CROWDSTRIKE

FALCON CLOUD WORKLOAD PROTECTION

Protezione dalle violazioni per container e workload cloud

SOLUZIONE DI PROTEZIONE DEI WORKLOAD CLOUD CHE TRASFORMA IL MODO DI LAVORARE DEL TEAM DEVOPS

L'esigenza di essere veloci e agili che hanno i business digitali di oggi implica la trasformazione dell'infrastruttura IT, e in particolare il passaggio ad architetture cloud e l'adozione di strumenti di DevOps. Questa esigenza ha portato molte aziende ad adottare container, microservizi e Kubernetes (K8s) nel tentativo di migliorare l'efficienza e la scalabilità delle attività di sviluppo e di gettare le basi per una nuova infrastruttura immutabile di ultima generazione.

In più, l'innovazione è accelerata dall'adozione del metodo CI/CD per la distribuzione frequente delle app, che prevede l'introduzione dell'automazione e del monitoraggio continui nelle varie fasi del ciclo di vita delle applicazioni: integrazione, test, distribuzione e deployment. Poiché tuttavia la metodologia CI/CD non è esente da rischi, i responsabili dell'infrastruttura, della sicurezza e il team DevOps devono assicurarsi che i container e i microservizi rimangano protetti, conformi e senza vulnerabilità nascoste.

Dal momento che il deployment in container comporta la creazione di un nuovo ambiente e il mondo Kubernetes richiede un sistema di gestione diverso, i responsabili della sicurezza faticano a stare al passo. Il risultato? Maggiori rischi imputabili a scarsa visibilità; processi frammentari per il rilevamento e la prevenzione delle minacce; errori di configurazione nei workload cloud, nei container e negli ambienti serverless; incapacità di mantenere la conformità.

Principali difficoltà legate alla messa in sicurezza dei container:

- Mancanza di visibilità nei workload cloud, nei container e negli ambienti Kubernetes
- Gestione inefficace delle vulnerabilità nelle immagini dei container, nei registri, nelle librerie e negli host
- Messa in sicurezza dell'orchestrazione dei container
- Protezione in fase di esecuzione dei container e dei workload nativi del cloud
- Mancanza di competenze sulla sicurezza del cloud ed estensione della superficie di attacco
- Imposizione della conformità e delle policy di sicurezza

Le aziende non possono affrontare questo cambiamento epocale e le particolari sfide associate all'uso dei container ricorrendo a processi manuali e soluzioni tradizionali. Un'alternativa potrebbe essere quella di adottare complesse piattaforme di sicurezza cloud o strumenti isolati, con il risultato, però, di rendere meno omogeneo l'ambiente e di complicare ulteriormente la gestione della sicurezza a livello aziendale.

PRINCIPALI VANTAGGI

Esegue scansioni continue alla ricerca di vulnerabilità, minacce, segreti incorporati e violazioni della conformità

Assicura un livello eccezionale di visibilità proponendo dettagli su eventi dei workload cloud, dei container e metadati

Individua i workload cloud in esecuzione nell'ambiente, compresi quelli con configurazioni potenzialmente pericolose

Assicura protezione continua in fase di esecuzione per tutti i workload cloud e i container

Accelera le attività di threat hunting e analisi sui workload

Protegge immediatamente senza sacrificare le performance rispettando la velocità del team DevOps

Si adatta in tempo reale alla scalabilità dinamica dei workload cloud e dei container

L'APPROCCIO DI CROWDSTRIKE PER METTERE IN SICUREZZA WORKLOAD CLOUD E CONTAINER

CrowdStrike basa il suo approccio alla sicurezza dell'infrastruttura cloud sul principio di stare un passo avanti rispetto agli avversari, obiettivo che persegue riducendo incessantemente la superficie di attacco e predisponendo una visibilità totale su tutti gli eventi che si verificano nell'ambiente gestito. L'incombenza di bloccare le violazioni di workload cloud, container e ambienti Kubernetes utilizzando dati e analisi su scala cloud richiede l'impiego di una piattaforma strettamente integrata. Poiché ogni funzione è indispensabile per individuare precocemente vulnerabilità e minacce, proteggere la fase di esecuzione e imporre la conformità, le funzioni devono essere pensate e realizzate in modo da favorire la velocità, la scalabilità e l'affidabilità.

L'esperienza che CrowdStrike ha accumulato gestendo uno tra i più grandi cloud di sicurezza del mondo le permette di avere informazioni preziose sugli avversari e di proporre soluzioni progettate appositamente per diminuire il workload dei team DevSecOps, proteggere i dati dalle violazioni e ottimizzare gli ambienti cloud.

FUNZIONALITÀ PRINCIPALI

SCANSIONE E GESTIONE DELLE VULNERABILITÀ

Visibilità completa su workload, container e host on-premise e cloud.

