Sicurezza Kubernetes native

Di cosa si tratta e perché è importante

Introduzione

Negli ultimi cinque anni il software per l'infrastruttura ha beneficiato della crescita esponenziale che ha interessato il settore delle architetture e delle tecnologie cloud native. Questi nuovi approcci permettono alle organizzazioni di sviluppare ed eseguire le applicazioni in modo più scalabile, flessibile e dinamico rispetto al passato. Container, microservizi, API dichiarative e tipi primitivi riducono le risorse sottostanti necessarie per l'elaborazione, la rete e lo storage, mentre la distribuzione continua e le procedure DevOps permettono a ogni azienda, indipendentemente dalla dimensione e dal settore in cui opera, di rilasciare software in modo più rapido e affidabile.

Nell'ambito di questo cambiamento sistemico riveste un ruolo di primo piano la piattaforma open source per l'orchestrazione dei container Kubernetes. Kubernetes è lo standard di settore per l'automazione del deployment e della gestione di applicazioni cloud native in produzione.

L'adozione di tecnologie cloud native introduce nuove problematiche di sicurezza, ma offre anche l'opportunità di migliorare le strategie di sicurezza esistenti. L'evoluzione cloud native ha fatto emergere un nuovo ambiente di rischio, che si caratterizza per una superficie di attacco dinamica, attiva e in continua evoluzione, come sono gli stessi container. Le applicazioni di oggi non sono più blocchi monolitici dai confini ben definiti, ma soluzioni volutamente frammentate, spesso in microservizi; ciò significa che la sicurezza deve operare su una serie di componenti interconnessi tra loro ma che si interfacciano in maniera autonoma. Inoltre, le caratteristiche principali dei container possono essere sfruttate da hacker per compiere attacchi più rapidi e scalabili rispetto al passato.

Analogamente alle macchine virtuali e agli ambienti cloud pubblici, i container e Kubernetes introducono nuovi livelli infrastrutturali, ciascuno con specifiche necessità in fatto di sicurezza. In risposta a questi cambiamenti, i prodotti del settore della sicurezza di solito adottano uno dei seguenti approcci:

1. Le soluzioni basate su host o su reti estendono la protezione ai container.
2. Le soluzioni si concentrano sulla sicurezza degli ambienti containerizzati.
3. Le soluzioni si concentrano sulla sicurezza dei container e di Kubernetes.

Differenze tra gli approcci alla sicurezza dei container

In breve: la sicurezza Kubernetes native potenzia gli approcci esistenti alla sicurezza dei container orientandoli alla difesa degli ambienti Kubernetes.

La prima categoria di strumenti per la sicurezza punta a proteggere gli ambienti basati su cloud adottando controlli per le macchine virtuali e gli endpoint (o le reti di endpoint), ad esempio attraverso l'applicazione di firewall. La maggior parte di questi strumenti però si concentra su uno scenario di utilizzo specifico (come ad esempio la gestione delle vulnerabilità, il rilevamento delle intrusioni o l'uso di firewall per applicazioni web) e mal si adatta alla sicurezza dei container, dove l'attenzione è dedicata ai carichi di lavoro e ai loro dati, e non più ai server e agli indirizzi IP.

Inoltre, questi strumenti non garantiscono la sicurezza per tutto il ciclo di vita delle applicazioni cloud native, e non sono progettati per gestire la natura dinamica, altamente scalabile e temporanea delle applicazioni containerizzate.

La seconda categoria comprende quelle soluzioni che forniscono protezione per tutto il ciclo di vita dei container e hanno un'architettura incentrata sui container. Rientrano in questa categoria la maggior parte degli strumenti per la sicurezza dei container. Queste soluzioni offrono funzionalità che operano a livello dei singoli container, sul runtime o motore (ad esempio Docker) e sugli artefatti usati per eseguirli (ovvero le immagini dei container). Lo svantaggio di questo approccio però è che non fornisce garanzie di sicurezza a livello di Kubernetes.

La terza categoria supera le soluzioni incentrate sui container per fornire strumenti e procedure di sicurezza specifiche per gli ambienti Kubernetes. Un'architettura Kubernetes native fornisce protezione per tutto il ciclo di vita delle applicazioni cloud native e interviene sui vettori di minaccia sia per i container sia per Kubernetes. Red Hat® Advanced Cluster Security for Kubernetes ha aperto la strada all'approccio Kubernetes native.

Che cos'è la sicurezza Kubernetes native

In breve: una soluzione di sicurezza per essere considerata Kubernetes native deve rispettare sei criteri fondamentali.

La sicurezza Kubernetes native parte dal presupposto che la protezione si implementa più efficacemente quando è in linea con il sistema che gestisce tutte le applicazioni containerizzate dell'organizzazione.
Per essere considerata Kubernetes native, una piattaforma di sicurezza deve presentare le seguenti caratteristiche:

1. Deve integrarsi direttamente con il server API Kubernetes per ottenere visibilità sui carichi di lavoro e sull'infrastruttura
2. Deve valutare le vulnerabilità nel software Kubernetes
3. Le sue funzionalità di sicurezza, inclusa la gestione dei criteri, devono essere basate sulle risorse disponibili all'interno del modello di oggetti Kubernetes, che include spazi dei nomi, deployment, servizi, pod e altro
4. Deve analizzare i dati dichiarativi delle configurazioni e degli artefatti specifici di Kubernetes, come i manifest dei carichi di lavoro
5. Deve gestire l'applicazione utilizzando le funzionalità di sicurezza integrate in Kubernetes, in modo da aumentare i livelli di automazione, scalabilità e affidabilità
6. Deve essere distribuita ed eseguita come un'applicazione Kubernetes, incluse le integrazioni e il supporto degli strumenti comuni nelle toolchain cloud native

Le organizzazioni che desiderano proteggere gli ambienti Kubernetes devono identificare e ordinare per priorità le esigenze di sicurezza dei principali scenari di utilizzo, con particolare attenzione a visibilità, gestione delle vulnerabilità, segmentazione della rete, gestione della configurazione, conformità, rilevamento delle minacce e risposta agli incidenti. Una piattaforma di sicurezza Kubernetes native che rispetta tutti e sei i criteri è in grado di soddisfare queste e altre esigenze di sicurezza basate su scenari di utilizzo.

