Absicherung von Microservice-Anwendungen mit Tufin Orca

Solution Brief

Schützen Sie Microservices in DevOps-Geschwindigkeit

Um die nötige geschäftliche Agilität zu erreichen, setzen DevOps-Teams zunehmend auf Container und Microservice-basierte Architekturen. Dies versetzt die Entwickler in die Lage, Änderungen an Produktionsumgebungen Dutzende Male pro Tag zu erstellen, zu testen und umzusetzen. IT-Sicherheitsteams, die sich weiter auf traditionelle Sicherheitstools und -praktiken verlassen, müssen feststellen, dass sie mit dem Tempo der Veränderungen nicht mehr mithalten können. Abhilfe schafft Tufin Orca: ein cloudbasierter Dienst, der automatisch Konnektivitätsmuster von Anwendungen erlernt, Sicherheitsrichtlinien erzeugt und die Sicherheit zur Laufzeit durchsetzt.

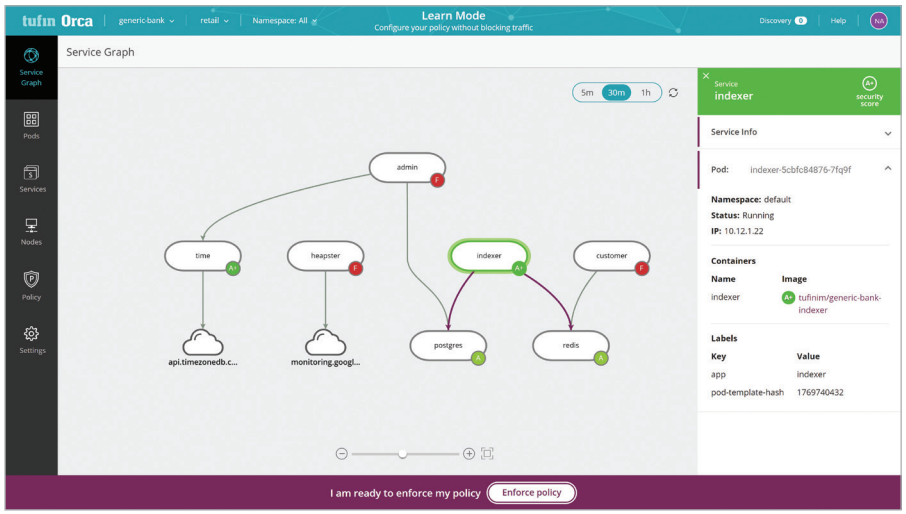
Die Herausforderungen

Die Kommunikation zwischen Microservices sicher zu verwalten ist eine hochkomplexe Aufgabe, die sich ständig wandelt. Im Gegensatz zu herkömmlichen Rechenzentren sind Microservice-Umgebungen wie Kubernetes allerdings vollständig automatisiert. Wenn die IT-Sicherheit nicht integraler Bestandteil des DevOps-Zyklus wird, werden traditionelle Sicherheitslösungen Mühe haben, mit den zunehmenden Veränderungen Schritt zu halten. Dies wiederum wird es dem Unternehmen erschweren, sich schnell auf neue Geschäftsanforderungen einzustellen. Insbesondere muss sich die IT-Sicherheit anpassen, um:

- Übersicht über die Microservice-Umgebungen zu gewinnen
- Mikrosegmentierung über Microservices und Firewalls hinweg definieren und durchsetzen zu können
- DevSecOps gerecht zu werden, indem Sicherheit in die CI/CD-Pipeline integriert wird

Die Übersicht zurückgewinnen

Microservice-Anwendungen werden in Container-Orchestrierungsplattformen bereitgestellt und über sie verwaltet, so etwa Kubernetes in der Cloud oder Red Hat OpenShift vor Ort. Diese Anwendungen umfassen oft Hunderte – oder gar Tausende – von aktiven Diensten. Im Gegensatz zu herkömmlichen Tools wurde Tufin Orca speziell für Microservices entwickelt. Die Lösung verschafft den Sicherheitsverantwortlichen Übersicht über sämtliche Microservice-Anwendungen und deren Komponenten. Tufin Orca zeigt genau, wie Dienste intern und extern kommunizieren, welche Dienste gefährdet sind und welche Sicherheitsprobleme bestehen. So können die IT-Sicherheits- und Cloud-Betriebsteams schnell diejenigen Ressourcen ermitteln, die Risiken darstellen oder Vorschriften verletzen und sofortiges Handeln erfordern.



