Container: cosa serve sapere

Author : Redazione

Date : 3 Aprile 2019

Si sta diffondendo rapidamente l'utilizzo dei container per la distribuzione delle applicazioni. Sia che si tratti di Kubernetes o Docker, gli strumenti open source oggi più diffusi sia per il deployment sia per le attività di orchestrazione, i container si rivelano utili per implementare gli elementi che compongono l'applicazione ed attivarli in ambienti cloud pubblici o ibridi. Sono ambienti runtime leggeri e forniscono un modo per astrarre e virtualizzare i componenti dei microservizi dall'hardware o dal servizio cloud sottostante, evitando di essere legati ad un ambiente specifico. In ogni caso, trasferire sui container significa prevedere dei cambiamenti per il team di sicurezza IT.

I container sono da comprendere e gestire, esattamente come l'infrastruttura IT tradizionale. Senza questa consapevolezza ed attenzione, è difficile mantenere le immagini aggiornate e in sicurezza. Qual è dunque la miglior combinazione pragmatica tra container, sicurezza e attività di monitoring?

Dove sono i container

Prima di tutto, è necessario capire se la *containerizzazione* sia in uso all'interno dell'organizzazione e dove, nello specifico, venga applicata.
Può sembrare un punto semplice, ma accade spesso che gli sviluppatori creino e avviino le loro applicazioni nel cloud senza coinvolgere gli altri team IT dell'azienda sin dall'inizio. È altrettanto importante capire quante implementazioni di questo tipo sono attivate nell'ambiente IT aziendale e per quali scopi.

Una volta identificati container in attività, è fondamentale capire quanto il processo di sviluppo del software sia basato su questa tecnica, in quanto normalmente accade che quanto prototipato in fase di sviluppo sia esteso alla produzione. Pertanto se i progetti iniziali sono sviluppati in container, è tipico che sia il processo di test che quello di *quality assurance* e le istanze di produzione finale, migrino nel tempo all'adozione di container.

Questa situazione può portare all'esecuzione di più piattaforme ed istanze in contemporanea.

Per una gestione ottimale, è opportuno capire l'attuale livello di visibilità di tutte le risorse IT aziendali; stabilire dove le informazioni siano sufficienti e dove il contesto richieda più dati.

Tale processo dimostra nel tempo il miglioramento della visibilità nell'ambiente IT aziendale.

Una volta individuate le aree di miglioramento, diventa possibile capire quali dati manchino. Per i container, ottenere informazioni sulle immagini in esecuzione può risultare difficile se non ci si è pensato in anticipo. Ad esempio, se un'azienda ha già distribuito più container applicativi in un servizio cloud, è possibile sapere quante immagini vengono eseguite in un dato momento, come?

Per ottenere quest'informazione, è necessario che in ogni container standard siano incorporati degli agenti; grazie a questi sensori inclusi in tutte le immagini, saremo in grado di generare automaticamente un report di status. Questo può aiutare a conoscere il numero delle immagini implementate, quali librerie software siano incluse nell'ambiente runtime e se queste siano aggiornate.

E' importante sottolineare che ognuna delle fasi indicate dovrà essere ripetuta in continuità.

I container sono istanziati e rimossi automaticamente in base alla domanda; di conseguenza la validazione e la protezione delle applicazioni nei container deve garantire la stessa ritmica, distribuita lungo l'intero ciclo di vita delle applicazioni: dal momento in cui sono sviluppate, codificate e spedite nei *registry* come immagini fino al momento in cui sono istanziate come applicazioni in esecuzione in container.

Questo approccio serve a coprire la valutazione e l'esecuzione per tutte le parti in movimento coinvolte nella gestione dei container: inclusi stack dell'infrastruttura container e ciclo di vita dell'applicazione *containerizzata* nel tempo. Queste due aree, stack e ciclo di vita, devono essere allineate meticolosamente.

Ancor più importante è che queste informazioni siano consolidate con dati sulle risorse IT tradizionali, agevolando la prioritizzazione nel rimedio delle aree di attenzione, a prescindere dalla loro *posizione IT*.

