tufin The Security Policy Company.

Tufin SecureCloud Solution Brief

Gain visibility and control of your security posture across multi-cloud and cloud-native environments to ensure continuous compliance– without compromise

The Challenge – Visibility and Compliance Across Multi-cloud and Cloud Native

As organizations expand their cloud utilization, whether through cloud native, hybrid cloud, multi-cloud, private cloud, or kubernetes, the complexity of maintaing visibility and security compliance across their environment increases. There are more people, technologies, solutions, platforms, and skillsets involved, which leads to blind spots and misconfigurations. Gartner's Neil MacDonald forecasts that "Through 2023, at least 99% of cloud security failures will be the customer's fault," hence will be due to misconfigurations. The complexity of so many moving parts has outstripped the ability to manage it all disparately, or manually.

Tufin SecureCloud: Secure Your Cloud Environment

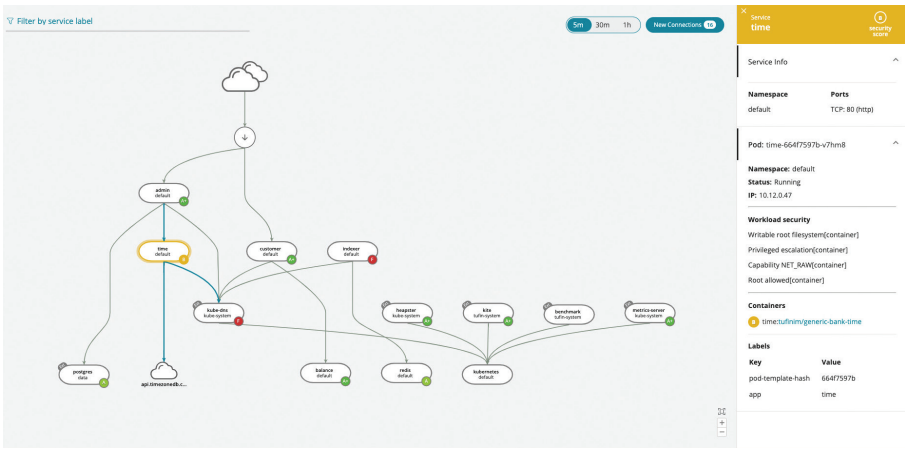
Tufin SecureCloud enables security teams to gain visibility into their cloud security posture, establish security guardrails and achieve continuous compliance, without compromising the business benefits of cloud computing. With SecureCloud you can make your agile environments, public clouds, and Kubernetes secure without getting in the way of developer productivity or creating roadblock to cloud process automation.

SecureCloud is the newest component of the Tufin Orchestration Suite uniquely providing a single vendor solution to manage security policy for the entire hybrid cloud estate, on-premises and cloud.

Regain Visibility of your Cloud Security Posture

SecureCloud provides a unique ability to gain visibility of your cloud workload access, including within and between pods, to help you quickly understand threats and vulnerabilities. SecureCloud provides:

- Visibility of E-W & N-S traffic flows
- Automated Workload and Policy Discovery – automatically discover and visualize all workloads and network security devices
- Application-centric Topology View – centralized view of all assets deployed, configurations and security settings (what is where, what can talk to what, etc.) to ensure only trusted workloads and traffic are allowed.
- Segmentation - automatically learn, generate and establish microsegmentation, based on actual traffic to ensure least privilege access



SecureCloud Topology: Full visibility of all services, security posture scores, and traffic flows across the cloud workloads, including real-time capability for discovery of all new connections.

Benefits

- Gain real-time visibility of cloud security posture
- Establish security guardrails for cloud native and public cloud workloads
- Ensure compliance of cloud workload and Kubernetes access policies and segmentation
- Security without comprosiming business agility and investments
- Efficient application without a new control plane, a large footprint or additional compute costs
- Achieve security without compromising the speed of deployment or business agility

[1] How to Make Cloud More Secure Than Your Own Data Center, Neil MacDonald, Tom Croll, Gartner, 9 Oct 2019, https://www.gartner.com/document/3970177?ref=solrAll&refval=247812029

Establish Cloud Security Guardrails

SecureCloud enables security teams to set "guardrails" or automated security policy guidelines, across all cloud environments. These guardrails can be embedded into the development process to shift-left security and serve as a basis for comparing or evaluating all policies across your environment. With SecureCloud you can:

