CROWDSTRIKE

Blueprint per workload AWS protetti

La piena visibilità e protezione di workload e container garantite da Falcon Cloud Security di Crowdstrike, oltre a una overview completa degli alert tramite AWS Security Hub, sono gli strumenti più efficaci per costruire architetture cloud sicure.

aws PARTNER

- Settore pubblico
- Amazon Linux Ready
- Marketplace Seller
- Competenza del software di sicurezza

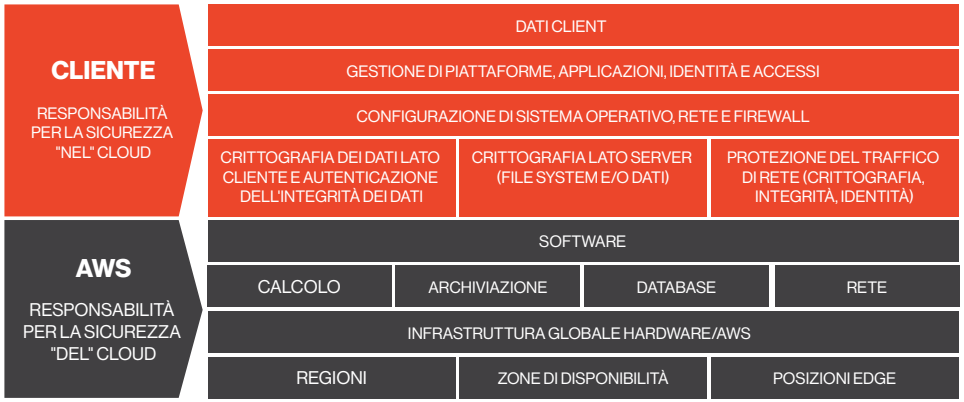
eBook CrowdStrike

Sommario

Blueprint obsoleti lasciano le architetture cloud di oggi vulnerabili agli attacchi

Anche se l'adozione del cloud è cresciuta esponenzialmente, molte posture di sicurezza restano ancorate al passato. Estendere al cloud l'impiego degli strumenti di sicurezza legacy on-premise si è rivelata una scelta inadeguata, che ha lasciato cloud architect e team DevOps senza un progetto chiaro per la protezione di applicazioni, workload e infrastrutture.

Scegli di costruire una solida base di sicurezza con Amazon Web Services (AWS) e CrowdStrike, leader nella protezione degli endpoint e dei workload in cloud. La combinazione di CrowdStrike Falcon e AWS Security Hub offre una gestione centralizzata e automatizzata degli alert sulle minacce provenienti dai servizi AWS, compreso Amazon GuardDuty. Con CrowdStrike Falcon Cloud Security puoi migliorare la protezione dei tuoi workload AWS e adottare il modello di responsabilità condivisa.



CrowdStrike Falcon Cloud Security protegge i tuoi workload in esecuzione su AWS

AWS protegge la tua infrastruttura cloud

AWS Security Hub offre una visione completa degli alert di sicurezza e della compliance

- Aggrega i dati degli alert provenienti da Falcon e dai servizi AWS nativi come Amazon GuardDuty
- Monitora lo stato della tua infrastruttura AWS attraverso display visivi
- Effettua controlli della compliance

CrowdStrike Falcon Cloud Security protegge i tuoi workload AWS attraverso un unico lightweight agent

- Sicurezza avanzata delle applicazioni native in cloud, compresa la prevenzione delle compromissioni, la protezione dei workload e la gestione della postura di sicurezza del cloud.
- Semplifica il tuo stack di sicurezza con un singolo agent che ha un ingombro ridotto sulle risorse AWS per prestazioni migliori.
- Condensa la quantità di architecture necessaria per una visibilità completa della sicurezza e riduci la complessità per ricavare più valore dagli investimenti in AWS.

Falcon e AWS integrano nei tuoi workflow une protezione ininterrotta

L'integrazione di CrowdStrike con AWS Security Hub rende possibile una visione completa in tempo reale degli alert di sicurezza ad alta priorità. L'approccio API-first di CrowdStrike integra Falcon Cloud Security e AWS Security Hub, rendendo più semplice per l'intero team – inclusi DevOps, CISO, cloud architect e operations – automatizzare i task di sicurezza e migliorare la protezione complessiva.

