SOLUTION OVERVIEW

TENABLE.CS & HASHICORP TERRAFORM CLOUD

ESTABLISH COMPLIANCE AND SECURITY GUARDRAILS IN THE DEVELOPMENT PROCESS BEFORE RUNTIME

TECHNOLOGY COMPONENTS

- Tenable.cs
- HashiCorp Terraform Cloud

KEY BENEFITS

- Identify and remove cloud flaws during development before they ever reach production.
- Take advantage of policies across all leading standards, or create your own.
- Improve communication between security, cloud operations and DevOps for greater efficiency.
- Understand the security posture of cloud environments alongside your on-prem assets.

BUSINESS CHALLENGE

Cloud services and applications are elastic, cost efficient, and most importantly, enable organizations to respond quickly to shifting customer needs. But, with the benefits of agility and efficiency, comes the challenge of protecting and securing resources and workloads in the public cloud.

There are existing solutions designed to protect the cloud, but they are applied too late. Risks identified in runtime are already exposed to attackers, and fixes applied in runtime will be overwritten with the next code deployment. Additionally, cloud environments are highly dynamic with new updates continuously released into production and workloads scaling up and down based on customer demand. Runtime-focused cloud security solutions aren't sufficient to enable agile DevOps principles because they are too disruptive to their automated development processes. Moreover, they do not provide the necessary context for developers to appropriately prioritize risks and remediate findings. These problems are exacerbated as developers embrace GitOps to automate the build and deployment processes.

Finally, existing security solutions are unable to support the full Software Development Lifecycle (SDLC) from development to operations, nor are they able to secure cloud environments from Infrastructure as Code to cloud resources to cloud workloads. Security teams need comprehensive, end-to-end capabilities to prevent cloud exposures, continuously monitor for configuration drift and continuously detect new vulnerabilities.

SOLUTION

Tenable.cs and HashiCorp Terraform Cloud enable teams to codify cloud security policies for infrastructure as code with automated enforcement and remediation recommendations as part of their development workflow. For HashiCorp Terraform Cloud users, it has never been easier to establish compliance and security guardrails in the development process that ensures infrastructure is secure before it is provisioned.

Tenable.cs can be used to evaluate your Terraform Cloud templates for security violations to reduce risk before they are introduced into your runtime environment. To accomplish this, Tenable.cs can be integrated as a "Run Task" that is triggered each time a Terraform Cloud plan is executed to find flaws and provide specific remediation recommendations.

VALUE

SECURE INFRASTRUCTURE AS CODE

Establish guardrails in automated GitOps and CI/CD processes that ensure secure deployments with minimal effort. It's extremely difficult to assess the setup and configuration of the 100 different services in Amazon Web Services (AWS) to answer the question "are these services configured securely?" Any misconfiguration in your cloud environment can expose you to risks such as unauthorized access to business critical assets. What makes it even more challenging is that there is no one-time fix for misconfiguration issues. In dynamic cloud environments, what's secure today may be a risk tomorrow.

LEVERAGE SPECIFIC REMEDIATION RECOMMENDATIONS, INSTANTLY

Knowing the exact remediation steps can be time intensive and challenging. Remediation guidance and recommendations are provided to help with patching operations for specific Terraform templates before being provisioned.

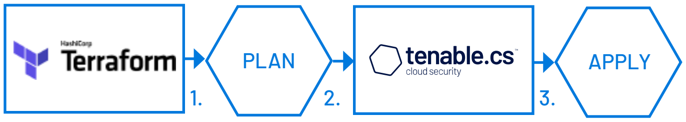
PREVENT CLOUD POSTURE DRIFT

Many cloud assets are clones of one another and have a cascade effect on other copies. Once an asset is exposed, even if it was short-lived, nobody can predict its blast radius before it is decommissioned. Automatically propagate compliant, authorized configuration changes from runtime to IaC.

POLICY ASSURANCE

It's extremely difficult to enforce and be consistent with security best practices in the cloud - the complexity of cloud and poor cloud security policy knowledge cause misconfiguration in the cloud and lack of compliance. Ensure cloud environments are compliant with policies from development through runtime, while addressing remediations in IaC and container images.

HOW IT WORKS



1. Submit a plan and apply run within Terraform Cloud

2. Once the Terraform Cloud plan is executed Terraform Cloud cloud will trigger Tenable.cs for security policy evaluation

3. Results of the scan are available within Tenable.cs and Terraform Cloud run can behalted if the Terraform Cloud run task is configured in "mandatory" mode and policy violations are found.

For More Information:
Please visit tenable.com

Contact Us:
Please email us at sales@tenable.com or visit
tenable.com/contact

ABOUT TENABLE

Tenable® is the Cyber Exposure company. Approximately 40,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include approximately 60 percent of the Fortune 500, approximately 40 percent of the Global 2000, and large government agencies. Learn more at tenable.com.

tenable®