- Define policy guardrails – create security policy guidelines against which all cloud security policies can be automatically compared
- Automate policy code generation – automatically generate native security policy YAMLS for Kubernetes clusters and confirm if they comply with your guardrails to avoid manual erros, save time, and streamline security policy implementation

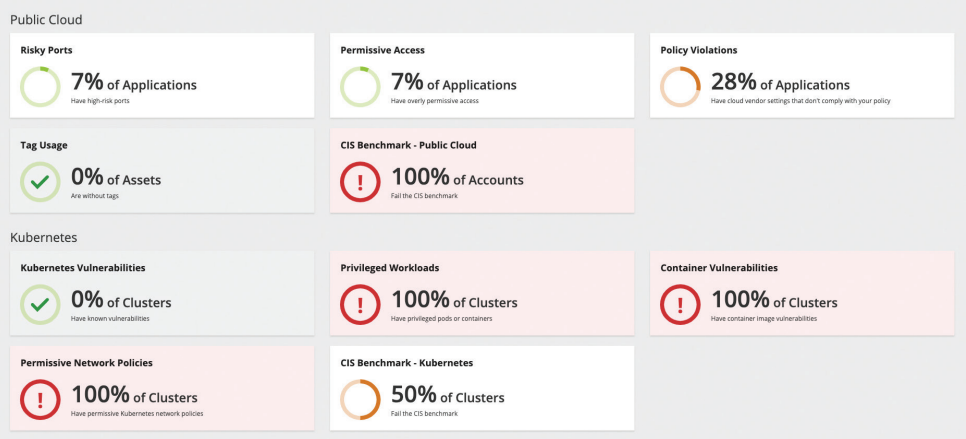
Ensure Continuous Compliance

SecureCloud leverages the guardrails you established to enable you to see at any point in time if your cloud workload and application access policies are properly configured and comply with these standards. Furthermore, with continuous monitoring and real-time alerts of policy violations you will have the information needed for fast and effective mitigation. SecureCloud includes:

- Enforce Policy & Segmentation – continuously monitor activities in the environment and automatically enforce microsegmentation for continuous compliance across large, complex cloud environments.
- Security Posture Dashboard – monitor containers, public cloud services, and firewalls to automatically detect security policy violations and highlight areas of risk
- Shift-left Security Controls in the CI/CD Pipeline - integrate network security into the CI/CD pipeline for end-to-end automation, ensuring only compliant code is deployed.
- Application Lifecycle Security – automate discovery, alerting, and remediation of security risks across the entire application lifecycle – build, test, deploy, and operate.
- Real-time reporting – dashboards and reports for audits, proof of compliance and office of the CISO

Single Platform for Managing Your Hybrid Cloud

Managing security in cloud and cloud-native environments is often only part of the equation. As workloads and applications migrate to the cloud, some applications need access to the on-premises environment. Even cloud-native applications often require access to resources protected behind traditional network security devices. SecureCloud, as part of the Tufin Orchestration Suite, integrates into SecureTrack for automated provisioning and compliance of on-prem security devices.



SecureCloud Dashboard: InfoSec cloud security risk dashboard - includes Kubernetes and cloud environment information, as well as a compliance status for workloads and assets deployed

Multi-cloud and Kubernetes Security Without Compromise

With SecureCloud, you can allow security teams to run at the same velocity and with the same agility as the rest of the organization without compromising security or the speed of the business. Over 2,300 of the world's largest global organizations trust Tufin to simplify and automate their security policy management across complex hybrid environments. Gain confidence in your cloud security and compliance posture.

SecureCloud Works With the Leading Industry Platforms

Azure · Google Cloud · aws · kubernetes · RED HAT OPENSHIFT · Istio · Jenkins · redhat IBM · CLOUD NATIVE COMPUTING FOUNDATION · slack

Tufin (NYSE: TUFN) simplifies management of some of the largest, most complex networks in the world, consisting of thousands of firewall and network devices and emerging hybrid cloud infrastructures. Enterprises select the company's Tufin Orchestration Suite™ to increase agility in the face of ever-changing business demands while maintaining a robust security posture. The Suite reduces the attack surface and meets the need for greater visibility into secure and reliable application connectivity. With over 2000 customers since its inception, Tufin's network security automation enables enterprises to implement changes in minutes instead of days, while improving their security posture and business agility.

Find out more at: www.tufin.com | Follow Tufin on Twitter: @TufinTech | Read more on Tufin's blog: Suite Talk