Mettere in sicurezza le applicazioni per microservizi con Tufin Orca

Informazioni sulla soluzione

Mettere in sicurezza alla velocità di DevOps

Per affrontare il bisogno di agilità aziendale i team DevOps stanno adottando sempre più architetture basate su microservizi e container. Questo passaggio consente agli sviluppatori di creare, testare e distribuire rapidamente le modifiche ad ambienti produttivi per decine di volte al giorno. I team di sicurezza IT che continuano ad affidarsi agli strumenti e alle pratiche di sicurezza tradizionali trovano che sia diventato impossibile stare al passo con la velocità dei cambiamenti. Tufin Orca è un servizio basato su cloud che apprende automaticamente i modelli di connettività delle applicazioni, genera policy di sicurezza e applica la sicurezza in fase di runtime.

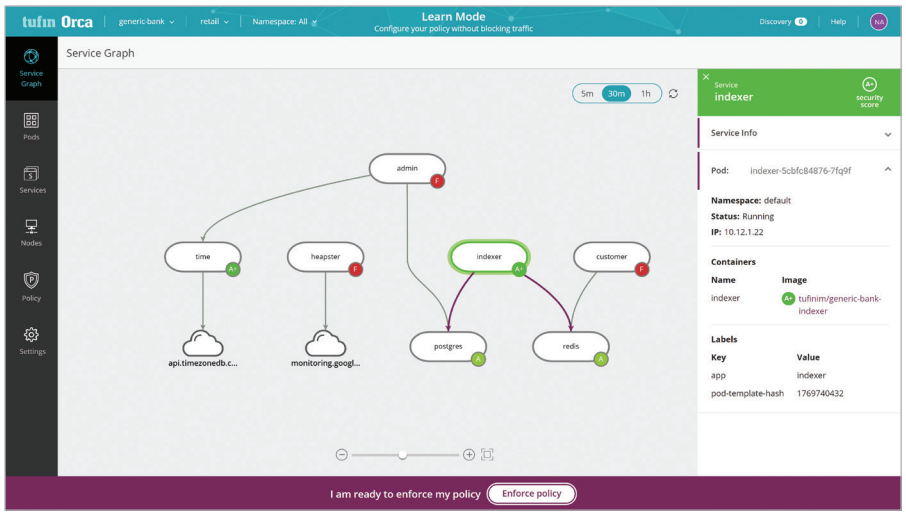
Le sfide

Gestire in modo sicuro la comunicazioni tra microservizi è decisamente complesso e richiede cambiamenti costanti. Tuttavia, in modo diverso da quanto accade con i data center tradizionali, gli ambienti dei microservizi quali Kubernetes sono totalmente automatizzati. A meno che la sicurezza IT non diventi parte integrante del ciclo DevOps, i servizi di sicurezza tradizionali fanno fatica a tenere il passo con i crescenti cambiamenti e inibiscono la rapida capacità di adattamento di un'organizzazione alle esigenze del business. Nello specifico, la sicurezza IT deve adattarsi a:

- Ottenere visibilità negli ambienti dei microservizi
- Definire e implementare la microsegmentazione tra microservizi e firewall
- Abilitare DevSecOps integrando la sicurezza nella pipeline CI/CD

Riottenere visibilità

Le applicazioni per microservizi vengono distribuite e gestite tramite piattaforme di orchestrazione dei container quali Kubernetes nel cloud e Red Hat OpenShift in loco. Queste applicazioni spesso contengono centinaia – se non migliaia – di risorse attive. Diversamente dagli strumenti di legacy, Tufin Orca è stato progettato per i microservizi. Consente ai responsabili della sicurezza di vedere tutte le applicazioni dei microservizi e i loro componenti. Tufin Orca mostra esattamente in che modo i servizi comunichino internamente ed esternamente, quali servizi siano a rischio e quali siano i problemi di sicurezza. Ciò aiuta i team di sicurezza IT e operatività cloud a identificare rapidamente risorse rischiose o non conformi che richiedono attenzione immediata.



Caratteristiche e benefici:

- Ottenere visibilità nella sicurezza dei microservizi
- Implementare le policy di microsegmentazione
- Assicurare la conformità continua e le notifiche
- Automazione della sicurezza con l'integrazione della toolchain DevOps
- ***Iscriviti per ottenere un account gratuito: tufin.io***