GUARDA – CON UNA VISIBILITÀ COMPLETA

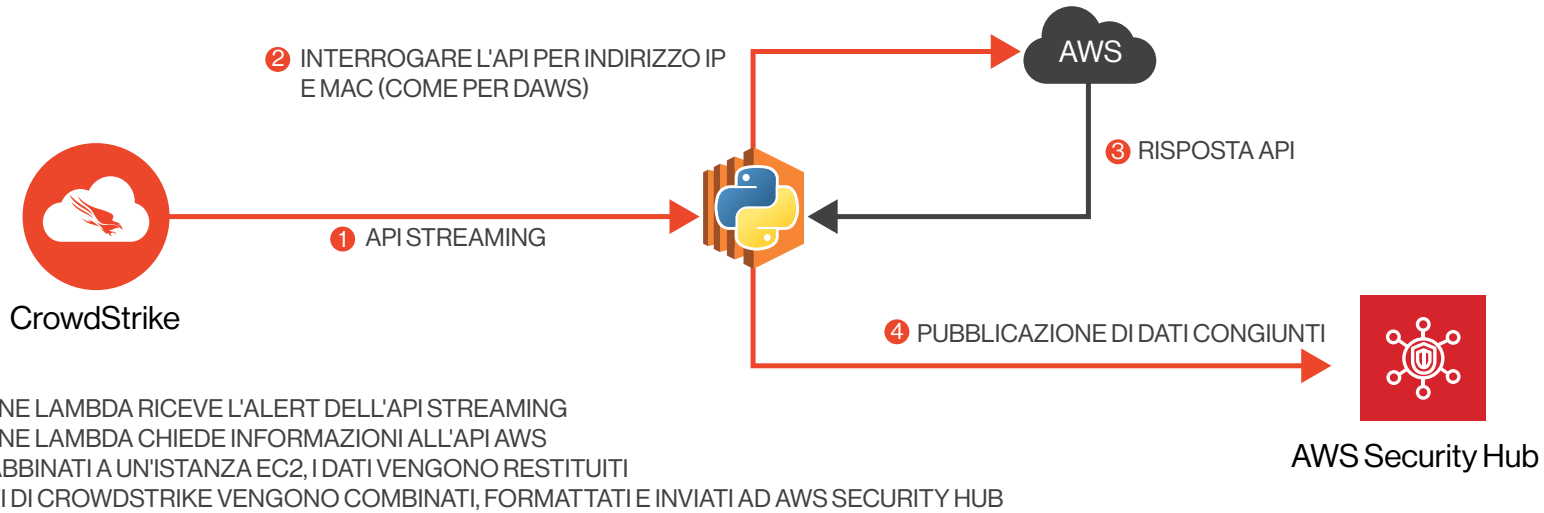
CrowdStrike Falcon Cloud Security protegge i tuoi workload AWS per tutto il ciclo di vita delle minacce tramite la fusione di machine learning, intelligenza artificiale, analisi comportamentale e threat hunting proattivo in un'unica soluzione.

PROTEGGI – CON PRESTAZIONI PIÙ EFFICACI

CrowdStrike Falcon Cloud Security funziona ovunque: istanze Amazon Elastic Cloud Compute (Amazon EC2), Amazon Elastic Container Service (Amazon ECS) su Amazon EC2 e Amazon Elastic Kubernetes Service (Amazon EKS) su Amazon EC2, garantendo la sicurezza degli endpoint e dei workload anche quando sono offline.

DIFENDI – CON UN'ARCHITETTURA SEMPLIFICATA

CrowdStrike Falcon Cloud Security semplifica le complesse pipeline DevSecOps e accresce l'affidabilità operativa semplificando anche le architetture cloud. Falcon consolida i tuoi agent di endpoint e workload con una piattaforma estensibile che cresce e si adatta alle tue esigenze senza accrescere la complessità.



1. LA FUNZIONE LAMBDA RICEVE L'ALERT DELL'API STREAMING
2. LA FUNZIONE LAMBDA CHIEDE INFORMAZIONI ALL'API AWS
3. SE SONO ABBINATI A UN'ISTANZA EC2, I DATI VENGONO RESTITUITI
4. EC2 E I DATI DI CROWDSTRIKE VENGONO COMBINATI, FORMATTATI E INVIATI AD AWS SECURITY HUB

Guarda – con una visibilità completa

Con gli alert di Amazon GuardDuty e Falcon Cloud Security, aggregati attraverso AWS Security Hub, il tuo team ha una visione unica che fornisce la consapevolezza situazionale necessaria per prendere decisioni strategiche sulla sicurezza e sulle risorse. Automatizzare l'analisi di sicurezza accelera la tua capacità di individuare e risolvere gli incidenti più critici in mezzo al rumore.

