# tufin Iris

# A Modern Approach to Cloud Security with Tufin Iris

## Solution Brief

## Security Policy Automation for Multi-Cloud Environments

Cloud-native platforms are powering Digital Transformations that increase business agility and accelerate innovation. And in the cloud-first world, the need to protect sensitive information and secure applications is as important as ever. This is increasingly difficult as developers use multiple cloud providers and applications are deployed more frequently. To keep pace with rapid change, IT security and cloud operations teams need new, cloud-native solutions to protect mission critical applications. Legacy security solutions were designed to protect physical infrastructure and their virtual counterparts. Tufin Iris enables security and IT operations teams to regain visibility and control security policies, powered by automation that integrates with DevOps pipelines.

## The Challenges

Traditional security tools protect applications by allowing or denying access based on IP addresses and ports. In a cloud-native environment, IP addresses are highly transient, and therefore services are often accessed by name, rather than address. Further, access control policies are defined by a combination of security groups and Identity and Access Management (IAM) roles. As a result, new solutions are needed to give IT security the visibility, control and automation to protect the business and ensure compliance.

## Regain Visibility

A single cloud environment may contain hundreds – possibly thousands – of active resources. Spread across multiple cloud accounts and vendors, it can be difficult to know what applications are deployed and if they comply with security policy. Tufin Iris intelligently monitors the cloud and discovers and displays all applications in an easy to navigate map. This helps IT security and cloud operation teams quickly identify risky or non-compliant resources needing immediate attention.
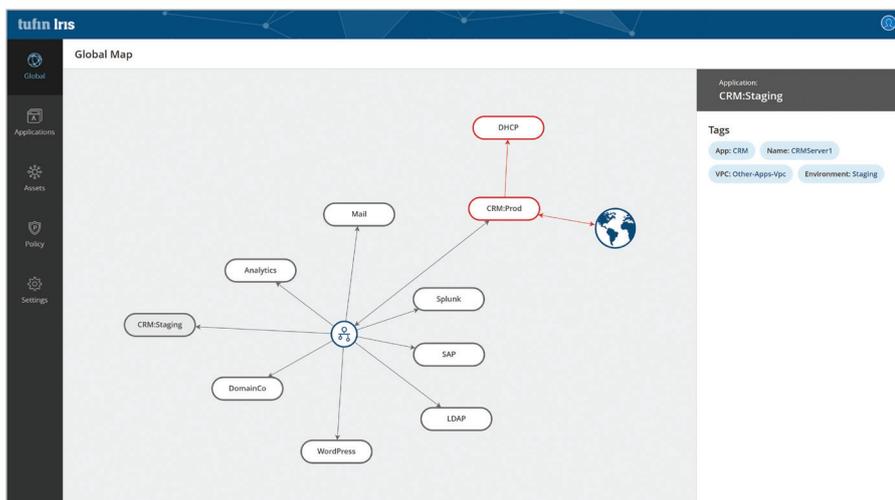


### Highlights and Benefits:

- Gain visibility into public cloud security settings

- Ensure continuous compliance and alerting

- Reduce policy complexity using security guardrails

- Microsegmentation policies for fine-grained access control

- Agentless solution delivered as a service

- Integrates with DevOps toolchain

- *Sign up for your free account: tufin.io*

### Tufin at a Glance

**Offices:** North America, Europe and Asia-Pacific

**Customers:** More than 2,000 in over 50 countries

**Leading Verticals:** Finance, telecom, energy and utilities, healthcare, retail, education, government, manufacturing, transportation and auditors

**Channel Partners:** More than 240 worldwide

**Technology Partners & Supported Platforms:** Amazon Web Services, BMC, Blue Coat, Check Point, Cisco, F5 Networks, Fortinet, Forcepoint, OpenStack, Palo Alto Networks, VMware and more
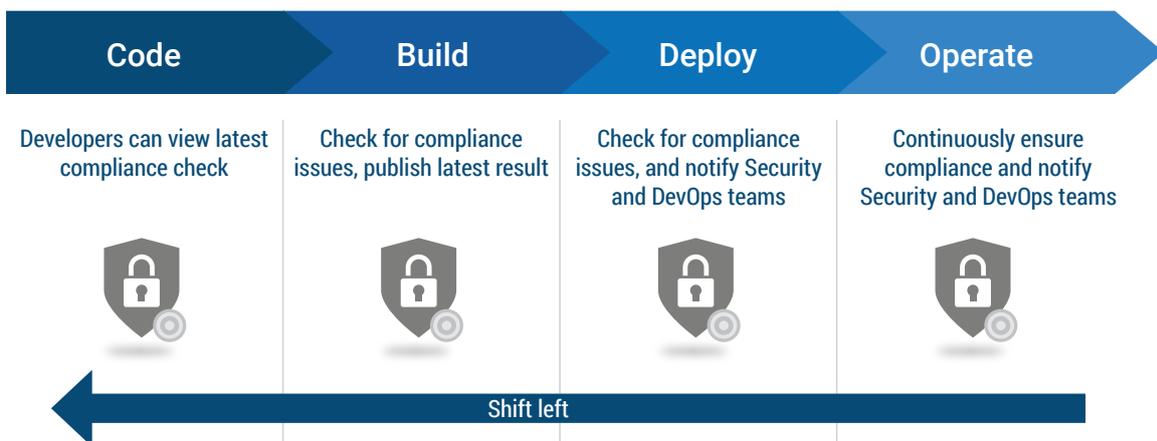
## Maintain Compliance

