Akamai

WHITE PAPER

Mantenere la promessa dei container

Semplificazione e accelerazione della segmentazione per risorse e applicazioni critiche

Introduzione

La containerizzazione è rapidamente emersa come soluzione ideale per l'implementazione di applicazioni negli ambienti cloud e ibridi e la proliferazione dei container continua ad accelerare. Secondo Gartner, il 90% delle organizzazioni a livello globale riuscirà ad eseguire applicazioni containerizzate in produzione entro il 2026, partendo da un 40% nel 2021.[1] E secondo uno studio Forrester per Capital One, **l'86% dei leader IT intervistati ha dato priorità all'uso esteso dei container per più applicazioni**.[2]

> Secondo Gartner, **il 90% delle organizzazioni a livello globale** riuscirà ad eseguire applicazioni containerizzate in produzione entro il 2026, partendo da un 40% nel 2021

Tutto ciò, ovviamente, esercita ulteriore pressione sui responsabili della protezione degli ambienti IT affinché tengano il passo con l'implementazione dei container, in particolare in un modello DevOps che dà la priorità a velocizzare l'adozione e l'espansione. Sebbene siano emerse numerose soluzioni specializzate per la sicurezza dei container, queste entità specifiche della piattaforma e basate solo sui container finiscono per aumentare complessità e costi di gestione senza considerare il data center aziendale nel suo complesso, complicando maggiormente la vita ai team di sicurezza. È necessaria un'unica soluzione di sicurezza completa che funzioni in modo coerente su tutte le applicazioni e tecnologie in esecuzione in ambienti on-premise, cloud e ibridi, compresi i container.

Prima di analizzare le soluzioni, però, diamo una rapida occhiata al fenomeno dei container, alle sue forze trainanti e alle implicazioni dal punto di vista della sicurezza.

La pressione è alta: le esigenze aziendali stimolano l'adozione

Il passaggio ai container e la prevista crescita della loro adozione possono dipendere dalle esigenze aziendali imposte ai reparti IT aziendali. Le imprese moderne si aspettano di essere in grado di muoversi con velocità e flessibilità in risposta alle minacce competitive e alle opportunità di mercato. Necessitano di soluzioni che supportino l'innovazione e accelerino il time-to-market. E sono sempre alla ricerca di un miglioramento continuo dell'efficienza. In un mondo sempre più interconnesso, desiderano semplificare le operazioni commerciali digitali, con fornitori e venditori, partner commerciali e soprattutto con i propri clienti.

Questi sono alcuni dei motivi principali per cui l'IT aziendale sta valutando l'adozione del cloud o, più precisamente, di modelli ibridi on-premise/cloud. Sono anche i fattori trainanti della tendenza DevOps, che cerca di accelerare l'implementazione di applicazioni critiche eliminando i punti critici esistenti tra le idee e l'implementazione vera e propria, sfruttando l'automazione e la scalabilità automatica per mettere le applicazioni in produzione più rapidamente.

> **"Le organizzazioni spesso sottovalutano lo sforzo richiesto per gestire i container in produzione".**
>
> **- Gartner**

Tutto ciò aiuta a spiegare i motivi per cui i reparti IT abbiano adottato la containerizzazione. Rispetto alle macchine virtuali, i container sono molto più facili e veloci da avviare, consentendo la delivery tempestiva praticamente senza latenza e permettendo ai team di concentrarsi "sull'avviamento di servizi, non di server". Uno dei vantaggi principali dei container è la portabilità per gli odierni ambienti data center dinamici: i container, infatti, semplificano la migrazione delle applicazioni tra le strutture locali verso istanze multicloud. Ciò è ulteriormente migliorato grazie al coordinamento dei container tramite Kubernetes, o "K8", che consente ai team di distribuire e gestire volumi più elevati di applicazioni containerizzate su larga scala in più ambienti. Il coordinamento è sempre più considerato una best practice nell'implementazione e nella gestione dei container.

In breve, i container consentono all'IT di rispondere meglio alle esigenze aziendali di velocità, automazione, resilienza e disponibilità, e di farlo a un costo totale di proprietà inferiore rispetto ad altre tecnologie. L'implementazione, tuttavia, non è priva di svantaggi. "Le organizzazioni spesso sottovalutano lo sforzo richiesto per gestire i container in produzione", afferma un rapporto Gartner del 2019 sulle best practice di containerizzazione.[3] Nonostante l'interesse diffuso per la containerizzazione, la tecnologia è ancora emergente e le best practice per l'implementazione sicura non sono completamente consolidate. Secondo il rapporto 2022 State of Kubernetes Security di Red Hat, "la sicurezza è [ancora] una delle principali preoccupazioni alla base dell'adozione della tecnologia dei container, i cui problemi continuano a causare ritardi nell'implementazione delle applicazioni in produzione".[4] Chiaramente, le imprese non possono sfruttare tutti i potenziali vantaggi dei container senza una strategia di implementazione che includa necessariamente la sicurezza informatica.

