Securing Microservice Applications with Tufin Orca

Solution Brief

Securing Microservices at the Speed of DevOps

To address the need for business agility DevOps teams are increasingly adopting containers and microservice-based architectures. This shift enables developers to rapidly build, test and deploy changes to production environments dozens of times a day. IT security teams that still rely on traditional security tools and practices find it has become impossible to keep up with the rate of change. Tufin Orca is a cloud-based service that automatically learns application connectivity patterns, generates security policies, and enforces security at runtime.

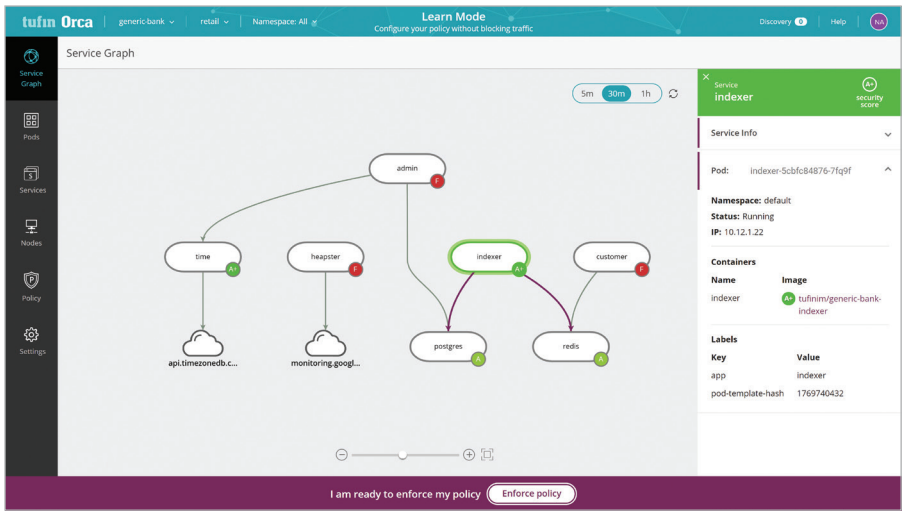
The Challenges

Securely managing communication among microservices is highly complex, and constantly changing. Yet, unlike traditional datacenters, microservice environments, like Kubernetes are entirely driven by automation. Unless IT security becomes integral to the DevOps cycle, traditional security services will struggle to keep pace with increasing changes and inhibit an organization's need for agility. Specifically, IT security must adapt to:

- Gain visibility into microservice environments
- Define and enforce microsegmentation across microservices and firewalls
- Enable DevSecOps by integrating security into CI/CD pipeline

Regain Visibility

Microservice applications are deployed into and managed by container orchestration platforms such as Kubernetes in the cloud and Red Hat OpenShift on-premises. These applications often contain hundreds – possibly thousands – of active services. Unlike legacy tools, Tufin Orca was designed for microservices. It enables security managers see all microservices applications and their components. Tufin Orca shows exactly how services communicate internally and externally, which services are at risk, and what security issues exist. This helps IT security and cloud operation teams quickly identify risky or non-compliant resources needing immediate attention.



Highlights and Benefits:

- Gain visibility into microservice security
- Enforce microsegmentation policies
- Ensure continuous compliance and alerting
- Automate security with DevOps toolchain integration
- ***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