- **Migliora il processo decisionale:** raccogli dati approfonditi sui tuoi workload cloud e container: immagini, registri, librerie e container generati dalle immagini.
- **Scopri le minacce nascoste:** riduci la superficie di attacco individuando qualsiasi malware nascosto, chiavi segrete incorporate, problemi di configurazione e molto altro all'interno delle immagini.
- **Ottieni la visibilità totale sui container:** visibilità completa sui container in esecuzione per portare alla luce dati sull'accesso ai file, comunicazioni di rete e processi.
- **Individua più velocemente le vulnerabilità:** risparmia tempo prezioso e individua velocemente vulnerabilità ed errori di configurazione con le policy di scansione delle immagini preconfigurate.
- **Individua le configurazioni dei container a rischio:** trova rapidamente i container pericolosi e mal configurati, come quelli con pochi punti di montaggio o link che segnalano una compromissione.
- **Elimina le minacce prima che entrino in produzione:** evita seccature al team di sicurezza utilizzando gli indicatori di attacco prima della fase di esecuzione per eliminare le vulnerabilità che possono essere sfruttate.
- **Attiva il monitoraggio continuo:** individua ogni nuova vulnerabilità in fase di esecuzione, emetti un avviso e intervieni senza dover analizzare da zero le immagini dei container.

AUTOMAZIONE DELLA SICUREZZA NEL PROCESSO CI/CD

Integra la sicurezza nella pipeline di integrazione e distribuzione continue (CI/CD).

- **Accelera la distribuzione:** crea policy verificate per assicurarti che solo immagini approvate vengano immesse nella pipeline e vengano eseguite negli host o nei cluster Kubernetes.

PROTEZIONE DEI WORKLOAD CLOUD OTTIMIZZATA PER DEVOPS

Un'unica piattaforma per tutti i workload e i container

Protegge i workloadcloud e i container ovunque si trovino.

Esegue la scansione di immagini e registri integrandosi direttamente nella pipeline CI/CD

Operativo sin dal primo giorno: operativo nel giro di qualche minuto, non richiede riavvii, messe a punto né configurazioni complesse

Classifica gli incidenti in modo intelligente in base alla gravità

Semplifica il processo di triage e risponde automaticamente

- **Individua precocemente le minacce:** sottoponi a scansione continua le immagini dei container per scoprire vulnerabilità, problemi di configurazione, segreti e chiavi incorporate e problemi di licenze dei software open source.
- **Valuta la condizione di vulnerabilità della tua pipeline:** scopri il malware sfuggito alle scansioni statiche prima del deployment dei container.
- **Migliora le operazioni di sicurezza:** migliora la visibilità delle operazioni di sicurezza fornendo più dati contestuali sugli errori di configurazione e le violazioni delle policy.
- **Integrazione con gli strumenti di sviluppo:** l'integrazione perfetta con Jenkins, Bamboo e GitLab consente di intervenire ed eseguire attività di remediation con gli strumenti DevOps che già usi.
- **Favorisci la collaborazione tra sicurezza e sviluppo:** l'utilizzo di report e dashboard favorisce allineamento e la collaborazione tra team di sicurezza, DevOps e responsabili delle infrastrutture.

PROTEZIONE IN FASE DI ESECUZIONE

Proteggi i workload cloud e i container ovunque si trovino.

- **Metti in sicurezza host e container:** la protezione in fase di esecuzione esercitata da CrowdStrike Falcon® mette i container al riparo da attacchi.
- **Supporto più esteso per i container:** la piattaforma Falcon supporta i container eseguiti su Linux e può essere implementata negli ambienti Kubernetes, ad esempio EKS. Supporta anche il modello di implementazione Container-as-a-Service, o CaaS – come Fargate – per il quale assicura il medesimo livello di protezione. Sono disponibili anteprime tecnologiche per AKS, GKE e Red Hat OpenShift.
- **Utilizza le tecnologie di protezione più all'avanguardia:** con il machine learning (ML), l'intelligenza artificiale (AI), gli indicatori di attacco e il blocco degli hash puoi difenderti automaticamente dal malware e dalle minacce sofisticate rivolte ai container:
  - **ML e AI:** Falcon utilizza queste tecnologie per rilevare tipi di malware noti e sconosciuti all'interno dei container senza ricorrere a scansioni o signature.
  - **Indicatori di attacco:** Falcon li utilizza per individuare le minacce sulle base del comportamento dell'attaccante. Ricostruire la catena dei comportamenti permette a Falcon di bloccare anche gli attacchi che non sono basati su malware, come gli attacchi fileless.
- **Blocca i comportamenti sospetti:** l'analisi dei comportamenti permette di fermare le attività che violano le policy senza incidere sulle attività legittime dei container.
- **Analizza più rapidamente gli incidenti che coinvolgono i container:** quando gli avvisi sono associati a un container specifico e non mescolati agli eventi dell'host, l'analisi degli incidenti è più semplice.
- **Tieni tutto sotto controllo:** acquisisci dati sull'avvio, l'arresto, l'esecuzione, l'immagine del container e su qualsiasi evento generato al suo interno, anche per container attivi per pochi secondi.
- **Deployment trasparente con Kubernetes:** includendo Falcon in un cluster Kubernetes, il deployment diventa facile e scalabile.
- **Migliora l'orchestrazione dei container:** acquisisci lo spazio dei nomi Kubernetes, i metadati Pod, i processi, i file e gli eventi di rete.