Highlights und Vorteile:

- Vermittelt Überblick über die Sicherheit von Microservices
- Hilft, Richtlinien zur Mikrosegmentierung durchzusetzen
- Unterstützt kontinuierliche Compliance und Benachrichtigungen
- Automatisierte Sicherheit durch Integration mit der DevOps-Toolchain
- ***Registrieren Sie sich, um Zugriff auf Ihr kostenloses Konto zu erhalten: tufin.io***

Tufin auf einen Blick

Standorte: Nordamerika, EMEA und Asien-Pazifik

Kunden: Mehr als 2.100 Kunden in über 50 Ländern

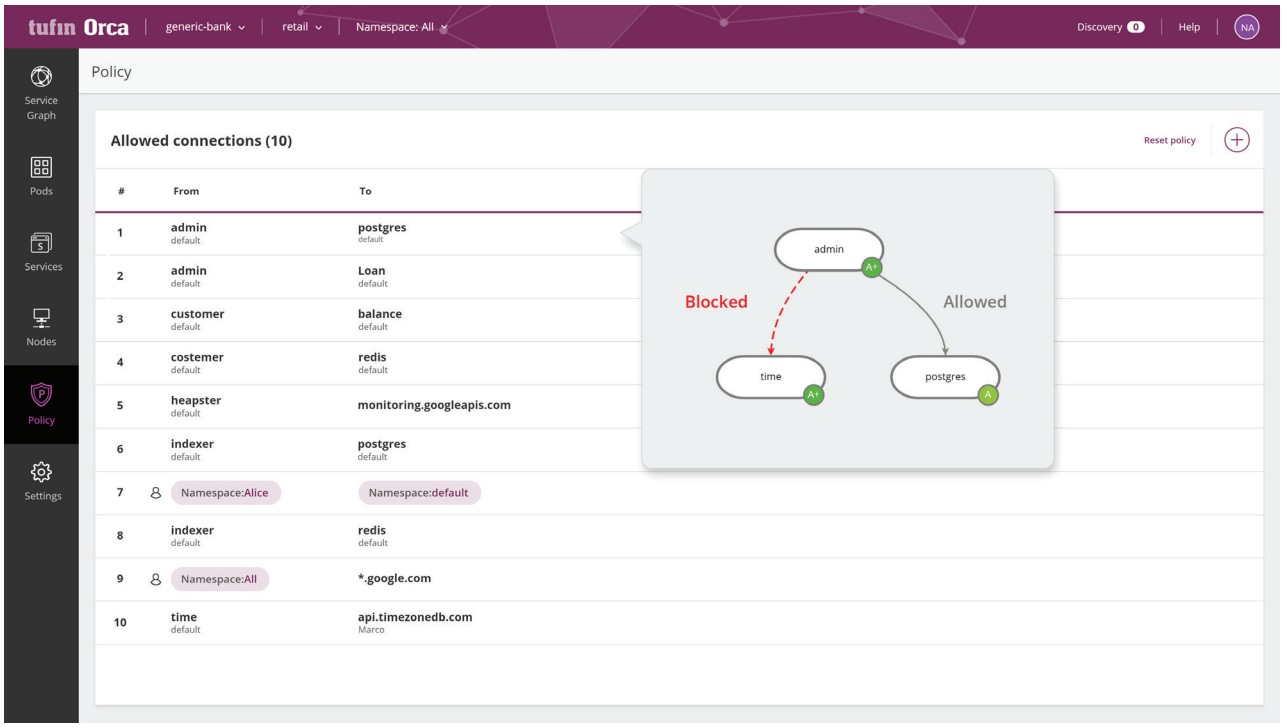
Wichtige Branchen: Finanzen, Telekommunikation, Energie und Versorgungseinrichtungen, Gesundheitswesen, Einzelhandel, Bildung, Behörden, Fertigung, Transport