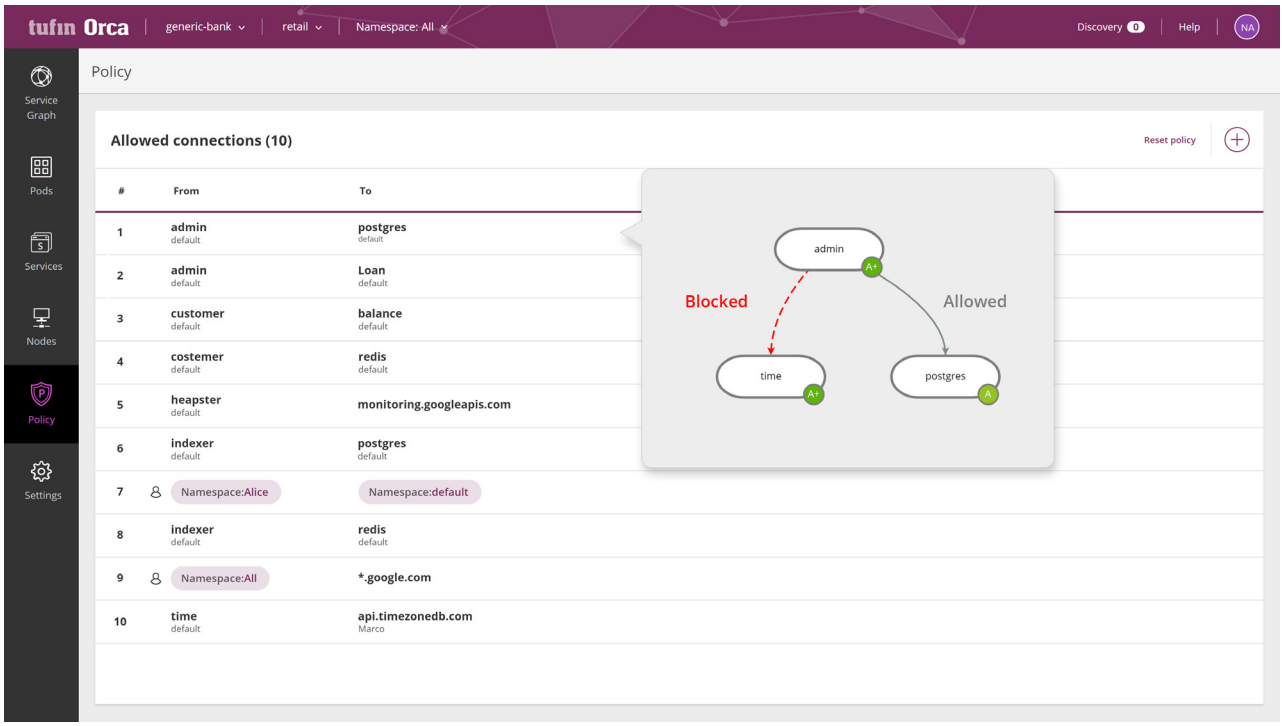
Leading Verticals: Finance, telecom, energy and utilities, healthcare, retail, education, government, manufacturing, transportation and auditors

Channel Partners: More than 240 worldwide

Technology Partners & Supported Platforms: Amazon Web Services, BMC, Blue Coat, Check Point, Cisco, F5 Networks, Fortinet, Forcepoint, Juniper Networks, Microsoft Azure, OpenStack, Palo Alto Networks, VMware and more

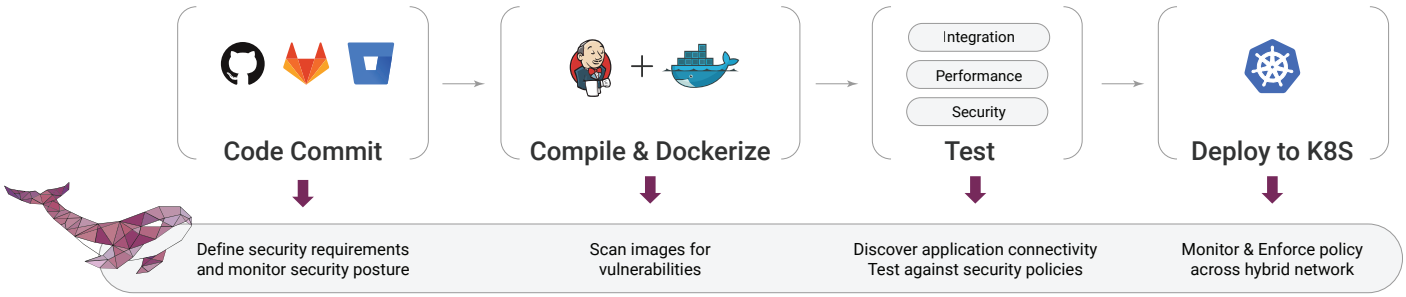
Automate Security Across a Hybrid Network

Security teams need the power to define and enforce security policies based on industry, regulatory or business requirements. Tufin Orca simplifies this process by monitoring communications and automatically generating security policies. Then security can adjust microsegmentation policies to meet changing business needs. The policy can then be enforced within the cluster and automatically extended to surrounding firewalls through an integration with Tufin Orchestration Suite.



Automate security in the CI/CD pipeline

Historically, security has been addressed late in the application development lifecycle; often relying on manual reviews that may last weeks. In an ideal world, security issues are found and remediated early, a practice commonly referred to as “shifting left.” With Tufin Orca, security policies become integral to your DevOps pipeline through common CI/CD tools such as Jenkins, helping to optimize security policies before going to production.



Try for free

Learn how Tufin Orca can help you secure your container and microservice applications.
Signup online for your free account: tufin.io

tufin
www.tufin.com

SB-11-18

tufin Orca