> Come descritto nel 2022 State of Kubernetes Security Report di Red Hat, " **la sicurezza è una delle principali preoccupazioni alla base dell'adozione dei container** e problemi di sicurezza continuano a causare ritardi nell'implementazione delle applicazioni in produzione"

Cosa significa tutto ciò per il team di sicurezza?

"La sicurezza non può passare in secondo piano", afferma Gartner nel suo rapporto sulle best practice. "Deve essere integrata nel processo DevOps." Troppo spesso, però, non è così. Nella fretta di implementare la containerizzazione, ai team di sicurezza può sembrare di trovarsi al vertice di un "triangolo impossibile", un'illusione ottica nota anche come triangolo impossibile di Penrose (noto anche in Akamai come triangolo impossibile di Klein e Howard).

> Le soluzioni di sicurezza tradizionali non sono adattabili all'impresa moderna. Le soluzioni di sicurezza devono essere veloci, adattabili, dinamiche e integrarsi perfettamente in un approccio "DevSecOps".

Allo stesso modo in cui il vertice del triangolo appare illusoriamente più lontano rispetto agli altri due angoli, la sicurezza sembra essere in ritardo rispetto alle esigenze aziendali e alle iniziative IT per soddisfarle. Ma proprio come per il triangolo, si tratta di un'illusione ottica, le soluzioni di sicurezza sono in realtà più vicine di quanto sembri. I team devono semplicemente andare oltre le ingombranti soluzioni legacy su cui hanno fatto affidamento in passato e cercare soluzioni che corrispondano alle modalità operative odierne dell'IT aziendale e che si adattino perfettamente a un approccio "DevSecOps". Ciò significa una soluzione che sia veloce, adattabile e dinamica e che di per sé utilizzi l'approccio del playbook DevOps. La cosa più importante è una soluzione svincolata dai sistemi operativi e dalla piattaforma sottostanti per semplificare l'implementazione e la gestione.

Triangolo impossibile Klein & Howard

Perché i controlli "nativi" non sono sufficienti

Agli albori della virtualizzazione e della migrazione al cloud, le aziende erano spesso indotte a credere che i controlli nativi del cloud fossero sufficienti per visualizzare, gestire e proteggere i propri carichi di lavoro. Solo dopo molti tentativi ed errori i responsabili IT si sono resi conto che era necessario un modello di gestione sovrapposto che integrasse soluzioni di terze parti in grado di garantire la sicurezza al di là dei controlli nativi.

Come hanno affermato Gartner e Forrester Research, una strategia di implementazione di container di successo si basa sulla "triade del container":

- Eseguire i container in modo portabile e indipendente dalla piattaforma, implementandoli senza sforzi su più architetture cloud e on-premise
- Sfruttare il coordinamento per eseguire e gestire i container su larga scala
- Utilizzare strumenti di terze parti per la gestione, la visibilità e la sicurezza dei container

A differenza dei precedenti tentativi di virtualizzazione e cloud, il settore dei container ha riconosciuto fin dall'inizio che i sistemi di gestione nativi del cloud, e i controlli di sicurezza in particolare, sono inadeguati per una strategia containerizzata efficace. Nello studio di Gartner sulle soluzioni di gestione dei container, **il 65% degli intervistati ha dichiarato di voler sfruttare strumenti di gestione di terze parti per visualizzare, gestire e proteggere i carichi di lavoro containerizzati**.[5] Tuttavia, questi strumenti di terze parti devono funzionare perfettamente sia su istanze locali che cloud e adottare un approccio granulare per evitare gli ostacoli dei metodi misti e ingombranti utilizzati in passato, come gruppi di sicurezza, VLAN e firewall, che offrono visibilità zero e granularità trascurabile.

Akamai Guardicore Segmentation favorisce l'adozione dei container

Akamai Guardicore Segmentation è stato progettato per rispondere alle sfide delle attuali infrastrutture di data center ibride e dinamiche. Forniamo visibilità completa su tutte le applicazioni e i carichi di lavoro in esecuzione su più ambienti e consentiamo una segmentazione definita dal software granulare e facilmente implementabile tramite la creazione, l'implementazione e l'applicazione rapida di policy di sicurezza per applicazioni singole o raggruppate logicamente.

Cerchiamo di essere chiari: Akamai Guardicore Segmentation non è un prodotto singolo destinato esclusivamente alla gestione dei container. Piuttosto, la sicurezza dei container è una funzionalità chiave della piattaforma, che funziona in modo coerente in ambienti misti che possono includere anche server bare metal, macchine virtuali, carichi di lavoro senza server e dispositivi remoti Di conseguenza, forniamo alle organizzazioni un'unica soluzione completa per proteggere tutti i data center e le risorse cloud indipendentemente da dove risiedono o da come vengono implementate, eliminando la necessità di gestire più soluzioni. E poiché la nostra soluzione è svincolata dalle piattaforme e dai sistemi operativi sottostanti, le policy di sicurezza seguono le applicazioni e i carichi di lavoro mentre si spostano tra ambienti on-premise e cloud, migliorando il fattore di portabilità che rende i container attraenti per l'implementazione delle applicazioni nelle infrastrutture cloud ibride.