PREVENZIONE DELLE COMPROMISSIONI CON THREAT GRAPH

Prevedi e blocca in tempo reale anche le minacce più recenti con l'ausilio della selezione più completa di dati telemetrici (su endpoint, workload cloud e container), threat intelligence e analisi basate sull'intelligenza artificiale.

- **Threat intelligence integrata leader del mercato:** Falcon utilizza i dati di threat intelligence arricchiti per elaborare una rappresentazione grafica delle relazioni tra ruoli degli account, workload e API e per offrire informazioni contestuali più approfondite che consentano una risposta agli incidenti più rapida ed efficace.
- **Prevenzione delle minacce automatizzata:** analisi comportamentali e potenziate dall'intelligenza artificiale individuano in tempo reale minacce nuove e insolite e intraprendono misure appropriate, sgravando i team di sicurezza.
- **Risposta più rapida:** CrowdStrike Threat Graph® rende tutte queste conoscenze disponibili in tempo reale, così che l'addetto all'intervento possa interpretare immediatamente le minacce e reagire con prontezza.

- **Riduce il sovraccarico di avvisi:** l'approccio mirato volto a identificare e gestire le minacce fa chiarezza tra gli avvisi di sicurezza degli ambienti multicloud e riduce il sovraccarico.
- **Svela la dinamica degli attacchi e migliora la risposta:** CrowdScore™ Incident Workbench di CrowdStrike aiuta a chiarire la dinamica degli attacchi e a migliorare i tempi di risposta distillando e mettendo in correlazione gli avvisi di sicurezza con gli incidenti per evidenziare quelli che richiedono un intervento urgente.

PUNTO DI RIFERIMENTO UNICO DOTATO DI POTENTI API

L'esistenza di un punto di riferimento unico consente ai team di sicurezza di accedere rapidamente alle informazioni di cui hanno bisogno per intervenire e analizzare l'evento.

- **Automazione a beneficio dei processi DevOps:** la selezione di potenti API supporta l'automazione delle funzionalità di CrowdStrike Falcon: rilevamento, gestione, risposta e cyberintelligence.
- **Ottimizzazione delle performance:** flussi di lavoro avanzati, come l'orchestrazione della sicurezza e l'automazione, consentono di ottimizzare le performance aziendali.
- **Integrazione con pipeline CI/CD:** le integrazioni per Chef, Puppet e AWS Terraform supportano i processi CI/CD.
- **Stessa velocità tra protezione e team DevOps:** Falcon offre una protezione immediata che corrisponde alla velocità dei team DevOps perché si adatta alla scalabilità dinamica dei container in tempo reale grazie all'integrazione CI/CD via API e agli script da eseguire prima dell'avvio.

SEMPLICITÀ E PERFORMANCE

Un'unica piattaforma per tutti i workload e i container che funziona in qualsiasi ambiente: privato, pubblico o cloud ibrido.

- **Semplifica l'adozione da parte di DevSecOps:** riduci i costi, l'attrito e la complessità associati alla protezione dei workload cloud, dei container e degli ambienti serverless.
- **Unico pannello di controllo:** un'unica console fornisce una visione centralizzata sullo stato di sicurezza cloud, sui workload e sui container, a prescindere dalla loro posizione.
- **Totale flessibilità per le policy:** le policy possono essere applicate a singoli workload, container, gruppi oppure a livello più elevato e possono essere unificate tra i deployment on-premise e multicloud.
- **Alta scalabilità:** non è necessario modificare l'architettura né ampliare l'infrastruttura.
- **Supporto per numerose piattaforme:** la piattaforma Falcon supporta i container di tipo OCI (Open Container Initiative) come Docker e Kubernetes e le piattaforme di orchestrazione autogestite e ospitate come GKE (Google Kubernetes Engine), EKS (Amazon Elastic Kubernetes Service), ECS (Amazon Elastic Container Service), AKS (Azure Kubernetes Service) e OpenShift.

INFORMAZIONI SU CROWDSTRIKE

CrowdStrike, leader della sicurezza informatica a livello globale, sta ridefinendo la sicurezza nell'era del cloud grazie alla sua piattaforma di protezione degli endpoint creata appositamente per bloccare le compromissioni. L'architettura basata su un unico agent a basso impatto della piattaforma CrowdStrike Falcon® applica l'intelligenza artificiale a livello del cloud per offrire protezione e visibilità istantanee sull'intera azienda e prevenire gli attacchi sugli endpoint e i carichi all'interno della rete e all'esterno. Sfruttando la tecnologia proprietaria di CrowdStrike Threat Graph®, ogni settimana CrowdStrike Falcon crea correlazioni in tempo reale tra più di 4 migliaia di miliardi di eventi legati agli endpoint provenienti da tutto il mondo, alimentando una delle piattaforme di sicurezza più avanzate mai esistite.