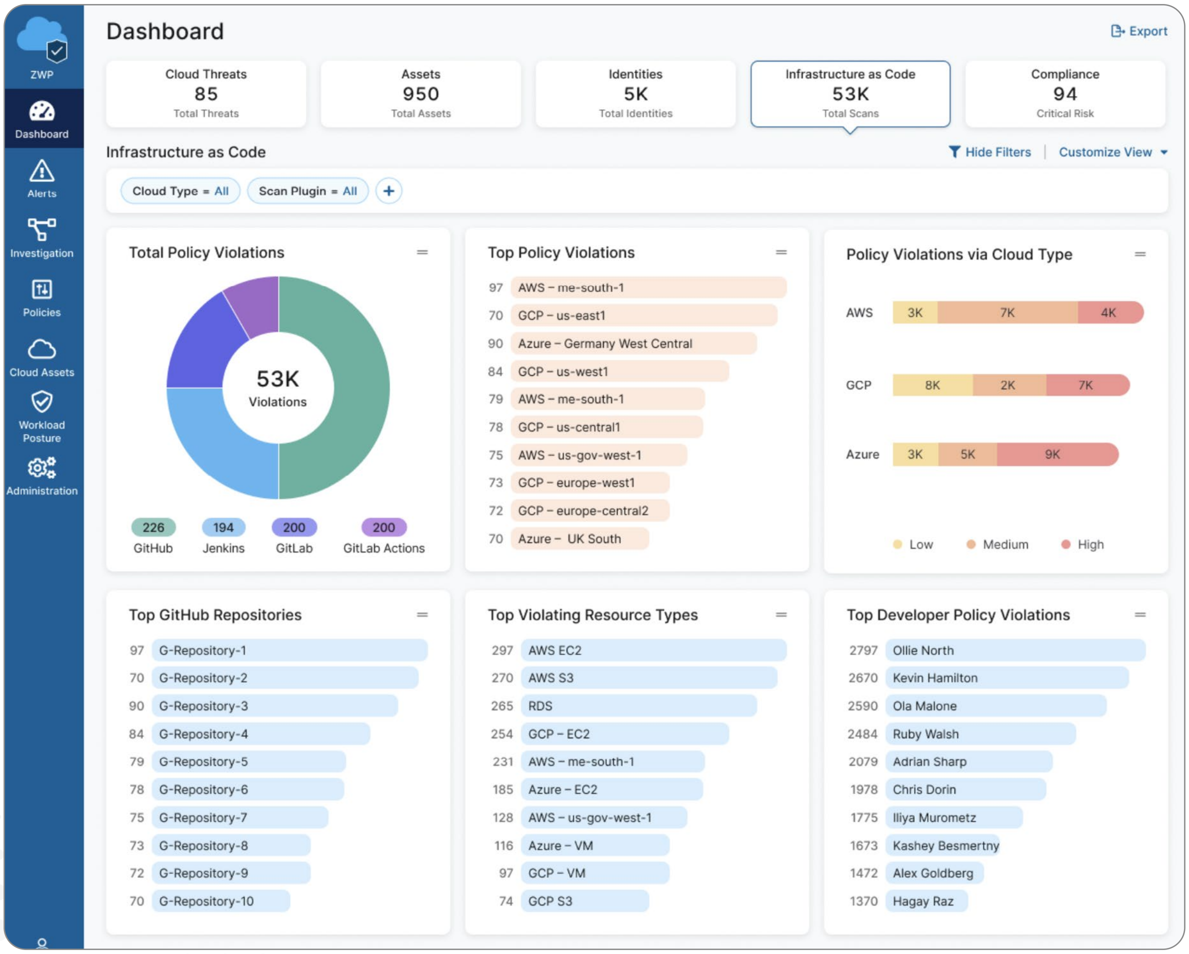
Posture Control Workflow



Scan terraform templates in all phases of the software development process

Scan workspaces by integrating with Terraform Cloud Run Tasks

Continuous scanner for cloud infrastructure



Dashboard

Cloud Threats	Assets	Identities	Infrastructure as Code	Compliance
85	950	5K	53K	94
Total Threats	Total Assets	Total Identities	Total Scans	Critical Risk

Infrastructure as Code

Cloud Type = All · Scan Plugin = All · +

Total Policy Violations

53K Violations

226	194	200	200
GitHub	Jenkins	GitLab	GitLab Actions

Top Policy Violations

97	AWS – me-south-1
70	GCP – us-east1
90	Azure – Germany West Central
84	GCP – us-west1
79	AWS – me-south-1
78	GCP – us-central1
75	AWS – us-gov-west-1
73	GCP – europe-west1
72	GCP – europe-central2
70	Azure – UK South

Policy Violations via Cloud Type

	Low	Medium	High
AWS	3K	7K	4K
GCP	8K	2K	7K
Azure	3K	5K	9K

Top GitHub Repositories

97	G-Repository-1
70	G-Repository-2
90	G-Repository-3
84	G-Repository-4
79	G-Repository-5
78	G-Repository-6
75	G-Repository-7
73	G-Repository-8
72	G-Repository-9
70	G-Repository-10

Top Violating Resource Types

297	AWS EC2
270	AWS S3
265	RDS
254	GCP – EC2
231	AWS – me-south-1
185	Azure – EC2
128	AWS – us-gov-west-1
116	Azure – VM
97	GCP – VM
74	GCP S3

Top Developer Policy Violations

2797	Ollie North
2670	Kevin Hamilton
2590	Ola Malone
2484	Ruby Walsh
2079	Adrian Sharp
1978	Chris Dorin
1775	Iliya Murometz
1673	Kashey Besmertny
1472	Alex Goldberg
1370	Hagay Raz

Fig: Posture Control IaC scan dashboard

About Posture Control

Posture Control, a cloud-native application protection platform (CNAPP), reimagines cloud-native application security as a 100% agentless solution that uses machine learning to correlate hidden risks caused by misconfigurations, threats, and vulnerabilities across the entire cloud stack. It empowers security, development, and DevOps teams to efficiently prioritize and remediate risks in cloud-native and VM-based applications as early as possible in the development cycle.

Posture Control helps organizations proactively secure IaC with an integrated, cloud-native platform that embeds security best practices in developer environments, integration tools, and source code repositories. Using predefined policies to identify and prioritize high-risk misconfigurations, code leaks, environmental drift, and more, organizations can keep continuous IaC governance under control with ease. Posture Control also provides rich context and guided remediation directly in popular DevOps tools and workflows, including integrated development environments (IDEs), continuous integration (CI) tools, and version control systems (VCS). Posture Control improves overall cloud security posture while reducing the burden on security and operations teams as well as mitigating cross-team friction.

Posture Control is part of Zscaler for Workloads, a comprehensive cloud security solution for any application running on any service in any cloud.

What to buy?

Posture Control **Advanced version** that includes Infrastructure as Code scanning**.**

Visit Posture Control **for more information or** contact us **to get started with a free assessment of the security of your DevOps pipeline.**

zscaler™ | Experience your world, secured.™

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.