> La sicurezza dei container è una funzionalità chiave della piattaforma Akamai Guardicore Segmentation, che funziona in modo coerente in ambienti data center dinamici ed eterogenei

Per quanto riguarda i container, Akamai Guardicore Segmentation funziona posizionando gli agenti sui nodi host dei container, consentendo la visibilità dell'intero cluster di container, compresi i flussi di comunicazione da pod a pod e da pod a macchina virtuale. Ciò consente l'implementazione e l'applicazione di policy di sicurezza molto granulari per processo, utente e nome di dominio completo (FQDN). In uno scenario di coordinamento, supportiamo il coordinamento K8 e consentiamo la visibilità nei metadati Kubernetes e OpenShift per un contesto superiore. Un modello di etichettatura flessibile consente agli operatori di esprimere policy utilizzando la terminologia K8 nativa. Per l'applicazione di K8, sfruttiamo la tecnologia CNI (Container Network Interface) nativa, un metodo non invasivo per l'applicazione delle policy in K8 senza limitazioni di scalabilità. I modelli dedicati consentono agli utenti di isolare le applicazioni Kubernetes business-critical, inclusi spazi dei nomi, applicazioni o altri oggetti. Inoltre, scaliamo alle quantità dei carichi di lavoro e ai tassi di modifica K8. Poiché la nostra soluzione funziona in modo simile anche con tutti gli altri carichi di lavoro aziendali, costituisce un'unica soluzione per visualizzare, gestire e proteggere le risorse nell'intera azienda.

Di particolare importanza in un ambiente DevOps, le policy di sicurezza create si integreranno efficacemente nei processi di integrazione CI/CD (Continuous Integration and Continuous Deployment), contribuendo a garantire che la sicurezza non passi in secondo piano, ma sia completamente integrata nel modello di delivery.

Conclusione

I container sono una parte sempre più integrante di molti ambienti aziendali. Possono aumentare l'efficienza dell'utilizzo delle risorse, semplificare i processi e consentire una maggiore portabilità e scalabilità. Allo stesso tempo, la sicurezza integrata che forniscono non è sufficiente, soprattutto per le aziende che utilizzano un ambiente ibrido.

Se cercate una soluzione di sicurezza in grado di crescere insieme alla vostra azienda, assicuratevi di scegliere uno strumento indipendente dalla piattaforma che fornisca informazioni granulari sui processi end-to-end, indipendentemente da dove vengono eseguiti. Akamai Guardicore Segmentation fa questo e altro ancora, offrendo la gamma di caratteristiche e capacità di cui le aziende moderne necessitano per essere preparate sia per il presente che per il futuro.

Utilizzando Akamai Guardicore Segmentation, il vostro team di sicurezza può ottenere una sicurezza coerente in ambienti data center dinamici ed eterogenei. In tal modo, potete aiutare i team IT a mantenere la promessa della containerizzazione, realizzando uno sviluppo e un'implementazione rapidi, convenienti e sicuri di applicazioni critiche essenziali per le esigenze aziendali della vostra azienda.

Semplificate la sicurezza nell'intero ambiente. Ulteriori informazioni sulla nostra potente soluzione di sicurezza unificata per container e altro ancora sono disponibili all'indirizzo akamai.com/guardicore.

1 Chandrasekaran Arun e Wataru Katsurashima. "Guida per i responsabili dell'innovazione sull'ecosistema dei container nativi del cloud", Gartner, 18 agosto 2021.

2 "L'adozione dei container del cloud nelle aziende", Forrester, giugno 2020.

3 "Best practice per l'esecuzione di container e Kubernetes in fase di produzione", Gartner, 25, febbraio 2019.

4 "Stato del rapporto sulla sicurezza di Kubernetes", Red Hat, maggio 2022.

5 "Gartner prevede un deciso aumento dei profitti per le aziende fornitrici di servizi e software per la gestione dei container a livello globale per tutto il 2024", 25 giugno 2020.

Akamai protegge l'experience dei vostri clienti, dipendenti, sistemi e dati aiutandovi ad integrare la sicurezza in tutti i vostri prodotti, ovunque vengano creati e distribuiti La visibilità della nostra piattaforma sulle minacce globali ci aiuta ad adattare ed evolvere la vostra strategia di sicurezza per favorire il modello Zero Trust, bloccare i ransomware, proteggere app e API o contrastare gli attacchi DDoS, offrendovi la sicurezza necessaria per concentrarvi costantemente sull'innovazione, sull'espansione e sulla trasformazione di tutto il possibile. Per ulteriori informazioni sulle soluzioni per la sicurezza, il computing e la delivery di Akamai, visitate il sito akamai.com e akamai.com/blog o seguite Akamai Technologies su Twitter e LinkedIn. Data di pubblicazione: 05/23.