Vantaggi della sicurezza Kubernetes native

In breve: una soluzione di sicurezza Kubernetes native offre vantaggi chiave rispetto ad altre soluzioni, come protezione superiore, tempi e costi ridotti e rischio operativo minimo.

Le organizzazioni che adottano un approccio alla sicurezza Kubernetes native ottengono tre vantaggi chiave:

1. **Protezione superiore:** la sicurezza Kubernetes native elimina i punti ciechi su tutta la superficie di attacco relativa all'agente di orchestrazione, in questo modo i team di sicurezza possono individuare vulnerabilità critiche e vettori di minaccia che altrimenti passerebbero inosservati.
2. **Tempi e costi ridotti:** un approccio Kubernetes native permette di ridurre l'investimento complessivo in termini di tempo, iniziative e personale necessario per adottare una strategia di sicurezza. Inoltre, grazie alla capacità di ottenere contesto dettagliato sull'infrastruttura e le applicazioni Kubernetes, consente di ottimizzare verifica, monitoraggio e correzione delle problematiche relative alla sicurezza.
3. **Rischio operativo minimo:** una soluzione di sicurezza Kubernetes native riduce al minimo l'impatto delle operazioni critiche dato che sfrutta per l'applicazione delle policy la scalabilità e la resilienza dell'agente di orchestrazione. Questo approccio evita anche i conflitti e la complessità che possono generare rischio operativo per le applicazioni principali.

Aumenta la protezione con la sicurezza Kubernetes native

Quando le organizzazioni scelgono di abbandonare l'esecuzione individuale dei container in favore dell'orchestrazione tramite un sistema come Kubernetes ottengono una serie di vantaggi operativi, tra cui la possibilità di eseguire i container su qualsiasi infrastruttura, un rilevamento dei servizi e bilanciamento del carico coerenti, oltre ad aggiornamenti e rilasci automatizzati. L'introduzione di una nuova piattaforma però espone anche a dei rischi: infatti la superficie di attacco dell'infrastruttura aumenta ed emergono vulnerabilità legate ad esempio ai software open source, alle nuove configurazioni e a vettori di attacco imprevisti.

Il livello di astrazione che Kubernetes fornisce a sviluppatori e team operativi può facilmente creare punti ciechi per le soluzioni di sicurezza tradizionali. I container e le applicazioni che questi creano non sono più limitati da confini e risorse fisici come i server; e siccome Kubernetes rende l'elaborazione, la rete e lo storage totalmente programmatici, eventuali lacune nella sicurezza rischiano di passare inosservate.

Elimina i punti ciechi con più visibilità e informazioni approfondite

In breve: le soluzioni di sicurezza Kubernetes native forniscono alle organizzazioni una visione globale della sicurezza del loro ambiente Kubernetes.

Il primo passo per una strategia di sicurezza efficace è la visibilità sull'ambiente e sul suo stato di sicurezza generale. La sicurezza Kubernetes native offre la visibilità diretta su Kubernetes grazie all'integrazione con il server API Kubernetes. Grazie a questa funzionalità è possibile monitorare la sicurezza dei container eseguiti sui cluster Kubernetes, ma soprattutto la sicurezza delle risorse e degli oggetti per come li vede Kubernetes. Queste astrazioni (deployment, daemonset, servizi, pod e altre risorse) fanno da riferimento per controller, raggruppamenti di reti e carichi di lavoro, quindi disporre di informazioni dettagliate su di loro fornisce un contesto a livello delle applicazioni di importanza fondamentale.

Per contro le soluzioni di sicurezza incentrate sui container offrono visibilità solo a livello dei singoli container e delle immagini corrispondenti, tralasciando la visibilità delle intere applicazioni. Red Hat Advanced Cluster Security integra il monitoraggio delle attività all'interno dei singoli container con la visibilità incentrata sui deployment, offrendo così ai clienti un quadro esaustivo e on demand sulle applicazioni Kubernetes e sulla loro sicurezza.

Visibilità sulle configurazioni

La visibilità diretta su Kubernetes, in particolare la valutazione approfondita di configurazioni e impostazioni, fornisce alle aziende un quadro sul livello di sicurezza del loro ambiente Kubernetes. La sicurezza Kubernetes native automatizza i controlli delle policy per garantire l'applicazione delle procedure di sicurezza consigliate e identificare configurazioni errate potenzialmente pericolose per i dati delle applicazioni. Red Hat Advanced Cluster Security svolge un'analisi continua su centinaia di configurazioni, affinché sia possibile verificare in ogni momento la sicurezza generale degli ambienti Kubernetes. Tra le altre cose, le configurazioni oggetto di analisi includono:

- Autorizzazioni basate sui ruoli.
- Accesso ai segreti.
- Traffico di rete consentito.
- Impostazioni dei componenti del piano di controllo.
- Altre impostazioni.