Using Tufin Iris, security teams can easily define security policies based on industry, regulatory or business requirements. To protect applications without increasing complexity or causing "rule bloat", IT can establish security guardrails that can be applied globally or to a general group of resources. For example, a guardrail could check that data storage is not accessible from the Internet. For fine-grained control, IT can define microsegmentation policies that tightly constrain access to protect mission critical resources, such as restricting access to a service that processes private customer records.
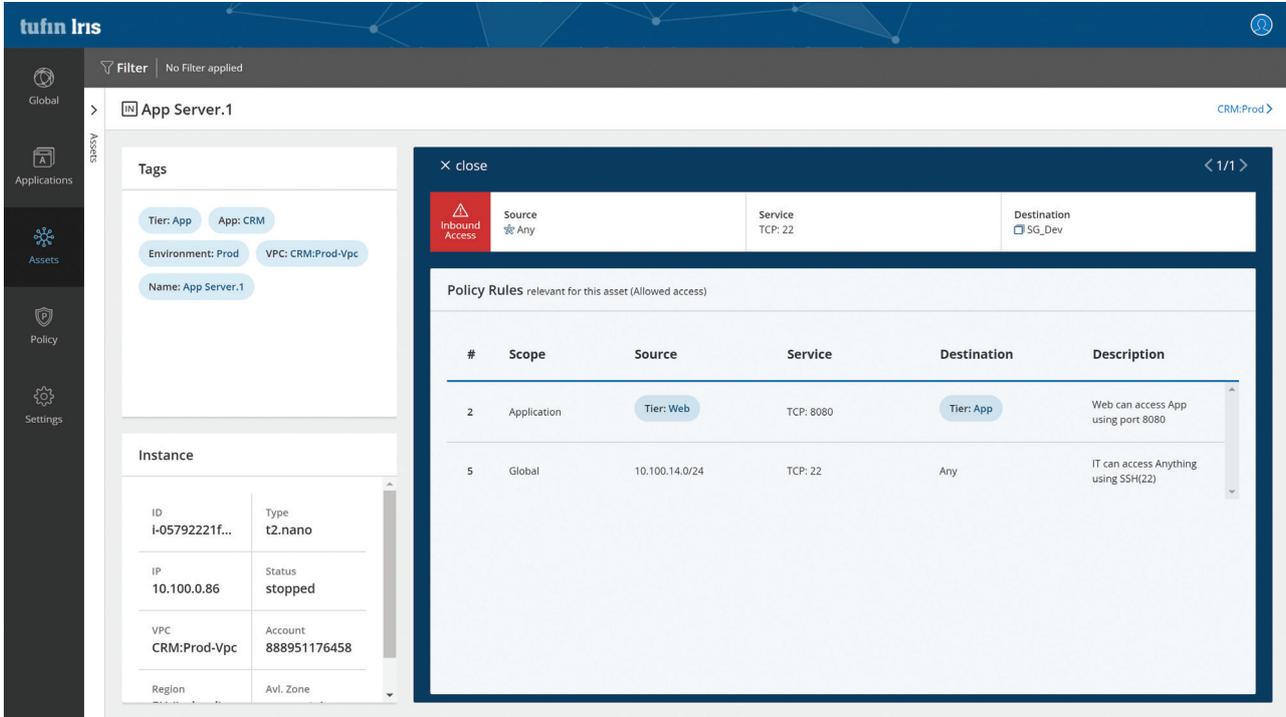


## Automate Security

Security in the cloud is best achieved through early prevention, often called "shifting left." Rather than have a scheduled final passthrough for security policy review, the security reviews integrated from the start of the development lifecycle, and throughout each step. Tufin Iris integrates into your DevOps pipeline through common CI/CD tools such as Jenkins to ensure you identify compliance issues before going to production.



| Code | Build | Deploy | Operate |
|---|---|---|---|
| Developers can view latest compliance check | Check for compliance issues, publish latest result | Check for compliance issues, and notify Security and DevOps teams | Continuously ensure compliance and notify Security and DevOps teams |

Shift left

## Try for free

Learn how Tufin Iris can help you secure your multi-cloud environment.
Signup online for your free account: tufin.io

www.tufin.com

SB-11-18