Mettere in sicurezza i processi di sviluppo del software, non solo la tecnologia

I container vengono comunemente adottati come parte di metodologie di sviluppo agile e di processi DevOps. Qualora i container siano già in uso da parte di alcuni team, è importante ampliare il raggio d'analisi al processo di integrazione e distribuzione continua (CI/CD), in cui vengono utilizzati anche i container. Integrazione continua o *Continuous Integration* (CI) implica la scomposizione dello sviluppo del software in blocchi più piccoli e gestibili che possono essere consegnati più rapidamente, mentre Continuous Deployment (CD) partecipa muovendo questi progetti di sviluppo attraverso attività di testing e messa in produzione.

Affinchè l'implementazione della *pipeline* CI/CD sia efficace, serve che i due processi siano automatizzati ed integrati. Questo aiuta gli sviluppatori nell'accelerare l'attività di test e messa

in produzione dei nuovi progetti software, mentre un’ulteriore integrazione con i servizi cloud supporta la collaborazione con i team operativi sull’ampliamento dell’implementazione in modo da soddisfare la domanda. L’utilizzo di strumenti come Jenkins, CircleCI o Travis CI può velocizzare questi processi, sebbene siano automatizzati i soli passaggi che si decide di includere.

Per i professionisti della sicurezza che cercano di capire come comportarsi con i container, non è sufficiente dire che la sicurezza andrebbe considerata sin dall’inizio. È fondamentale sottolineare come la sicurezza possa aggiungere valore per gli sviluppatori al ciclo DevOps, fornendo al team di sicurezza tutte le informazioni necessarie sullo stato delle risorse IT e dell’infrastruttura.

Ad esempio, è possibile aiutare gli sviluppatori fornendogli la possibilità di eseguire in completa autonomia la verifica di potenziali vulnerabilità di sicurezza all'interno di componenti o librerie software. Questa attività può essere resa parte dei loro *workflow*, inserendo automaticamente ogni anomalia riscontrata nel software di tracciamento dei problemi di sviluppo software per pianificarne il rimedio. L’eliminazione della burocrazia nella segnalazione dei problemi di sicurezza scoperti durante la scansione delle applicazioni o i controlli delle immagini dei container aiuta il team di Security a facilitare il processo di sviluppo del software.

Per i team che utilizzano i container, questo processo di scansione deve coprire tutte le diverse posizioni in cui possono esser presenti le immagini. Questo include tutte le risorse software utilizzate all'interno dei container, tutte le immagini di container già archiviate nella libreria aziendale, tutte le immagini di container estratte dagli archivi pubblici, tutti i container stessi quando in esecuzione.

Ottenere queste informazioni supporta gli sviluppatori a capire dove applicare fix all'interno dei container, e aiuta nella comprensione della superficie vulnerabile. La collaborazione al processo di discovery e l’aiuto agli sviluppatori nel gestire la propria parte autonomamente, aumenta – semplificandolo – il livello di sicurezza.

Ancor più importante, queste informazioni sono rese disponibili contestualmente a quelle provenienti dalle altre piattaforme e dall’infrastruttura.

L'esecuzione di un servizio di gestione degli asset in questo contesto richiede visibilità e protezione native per i container, implementate sin dal principio. Questo processo deve anche integrarsi perfettamente con le pipeline CI / CD aziendali esistenti, in modo che ogni container venga gestito e tracciato correttamente.

La tecnica di gestione asset basata su layering dovrebbe includere il monitoraggio del tempo di esecuzione di ogni container, cosicché qualsiasi modifica nell'immagine possa essere evidenziata per tempo.

Per i team di sicurezza IT ottenere informazioni dettagliate sullo stato di tutte le risorse IT aziendali è essenziale per mantenere i dati protetti, sia che si tratti di server fisici tradizionali, endpoint su rete aziendale o anche nuove applicazioni distribuite in container su cloud pubblico.

Senza questa visibilità sugli eventi del panorama IT aziendale, è facile non accorgersi dei potenziali rischi che si corrono. Tuttavia, i cambiamenti che ruotano attorno ai container in termini di modalità di sviluppo e utilizzo delle applicazioni fanno sì che sia importante adottare un approccio più pragmatico per ottenere questi dati il prima possibile.

Comprendendo i cambiamenti che avvengono nello sviluppo del software, è possibile integrare tempestivamente la sicurezza nel processo. Allo stesso modo, centralizzando informazioni e contesto relativi alle risorse IT è possibile aumentare l'efficacia decisionale nell'utilizzo delle risorse di sicurezza.

A cura di **Marco Rottigni**, Chief Technical Security Officer EMEA di Qualys