Le soluzioni incentrate sui container invece si focalizzano sulle configurazioni relative al motore di runtime dei container e ai singoli container (come i privilegi dei container e le funzionalità del kernel). Queste soluzioni non operano su tutte le categorie di comandi di Kubernetes, quindi alcune configurazioni non sicure potrebbero passare inosservate e causare exploit.

Visibilità sulla conformità

Un altro elemento fondamentale per ottenere una visibilità Kubernetes native è la conformità, in particolare a standard di settore come PCI, HIPAA, SOC 2 e FedRAMP. Anche se il profilo di sicurezza di un'organizzazione è ineccepibile, la sicurezza dell'infrastruttura e delle applicazioni Kubernetes deve essere opportunamente verificata per garantire sempre la conformità. Controlli e certificazioni possono richiedere misure di sicurezza avanzate, come la completa visibilità su Kubernetes.

L'approccio Kubernetes native di Red Hat Advanced Cluster Security prevede l'applicazione di controlli specifici per i cluster Kubernetes, che sono automaticamente associati ai controlli di conformità. Le organizzazioni ottengono così una visione in tempo reale del tasso di successo/insuccesso. Ad esempio, è possibile limitare gli accessi alla rete tra Internet e i servizi che elaborano dati sensibili o individuare le vulnerabilità nella versione di Kubernetes in uso.

Le soluzioni di sicurezza incentrate sui container invece eseguono controlli di conformità, in genere basati sul benchmark CIS per Docker, senza tenere conto del sistema di orchestrazione specifico e danno luogo a valutazioni lacunose sulla conformità generale di un certo ambiente.

Visibilità sull'isolamento dei carichi di lavoro

I container per loro natura offrono un minor isolamento rispetto alle macchine virtuali, soprattutto in scenari che richiedono multitenancy. Uno dei vantaggi fondamentali di Kubernetes è la vasta offerta di opzioni per l'isolamento dei carichi di lavoro su container in esecuzione. La difesa di qualsiasi ambiente Kubernetes infatti non può prescindere da una strategia di isolamento, e queste opzioni forniscono confini fisici (cluster e nodi) e virtuali, applicabili tramite funzioni come spazio dei nomi e policy di rete.

Adottare una strategia di sicurezza Kubernetes native significa disporre di queste diverse soluzioni per riconoscimento e implementazione di carichi di lavoro isolati su Kubernetes.

Invece la sicurezza incentrata sui container in buona sostanza ignora questi confini, interessandosi principalmente degli host su cui sono eseguiti i diversi container: risulta quindi difficile capire se le applicazioni e i loro servizi sono sufficientemente isolati.

Red Hat Advanced Cluster Security fornisce informazioni che:

- si basano sulla comprensione approfondita di cluster, spazio dei nomi e pod.
- derivano dai dati raccolti da tutti gli host.
- si integrano con le policy di rete di Kubernetes per fornire un quadro completo sull'isolamento delle applicazioni.

Una strategia di sicurezza risulta efficace quando è costruita su fondamenta solide, la visibilità completa su Kubernetes è quindi un elemento imprescindibile per la protezione ottimale delle applicazioni cloud native.

Individua vulnerabilità e vettori di minaccia critici

In breve: le soluzioni di sicurezza Kubernetes native individuano e proteggono gli ambienti Kubernetes da vulnerabilità, vettori di attacco e configurazioni errate.

Per proteggere i carichi di lavoro eseguiti su Kubernetes è essenziale conoscere i propri ambienti cloud native e proteggerli da minacce specifiche, quindi non solo dalle minacce per i container ma da quelle che interessano l'intera piattaforma Kubernetes. L'estensione e la complessità insite in Kubernetes, oltre ai contributi continui per il miglioramento della piattaforma della Cloud Native Computing Foundation (CNCF), delle community open source e di altre organizzazioni interessate, generano una serie di vettori di attacco in continua crescita ed evoluzione. Le minacce alla sicurezza specifiche di Kubernetes con impatto pubblico sono state:

- Una dashboard di Kubernetes con una configurazione non sicura nell'ambiente cloud di Tesla[1] ha permesso a utenti malintenzionati di ottenere l'accesso alle credenziali degli account e minare criptovalute.
- Un servizio di Shopify esposto a una vulnerabilità SSRF (Server-Side Request Forgery, falsificazione delle richieste lato server)[2] rischiava di fornire a utenti malintenzionati le credenziali del kubelet e di conseguenza l'accesso root a tutti i container.

Anche la community cloud native conferma la presenza di queste minacce alla sicurezza di Kubernetes. Un primo controllo di sicurezza svolto nel 2020[3] ha rilevato su Kubernetes alcune aree di fragilità in fatto di sicurezza ed elaborato un modello di rischio che coinvolge otto componenti principali di Kubernetes. La sicurezza Kubernetes native di Red Hat Advanced Cluster Security poggia su questa e altre ricerche svolte nell'ecosistema cloud native e offre funzionalità all'avanguardia per identificare vulnerabilità, configurazioni errate ed exploit in tutti gli ambienti Kubernetes.

1 *Lily Hay Newman, "Hack Brief: Hackers Enlisted Tesla's Public Cloud to Mine Cryptocurrency", Wired, 28 febbraio 2018.*

2 *Sean Michael Kerner, "How Shopify Avoided a Data Breach, Thanks to a Bug Bounty", eWeek, 17 dicembre 2018.*

3 *"Kubernetes Final Report", GitHub (kubernetes/community/wg-security-audit/findings), 6 agosto 2019.*

Rileva vulnerabilità specifiche di Kubernetes

Tra i vari componenti di Kubernetes, il server API è senza dubbio il più importante da salvaguardare, dato il ruolo fondamentale che riveste nell'orchestrazione e nella gestione delle applicazioni containerizzate. Un esempio di vulnerabilità critica che influisce sul server API Kubernetes è CVE-2018- 1002100: una vulnerabilità particolarmente difficile da individuare perché permettere a utenti malintenzionati di compromettere un intero cluster tramite richieste autorizzate. Scoperta solo tre anni dopo il primo rilascio di Kubernetes, questa vulnerabilità era presente su tutte le versioni precedenti.