Panoramica di Tufin

Uffici: Nord America, EMEA e Asia-Pacifico

Clienti: Più di 2.100 in oltre 50 Paesi

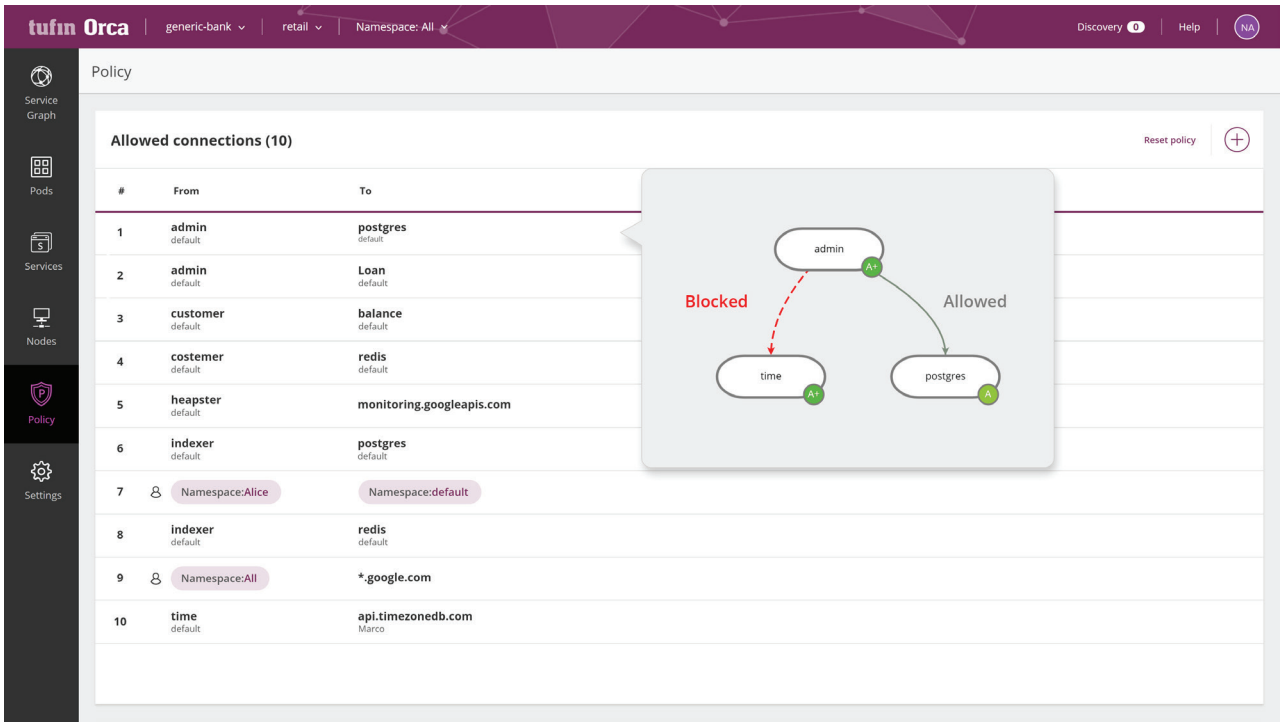
Principali settori di riferimento: Finanza, telecomunicazioni, energia e imprese di pubblica utilità, salute, vendita al dettaglio, educazione, agenzie governative, produzione, trasporti

Partner di canale: Oltre 150 partner attivi in tutto il mondo

Partner tecnologici e piattaforme supportate: Amazon Web Services, BMC, Blue Coat, Check Point, Cisco, F5 Networks, Fortinet, Forcepoint, Juniper Networks, Microsoft Azure, OpenStack, Palo Alto Networks, VMware e molti altri

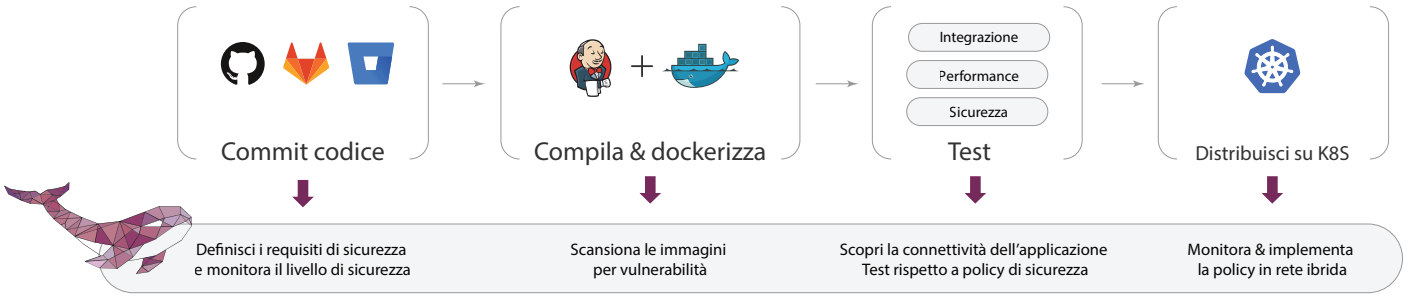
Automazione della sicurezza attraverso una rete ibrida

I team di sicurezza hanno bisogno di definire e applicare policy di sicurezza basate su requisiti di settore, normativi o aziendali. Tufin Orca semplifica questo processo controllando le comunicazioni e generando automaticamente policy di sicurezza. La sicurezza può, successivamente, adattare le policy di microsegmentazione per soddisfare le necessità aziendali in fase di cambiamento. La policy può essere applicata all'interno del cluster ed estesa automaticamente ai firewall circostanti attraverso un'integrazione con Tufin Orchestration Suite.



Automazione della sicurezza nella pipeline CI/CD

Storicamente la sicurezza viene affrontata in ritardo nel ciclo di vita dello sviluppo dell'applicazione, basandosi spesso su revisioni manuali che possono durare settimane. In un mondo ideale, i problemi di sicurezza vengono individuati e risolti in anticipo, una pratica comunemente indicata come "shift left". Con Tufin Orca, le policy di sicurezza diventano parte integrante della pipeline DevOps grazie a strumenti CI/CD comuni, come Jenkins per l'identificazione dei rischi e verificare la conformità prima dell'avvio della produzione.



Provalo gratis

Scopri come Tufin Orca protegge le tue applicazioni container e di microservizi.
Iscriviti online per ottenere un account gratuito: tufin.io

tufin
www.tufin.com

SB-03-19

tufin Orca