Unified Management of Native Security Controls Across All Your Platforms & Technologies

aws · Red Hat OpenShift · Istio · Azure Kubernetes Service (AKS) · RANCHER · Azure · Google Cloud Platform · Google Kubernetes Engine · HashiCorp Terraform · Microsoft Teams · slack · ANSIBLE
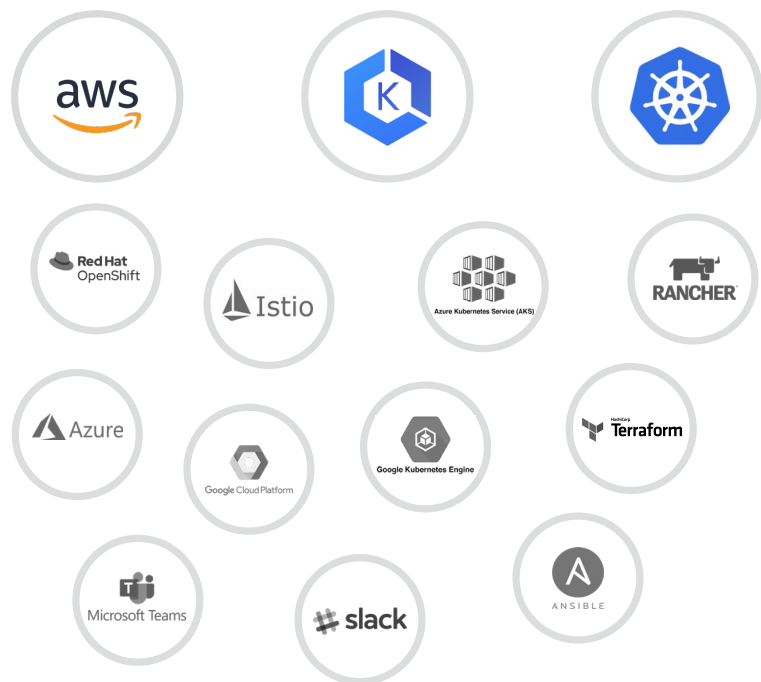
Tufin Cloud: Specifications at a Glance

- Enterprise-class secure SaaS solution (SOC2, ISO 27001 | 27017 | 27018, HIPAA)
- AES256 encryption at-rest
- No agents required (K8s support requires Kite module on target cluster)
- Requires read-only access

Try Tufin Cloud Free: Deploy in Minutes

Get your free, automated Cloud Security Assessment in minutes

Full-featured 30-day trial of Tufin Cloud available at:

tufin.com/try-securecloud →

---

tufin
The Security Policy Company.

Tufin Cloud: Security for AWS & EKS

Security Policy Automation for AWS, Multi-Cloud, Hybrid, and Kubernetes Environments

---

tufin
The Security Policy Company.

aws · Amazon EKS

Streamline security posture management across your complex cloud and hybrid environments with granular visibility and precision security policy automation.

Kubernetes Policy Management

- Real-time service-centric cluster topologies
- Drill-down to evaluate configuration risks

Visibility

- Real-time app-centric topologies
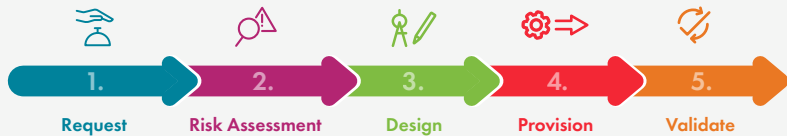- Drill-down to evaluate configuration risks
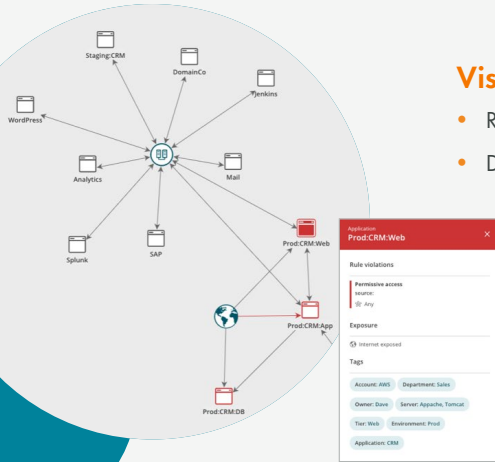
Risk Analysis

- Easily identify CVEs and access/ connectivity risks
- Compare all configurations to CIS benchmarks

Change Automation

- Centrally provision and audit all firewall and Security Group access requests
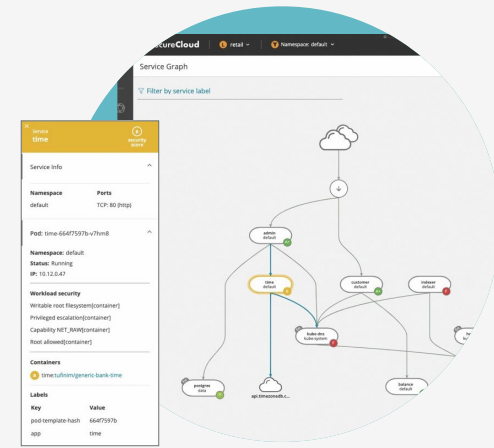- Automate rules-cleanup

1. Request
2. Risk Assessment
3. Design
4. Provision
5. Validate

DevOps Integration

- Inject security policy into CI/CD pipelines
- Accelerate build promotion and "Shift-Left" security

DEV OPS

Tufin Cloud: Unified Security Policy Automation for Hybrid, Multi-cloud, and K8s Environments

App-centric topologies of your AWS assets, services, and traffic

Visualize traffic, identify access and connectivity risks, and evaluate configurations against CIS benchmarks within AWS, on-prem, and other cloud infrastructures

Unified security control management across AWS, on-prem, and multi-cloud instances

Design and deploy security policies for cloud-native controls to ensure compliant operations and other cloud infrastructures

Automated change and rule management for AWS Security Groups and 3rd party cloud firewalls

Leverage a secure workflow to request, provision, validate, and audit access requests for AWS firewalls (3rd party) and Security Groups

Proactive security policy violation alerting

Receive prescriptive alerts via real-time risk analysis engine when any build contains non-compliant configurations, for fast remediation

Kubernetes/EKS visibility and security automation

Visualize service-level traffic of K8s clusters and enforce security policies based upon both CIS benchmarks and approved traffic flows to accelerate build promotion

"Shift Left" security via policy integration with DevOps pipelines

Automate YAML security policy creation and leverage APIs to inject security configurations into popular CI/CD tools