La sicurezza Kubernetes native individua automaticamente le vulnerabilità di Kubernetes note, così amministratori e operatori dei cluster possono gestire i rischi più insidiosi per i loro ambienti.

Invece le soluzioni incentrate sui container si preoccupano esclusivamente delle vulnerabilità che coinvolgono le immagini dei container. Quindi anche se i container con meno vulnerabilità risultano più sicuri, con un'infrastruttura Kubernetes mal protetta non sono esenti da attacchi. Red Hat Advanced Cluster Security individua proattivamente i cluster con il maggior numero di vulnerabilità proprie di Kubernetes e permette agli utenti di definire policy in base alle vulnerabilità individuali.

Rileva configurazioni errate specifiche di Kubernetes

Come le vulnerabilità anche le configurazioni errate dei comandi centrali di Kubernetes possono generare exploit ed esposizioni dei dati sensibili, soprattutto se vengono propagate automaticamente in tutti i cluster. Le configurazioni errate possono derivare sia da errori degli utenti sia da una scarsa dimestichezza con Kubernetes. Con configurazione errata si intende ad esempio la possibilità di assegnare autorizzazioni amministrative complete per i cluster all'account utente e di servizi non qualificato tramite il controllo degli accessi basato sui ruoli (RBAC), oppure di esporre inutilmente i segreti di Kubernetes permettendo ai deployment di eseguire il pull dei segreti anche quando non è necessario.

Integrando questi comandi, Red Hat Advanced Cluster Security avvisa tempestivamente le organizzazioni in caso emergano configurazioni errate e permette loro di migliorare nel complesso la gestione delle configurazioni.

Le soluzioni incentrate sui container prendono in considerazione solo le configurazioni problematiche del runtime dei container o dei singoli container; quindi la protezione che forniscono è parziale e facilmente eludibile. Poter gestire le configurazioni errate di un container specifico non è abbastanza poiché con una configurazione errata di Kubernetes un utente malintenzionato può comunque compromettere il nodo su cui è eseguito il container; e anche se quest'ultimo è configurato correttamente risulta compromesso.

Red Hat Advanced Cluster Security colma questa lacuna ricercando le configurazioni errate sia di Kubernetes sia dei container.

Proteggi le comunicazioni di rete in ingresso e in uscita

Kubernetes mette a disposizione anche una vasta gamma di opzioni di rete, tra cui soluzioni per la comunicazione tra pod attraverso specifiche per le policy di rete. Queste impostazioni però hanno conseguenze sulla sicurezza che rischiano di essere sottovalutate. Ad esempio, se a un determinato pod non viene applicata nessuna policy di rete di Kubernetes, allora tutto il traffico di rete (in ingresso e in uscita) è autorizzato perché per impostazione predefinita Kubernetes non applica policy di rete.

L'approccio alla sicurezza Kubernetes native determina immediatamente la topologia di rete in base a come le policy di rete sono configurate, solitamente dai team operativi e DevOps.

Le soluzioni incentrate sui container invece determinano come è configurato il traffico di rete in base a regole all'interno delle loro interfacce proprietarie e al di fuori di Kubernetes. Red Hat Advanced Cluster Security garantisce l'applicazione di regole per il traffico di rete coerenti, aperte e standardizzate in tutti gli ambienti Kubernetes.

La protezione ottimale delle applicazioni containerizzate passa necessariamente prima dalla protezione dell'infrastruttura containerizzata su cui queste sono eseguite. Questo passaggio richiede funzionalità che solo una soluzione di sicurezza Kubernetes native può offrire, come la capacità di riconoscere le vulnerabilità critiche, i vettori di minaccia e le configurazioni errate.

Riduci tempi e costi con la sicurezza Kubernetes native

Kubernetes è una piattaforma unificata concepita per agevolare il provisioning e l'operatività dei servizi per l'infrastruttura, sia nel cloud sia on premise. Permette di risparmiare tempo e ridurre i costi, eliminando la complessità operativa e le incongruenze, e semplificando i flussi di lavoro per sviluppatori, team operativi e team di sicurezza. In maniera analoga, le organizzazioni dovrebbero proteggere i loro ambienti Kubernetes preferendo soluzioni che richiedono meno investimenti in termini di tempo e denaro.

Per scegliere una soluzione di sicurezza idonea è opportuno porsi le seguenti domande:

- La soluzione accelera la curva di apprendimento dei team di sicurezza e DevOps?
- La soluzione permette ai team di accelerare analisi, indagine e correzione degli incidenti?
- La soluzione offre funzionalità per l'automazione e la raccolta dei dati rilevanti?

Un'architettura Kubernetes native soddisfa tutti questi requisiti.

Curva di apprendimento più semplice per i team

In breve: le soluzioni di sicurezza Kubernetes native semplificano la sicurezza di Kubernetes integrandosi con astrazioni e strumenti standardizzati e open source già in uso dai team DevOps.

La complessità mina la sicurezza. Kubernetes, con i numerosi componenti e strumenti associati, richiede agli sviluppatori e ai team operativi di apprendere nuove competenze e adottare nuovi flussi di lavoro. L'ultima cosa di cui i team hanno bisogno quindi è aumentare la complessità adottando una soluzione di sicurezza completamente separata che richieda ulteriori investimenti in termini di processi e toolchain.