Vertriebspartner: Mehr als 150 aktive Partner weltweit

Technologiepartner und unterstützte Plattformen: Amazon Web Services, BMC, Blue Coat, Check Point, Cisco, F5 Networks, Fortinet, Forcepoint, Juniper Networks, Microsoft Azure, OpenStack, Palo Alto Networks, VMware und mehr

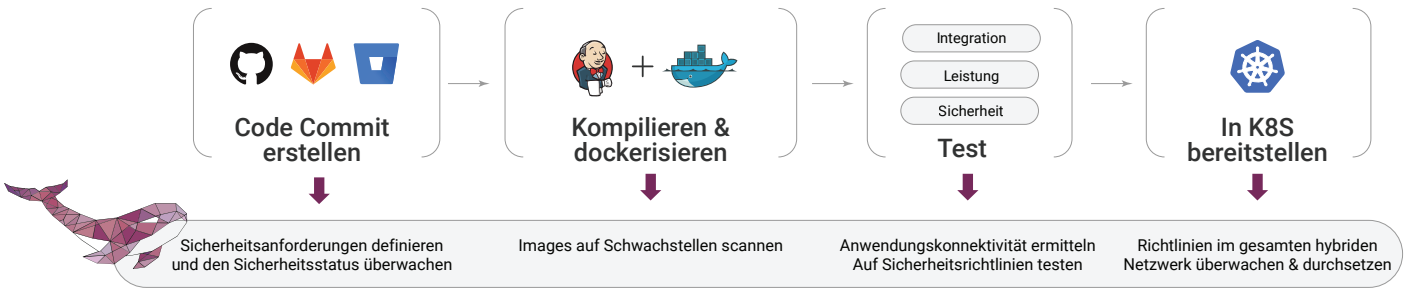
Sicherheit in hybriden Netzwerken automatisieren

Sicherheitsteams müssen in der Lage sein, Sicherheitsrichtlinien auf Basis von Branchen-, gesetzlichen oder geschäftlichen Anforderungen zu definieren und durchzusetzen. Die Lösung Tufin Orca vereinfacht diesen Prozess, indem sie die Kommunikation überwacht und Sicherheitsrichtlinien automatisch erstellt. Dann können die Sicherheitsteams die Richtlinien zur Mikrosegmentierung anpassen, um veränderlichen Geschäftsanforderungen gerecht zu werden. Die Richtlinien können innerhalb des Clusters durchgesetzt und durch Integration mit der Tufin Orchestration Suite automatisch auf umliegende Firewalls ausgedehnt werden.



Sicherheit in der CI/CD-Pipeline automatisieren

Herkömmlicherweise wird die Sicherheit erst spät im Lebenszyklus der Anwendungsentwicklung adressiert. Dazu finden häufig manuelle Überprüfungen statt, die Wochen dauern können. Idealerweise werden Sicherheitsprobleme jedoch frühzeitig entdeckt und behoben – eine Praxis, die oft als „Linksverschiebung“ bezeichnet wird. Tufin Orca ermöglicht es, Sicherheitsrichtlinien mithilfe gängiger CI/CD-Tools wie Jenkins zu einem integralen Bestandteil Ihrer DevOps-Pipeline zu machen. So hilft Ihnen Tufin Orca, Risiken zu identifizieren und die Konformität zu überprüfen, bevor Sie in den Produktivbetrieb gehen.



Testen Sie Tufin Orca kostenlos

Erfahren Sie, wie Tufin Orca Ihnen helfen kann, Ihre Container- und Microservices-Anwendungen abzusichern. Registrieren Sie sich online, um Ihr kostenloses Konto zu erhalten: tufin. io.

tufin
www.tufin.com

SB-02-19

tufin Orca