Utilizza un unico framework conosciuto

Un'architettura Kubernetes native riduce al minimo il numero di nuove interfacce, configurazioni e modelli di risorse che gli utenti devono imparare a utilizzare per proteggere i carichi di lavoro cloud native. Per compilare e distribuire applicazioni containerizzate, gli sviluppatori e i team operativi si servono già di astrazioni standardizzate come i manifest Kubernetes. Le funzionalità di sicurezza di Red Hat Advanced Cluster Security si basano sulle stesse astrazioni; quindi sviluppatori, team operativi e team di sicurezza possono utilizzare un unico framework per compilare, distribuire ed eseguire le applicazioni.

Ad esempio, gli utenti di Red Hat Advanced Cluster Security possono vedere i metadati dei file dei manifest Kubernetes e individuare un contesto rilevante per la sicurezza per un'intera applicazione e la sua funzione. Per contro, le soluzioni incentrate sui container si concentrano sui Dockerfile, che comprendono soltanto i comandi necessari per compilare le immagini.

Red Hat Advanced Cluster Security sfrutta anche strumenti standardizzati di gestione dei pacchetti per distribuirli allo stesso modo delle altre applicazioni containerizzate. Ad esempio, Red Hat Advanced Cluster Security esegue il deployment utilizzando i grafici Helm mentre le soluzioni incentrate sui container si affidano a opzioni di gestione dei pacchetti potenzialmente non compatibili con Kubernetes. Basare la strategia di sicurezza su astrazioni e pacchetti standardizzati e open source permette di eliminare il divario tra i team di sicurezza e gli altri stakeholder; si agevola così la collaborazione e si risparmia tempo prezioso.

Sfrutta il modello *una singola configurazione utilizzabile ovunque* per agevolare l'*integrazione a monte*

La sicurezza Kubernetes native riduce lo sforzo necessario per implementare configurazioni sicure: grazie a Kubernetes infatti è possibile orchestrare configurazioni dichiarative in tutto l'ambiente sfruttando il modello *una singola configurazione utilizzabile ovunque*. In questo modo le organizzazioni possono automatizzare facilmente centinaia di controlli per policy e procedure di sicurezza consigliate.

Con Red Hat Advanced Cluster Security, gli utenti riescono a propagare un'unica configurazione (ad esempio una policy di rete) in tutti i pod di un deployment; non come alcune soluzioni incentrate sui container che richiedono di configurare i comandi a livello di sistema su tutti gli host di un cluster. Si può dire che le soluzioni incentrate sui container non approfittano a pieno della scalabilità e della resilienza offerte da Kubernetes; Red Hat Advanced Cluster Security invece sa trarre il massimo da queste caratteristiche dei comandi nativi di Kubernetes a vantaggio dell'organizzazione.

La sicurezza delle applicazioni containerizzate dipende dai comandi implementati su tutta la catena di distribuzione del software e inizia ben prima che i container siano eseguiti. Questo approccio dà a sviluppatori e team DevOps l'opportunità di sfruttare la loro conoscenza di Kubernetes per spingere l'organizzazione verso l'*integrazione a monte* e una mentalità Security as Code. La maggior parte dei team ha già dimestichezza con questo concetto, visto che ricorda da vicino le efficaci metodologie Infrastructure as Code in uso oggi.

La sicurezza Kubernetes native arricchisce le iniziative esistenti con funzionalità come l'applicazione di policy di deployment tramite il controllo ammissione dinamico integrato in Kubernetes. Le soluzioni incentrate sui container utilizzano le architetture tradizionali per applicare le policy al momento del deployment e non danno a sviluppatori e team DevOps la possibilità di creare un collegamento profondo tra misure di sicurezza e toolchain Kubernetes.

Allineando la sicurezza con le astrazioni e le toolchain che sviluppatori e team DevOps già conoscono, Red Hat Advanced Cluster Security permette alle organizzazioni di risparmiare tempo e ridurre i costi durante l'applicazione di strategie di sicurezza cloud native.

Analisi e correzione più rapide

In breve: le soluzioni di sicurezza Kubernetes native semplificano indagine, risposta agli incidenti e valutazione dei rischi grazie al contesto dettagliato derivato direttamente da Kubernetes.

Oggi i team di sicurezza devono faticare molto per ottenere le risposte che cercano. Gestiscono infatti un insieme complesso e frammentario di strumenti con il solo ausilio di flussi di lavoro manuali e integrazioni personalizzate a fare da collante. Questo significa che si trovano spesso a vagliare un flusso infinito di avvisi; e l'introduzione dei container non ha certo semplificato la situazione. I team di sicurezza devono affrontare sfide notevoli per proteggere gli ambienti cloud native, come ad esempio:

- Gli incidenti e i nuovi modelli di minaccia non lineari (indicatori di attacco e compromissione) sono sparsi in tutti i componenti delle applicazioni e negli ambienti distribuiti, perché i container sono orchestrati in modo dinamico sulle macchine.
- Gli strumenti e i flussi di lavoro esistenti non riescono a tenere il passo con l'enorme mole di dati prodotti da tanti container.
- Molti approcci tradizionali alla risposta agli incidenti, che sfruttano i dati stateful per studiare gli attacchi e scoprire le tecniche adottate dagli utenti malintenzionati, risultano inefficaci a causa della natura temporanea dei container.

Rileva le minacce in modo più accurato

Il contesto dettagliato che la sicurezza Kubernetes native fornisce accelera le indagini sugli incidenti di sicurezza e la conseguente correzione dei problemi alla base. Le applicazioni containerizzate, in particolare quelle che utilizzano le architetture di microservizi, permettono un rilevamento delle minacce più semplice e accurato perché lavorano, per osservare e identificare le anomalie, su componenti più piccoli con un'attività prevedibile. Unendo queste competenze al contesto aggiuntivo fornito da Kubernetes, le organizzazioni possono facilmente distinguere le vere minacce dai falsi positivi.

Il contesto fornito da Kubernetes comprende informazioni che interessano l'intero deployment, tra cui:

- Quali processi saranno eseguiti.
- Se esistono limiti delle risorse per evitare che i container interferiscano tra loro.
- Quali privilegi e funzionalità ha ciascun container.
- Se il file system root dei container è scrivibile.
- Quali dispositivi, configurazioni e segreti sono presenti.

Comprende anche metadati preziosi come le etichette che aiutano a identificare la natura di un'applicazione e le annotazioni che aggiungono descrizioni sull'applicazione.

Red Hat Advanced Cluster Security sfrutta questo contesto per allineare i dati pertinenti di tutti i carichi di lavoro (le informazioni sulle immagini dei container e sull'attività a livello di sistema dai singoli container al runtime) con i dati di configurazione forniti da Kubernetes. La sicurezza di Kubernetes influenza quella dei singoli container e viceversa.

Acquisendo dati sui singoli container e sulle loro interazioni, Red Hat Advanced Cluster Security permette di concentrarsi sui problemi di sicurezza distribuiti in ambienti di grandi dimensioni. Le soluzioni incentrate sui container invece trascurano questi metadati di Kubernetes, fornendo ai team di sicurezza una conoscenza solo parziale della causa radice degli incidenti.

Una soluzione Kubernetes native integra un insieme di dati eterogenei derivati da container, Kubernetes e ciclo di vita delle applicazioni (dalla creazione delle immagini all'esecuzione dei container). Grazie a queste informazioni, i team possono confrontare l'effettiva attività di runtime con quali erano le configurazioni dichiarative dei container in base alle impostazioni di Kubernetes. In questo modo Red Hat Advanced Cluster Security riesce a individuare attività di runtime anomale o sospette con maggiore precisione, evitando allo stesso tempo i falsi positivi e riducendo la desensibilizzazione agli allarmi.

Le soluzioni incentrate sui container basano il rilevamento delle minacce esclusivamente sulle informazioni osservate durante l'esecuzione dei container, il che si traduce in un flusso di avvisi di cui i team di sicurezza dovranno occuparsi. Red Hat Advanced Cluster Security invece confronta automaticamente le informazioni relative alle minacce del ciclo di vita, dei container e di Kubernetes, evitando così di generare silos di informazioni che i team di sicurezza devono collegare manualmente.

Dai priorità alla sicurezza basata sul rischio

La sicurezza Kubernetes native è in grado di creare collegamenti tra le informazioni sulle vulnerabilità, grazie alla conoscenza di configurazioni e rilevamenti delle attività di runtime, e valutare il rischio che certe vulnerabilità vengano effettivamente sfruttate.

Ad esempio, sfruttare una vulnerabilità che richiede determinati privilegi è possibile solo se quei privilegi esistono per i container di uno specifico deployment. Approfittare di una vulnerabilità scrivendo sul file system di un container non desta particolare preoccupazione se il file system è di sola lettura oppure configurare accessi alla rete di alto livello per un determinato deployment non pone rischi critici se si tratta di un cluster di esempio non di produzione o di un'applicazione web esterna.

Red Hat Advanced Cluster Security determina il livello di rischio associato a ogni deployment dell'ambiente e li mette in ordine di priorità per i team di sicurezza. Le soluzioni incentrate sui container valutano i rischi principalmente in base alle vulnerabilità delle immagini e a misure standardizzate come il Common Vulnerability Scoring System (CVSS), rendendo di fatto inutile ogni genere di valutazione del rischio. Un quadro completo del rischio si ottiene solo con la piena conoscenza di Kubernetes.

L'analisi e la risposta agli incidenti può essere efficace solo se i dati che la soluzione per la sicurezza acquisisce e sottopone a indagine sono efficaci. I team di sicurezza hanno tempo e risorse limitati, devono quindi velocizzare analisi e correzione dei problemi con la sicurezza Kubernetes native.

Riduci al minimo il rischio operativo con la sicurezza Kubernetes native

Kubernetes è una piattaforma robusta e scalabile che permette di eseguire pressoché qualunque applicazione, compresi i carichi di lavoro portanti per l'azienda. Lo sviluppo di Kubernetes si concentra su funzionalità che ne aumentano la resilienza operativa come:

- Correzioni automatiche, inclusa la capacità di gestire il riavvio dei container.
- Riprogrammazione.
- Arresto dei container che non superano i controlli di integrità.

Kubernetes è anche altamente scalabile e applica gli stessi principi che Google utilizza per eseguire miliardi di container ogni settimana. L'infrastruttura Kubernetes soddisfa i requisiti operativi di disponibilità (uptime), affidabilità (tempo medio fra i guasti), latenza e altre metriche di importanza critica per l'organizzazione. Fa tutto ciò senza aumentare il rischio operativo per applicazioni, infrastruttura e azienda.

Alcuni strumenti offrono funzionalità per l'applicazione della sicurezza attiva che hanno un impatto diretto sull'ambiente, ad esempio permettono di arrestare container e processi (o impedirne l'avvio), bloccano il traffico di rete o limitano le chiamate di sistema che un'applicazione può eseguire. Questi strumenti aumentano il rischio per l'organizzazione per due motivi principali:

1. Le azioni intraprese per sbaglio possono portare all'interruzione delle applicazioni.
2. Gli strumenti diventano ulteriori dipendenze di cui i team operativi devono occuparsi. Se si verifica un malfunzionamento e sono chiuse, causano significative interruzioni delle applicazioni; se invece sono aperte l'organizzazione si ritrova senza protezioni.

Uno strumento di sicurezza serve proprio per ridurre questi rischi.

Applicazione scalabile

In breve: la sicurezza Kubernetes native offre un'applicazione della sicurezza altamente scalabile e riduce al minimo le eventuali interruzioni delle applicazioni critiche, sfruttando comandi di sicurezza nativi di Kubernetes.

Utilizzare un agente di orchestrazione per l'applicazione delle misure di sicurezza riduce al minimo il rischio operativo e offre una maggiore scalabilità negli ambienti Kubernetes. Questo approccio non era possibile quando le piattaforme dell'infrastruttura non disponevano di capacità di sicurezza Kubernetes native. Oggi Kubernetes comprende:

- Policy di rete per la segmentazione della rete.
- Controller di ammissione per intercettare le richieste al server API Kubernetes.
- Segreti per memorizzare le credenziali sensibili.
- Controllo degli accessi basato sui ruoli (RBAC) per autorizzare funzionalità specifiche per determinati account utente e di servizi
- Molte altre funzionalità.

Questo approccio architetturale rende superflua l'adozione di ulteriori strumenti di sicurezza per l'applicazione delle policy.

Invece le soluzioni incentrate sui container comportano numerosi rischi operativi per l'organizzazione. Ad esempio, spesso devono appoggiarsi a proxy inline per limitare il traffico di rete tra i container oppure devono adottare misure più invasive, come sovrascrivere le regole IP per l'applicazione di firewall.

Inoltre, per evitare che i container eseguano il deployment quando sono presenti vulnerabilità critiche o pacchetti non autorizzati, una soluzione incentrata sui container di solito si affida a uno shim per intercettare e sostituire le richieste per il motore dei container. In questo modo si introducono singoli punti di guasto in tutto l'ambiente e se lo shim del proxy inline o del motore dei container si arresta, può causare l'arresto dell'intera applicazione.

Red Hat Advanced Cluster Security archivia le policy per la segmentazione della rete, il controllo delle ammissioni e altre funzionalità di sicurezza all'interno di Kubernetes, rimuovendo le dipendenze operative. Quindi se per qualche ragione Red Hat Advanced Cluster Security non è disponibile, i criteri di sicurezza vengono comunque applicati. Non si può dire lo stesso delle soluzioni incentrate sui container.

Le soluzioni incentrate sui container introducono anche problemi di scalabilità perché, in certi casi, i diversi componenti necessari per l'applicazione delle policy devono essere eseguiti separatamente su ogni host all'interno di un cluster. Questo approccio pesa molto sull'azienda perché comporta un sovraccarico delle prestazioni, influisce sulla disponibilità di risorse per i container delle applicazioni e richiede uno sforzo maggiore ai team operativi.

Red Hat Advanced Cluster Security mette l'agente di orchestrazione al centro della sua strategia di applicazione, approfittando delle funzionalità specifiche di Kubernetes per un'applicazione altamente scalabile e affidabile. Gli amministratori dei cluster e i team responsabili dell'infrastruttura possono dedicarsi interamente alle operazioni di Kubernetes senza la distrazione di componenti di terze parti. Le organizzazioni ottengono nuovi controlli di sicurezza con tutta l'affidabilità e la scalabilità del sistema Kubernetes, che si appoggia a un ecosistema di centinaia di aziende e una community di migliaia di sviluppatori.

Inoltre, una soluzione di sicurezza Kubernetes native è indipendente dalle architetture promosse dalla community. Un esempio è la Container Network Interface (CNI), una specifica standard per l'interfaccia di rete. Le funzionalità di segmentazione della rete di Red Hat Advanced Cluster Security funzionano in modo coerente in tutti i plugin CNI.

Le soluzioni incentrate sui container invece sono talvolta dipendenti da determinati plugin oppure mostrano problemi di compatibilità, e rischiano solo di aumentare le criticità operative che l'organizzazione deve affrontare. I comandi di Red Hat Advanced Cluster Security non hanno dipendenze verso specifici strumenti o plugin e consentono quindi ai team operativi e DevOps di scegliere i più adatti alle loro esigenze.

Elimina i conflitti operativi

In breve: la sicurezza Kubernetes native contribuisce a ridurre i problemi operativi dovuti a configurazioni incoerenti, mancanza di coordinazione ed errori degli utenti.

Per ridurre al minimo il rischio operativo, le organizzazioni devono evitare configurazioni della sicurezza incoerenti che possano portare a comportamenti delle applicazioni imprevedibili e generare una complessità che spinga gli utenti in errore. Un'architettura Kubernetes native riduce il rischio che si verifichino questi problemi operativi.

Se team di sicurezza e DevOps implementano strumenti, controlli e comandi diversi si possono generare delle incongruenze nelle configurazioni di sicurezza. Lo stesso succede se entrano in conflitto le configurazioni a diversi livelli dello stack dell'infrastruttura. Ad esempio, se le impostazioni configurate a livello di container risultano incompatibili con quelle a livello di Kubernetes.

La sicurezza Kubernetes native offre ai team operativi, di sviluppo e di sicurezza una visibilità e gestione di criteri e applicazione centralizzate tramite Kubernetes. Con Red Hat Advanced Cluster Security i criteri di segmentazione della rete e di controllo ammissione rimangono su Kubernetes per una consultazione più agevole.

Le soluzioni incentrate sui container obbligano gli utenti a implementare i comandi con strumenti diversi, generando problemi di coordinamento all'interno dell'organizzazione. Ad esempio, i team DevOps utilizzano policy di rete di Kubernetes per limitare il traffico di rete autorizzato per le applicazioni, mentre i team di sicurezza nella stessa situazione adottano firewall proprietari. Di conseguenza è alto il rischio che emergano conflitti nelle configurazioni e lacune nella protezione.

Le incongruenze tra le configurazioni a livello di Kubernetes e di container possono anche avere ripercussioni inaspettate sulle applicazioni in esecuzione. Ad esempio, le soluzione incentrate sui container possono limitare le chiamate di sistema che un certo container può eseguire, anche se queste limitazioni non sono configurate su Kubernetes tramite criteri di sicurezza dei pod. Ne consegue che un utente di Kubernetes si trova spaesato di fronte a certi problemi operativi di cui non capisce la causa poiché la configurazione rilevante è specificata a un altro livello.

Esistono poi casi in cui sono le limitazioni a entrare in conflitto e il traffico non è più autorizzato o limitato come dovrebbe. Ad esempio, una policy di rete di Kubernetes consente il traffico tra il container A e il container B, ma un proxy inline incentrato sui container limita il traffico tra questi due container. Ne risulta una confusione operativa generale.

Nella sicurezza Kubernetes native, Kubernetes funge fonte di attendibilità per le funzioni di sicurezza e riduce la commutazione del contesto necessaria ai team responsabili di operazioni e Site Reliability Engineering (SRE). I problemi di sicurezza vengono immediatamente associati agli oggetti e alle risorse di Kubernetes, ovvero agli strumenti con cui questi team lavorano quotidianamente per garantire la disponibilità e l'affidabilità di Kubernetes.

Questo approccio riduce la complessità operativa che spesso porta gli utenti a commettere errori deleteri per gli ambienti Kubernetes. Le soluzioni incentrate sui container richiedono ai team operativi e SRE di analizzare i problemi di sicurezza individuando le correlazioni tre le informazioni specifiche del fornitore e i dati di Kubernetes. Red Hat Advanced Cluster Security permette agli utenti di visualizzare le informazioni in un formato compatibile con Kubernetes; agevola e accelera quindi la capacità dei team di individuare e risolvere i problemi utilizzando le toolchain e i flussi di lavoro più adatti.

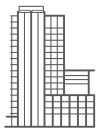
Conclusioni

Le tecnologie cloud native hanno rivoluzionato, e continueranno a farlo, il modo in cui le organizzazioni eseguono le applicazioni e di conseguenza l'approccio alla sicurezza. Consentendo l'adozione di pratiche collaborative come DevSecOps e altre soluzioni, hanno promosso un'evoluzione del settore verso un modello Security as Code. Alla base di questo cambiamento generazionale nel software per l'infrastruttura c'è Kubernetes, il sistema di orchestrazione dei container leader di settore. E anche se esistono molti approcci alla difesa degli ambienti containerizzati, la sicurezza Kubernetes native è più efficace perché permette visibilità approfondita, analisi più rapida e operazioni semplificate.

La sicurezza Kubernetes native di Red Hat offre una serie di vantaggi unici per la creazione ed esecuzione di applicazioni containerizzate, come:

- Aumenta la protezione eliminando i punti ciechi e individuando vulnerabilità e configurazioni errate proprie di Kubernetes.
- Fa risparmiare tempo e riduce i costi accelerando la curva di apprendimento dei team e semplificando indagine e correzione grazie al prezioso contesto fornito da Kubernetes.
- Riduce al minimo il rischio operativo generale grazie a Kubernetes e alle sue funzioni di applicazione scalabili, e elimina la complessità operativa che deriva dalle configurazioni incoerenti e dagli errori degli utenti.
- Fornisce una piattaforma standardizzata per gli scenari di utilizzo relativi alla sicurezza di tutto il ciclo di vita delle applicazioni cloud native; scenari sfruttabili da sviluppatori, team operativi e di sicurezza.

Con Red Hat Advanced Cluster Security le organizzazioni possono proteggere i loro ambienti Kubernetes ovunque in produzione e in modo scalabile.



Informazioni su Red Hat

Red Hat è leader mondiale nella fornitura di soluzioni software open source. Con un approccio basato sul concetto di community, distribuisce tecnologie come Kubernetes, container, Linux e cloud ibrido caratterizzate da affidabilità e prestazioni elevate. Red Hat favorisce l'integrazione di applicazioni nuove ed esistenti, lo sviluppo di applicazioni cloud native, la standardizzazione su uno dei principali sistemi operativi enterprise, e consente di automatizzare e gestire ambienti complessi in modo sicuro. I pluripremiati servizi di consulenza, formazione e assistenza hanno reso Red Hat un partner affidabile per le aziende della classifica Fortune 500. Lavorando al fianco di fornitori di servizi cloud e applicazioni, integratori di sistemi, clienti e community open source, Red Hat prepara le organizzazioni ad affrontare un futuro digitale.

facebook.com/RedHatItaly
twitter.com/RedHatItaly
linkedin.com/company/red-hat

ITALIA
it.redhat.com
italy@redhat.com

EUROPA, MEDIO ORIENTE,
E AFRICA (EMEA)
00800 7334 2835
it.redhat.com
europe@redhat.com

it.redhat.com
#F28129_0421