Sfrutta l'intelligence Threat Graph

Scopri le potenziali minacce in modo rapido e preciso con l'intelligence Threat Graph basata su tecnologia AI, per raggiungere un livello di protezione dei tuoi workload AWS in precedenza inarrivabile.

Automatizza i task di sicurezza

Senza Threat Graph, gli analisti dovrebbero raccogliere manualmente la telemetria di endpoint e workload, aggiungere feed di intelligence, scrivere regole di correlazione e incrociare infine i dati per determinare come gli eventi di sicurezza potrebbero essere correlati. Grazie a Falcon Cloud Security, invece, tutte le informazioni, gli eventi e le reciproche relazioni sono raccolti in un unico posto, consentendo ai security administrators di automatizzare l'analisi per ottenere una visibilità più intelligente e approfondita durante le indagini su potenziali violazioni.

Integra la sicurezza nelle pipeline CI/CD

Falcon Cloud Security consente ai team di sicurezza cloud di stare al passo con la natura dinamica e flessibile dei workload AWS. Il supporto ininterrotto al deployment CI/CD di workflow è garantito da potenti API e dall'integrazione semplificata con AWS Security Hub.

I team DevOps promuovono l'incremento dell'automazione

- Automatizza il delivery di pipeline di development
- Riduci la complessità di deployment e gestione
- Ottieni la sicurezza alla velocità del delivery delle applicazioni

I team di sicurezza acquisiscono informazioni più approfondite

- Aggiungi maggiore contesto agli avvisi di sicurezza AWS
- Comprendi l'impatto degli eventi di sicurezza
- Semplifica la risposta agli incidenti
- Identifica l'intento in base agli indicatori di attacco
- Riduci i falsi positivi e aumenta l'efficienza della sicurezza

> 7.000 miliardi
di eventi alla settimana

200K
nuovi IOC pubblicati ogni giorno

> 200
avversari monitorati

> 1,2 milioni
di campioni malware elaborati ogni giorno

Proteggi – con prestazioni più efficaci

Con CrowdStrike, un unico sensore è sufficiente per proteggere tutti gli endpoint e i workload, dai dispositivi IoT ai laptop, fino alle istanze di cloud computing. Utilizzando AWS Security Hub come dashboard, puoi aggregare e dare priorità agli alert di Falcon Cloud Security e di Amazon GuardDuty per proteggere le istanze Amazon EC2 o i container in esecuzione su Amazon ECS e Amazon EKS.

Mantieni le istanze Amazon EC2 protette e performanti

Falcon Cloud Security utilizza lo scaling cloud native per proteggere le istanze Amazon EC2 con un impatto minimo sulle prestazioni di runtime e senza scansioni temporali o aggiornamenti invasivi delle firme. Fornisce protezione contro tutti gli attacchi avanzati che eludono gli approcci tradizionali basati sul perimetro e sulle firme.

Proteggi i container in esecuzione su Amazon ECS e Amazon EKS

Falcon Cloud Security viene eseguita sul nodo dell'istanza Amazon EC2, proteggendo tutti i container in esecuzione su di esso, compresi quelli gestiti da Amazon ECS e Amazon EKS. Dal malware noto agli attacchi più sofisticati, Falcon protegge i container attraverso il monitoraggio e la scoperta dei workload, esaminando parametri come l'identificatore univoco del container e il tipo di configurazione, per poi inoltrare gli alert ad AWS Security Hub.

Shift left della sicurezza dei container nelle pipeline CI/CD

Lo spostamento delle attività di sicurezza nelle fasi precoci del ciclo di vita dello sviluppo del software consente ai team di individuare le falle prima che subiscano un forte impatto. Aggiungendo Falcon Cloud Security ai tuoi workflow di deployment CI/CD, ti assicuri la sicurezza del runtime per i workload Amazon ECS e Amazon EKS, oltre alla visibilità sulle applicazioni containerizzate. Visualizza e gestisci eventi come immagini di container rischiosi tramite la dashboard di AWS Security Hub.

1
agent leggero

0
riavvii necessari

I team DevOps possono codificare più facilmente

- Assicurati la protezione dal malware senza integrare dispositivi legacy
- Semplifica codice e script con un unico agent che si collega in modo fluido

I team di sicurezza migliorano la comprensione

- Metti in relazione gli alert AWS con Falcon Cloud Security per accelerare triage e remediation
- Fornisci una piattaforma di threat hunting per il team operativo

Difendi – con un'architettura semplificata

L'efficienza ottenuta con il lavoro congiunto di Falcon Cloud Security e AWS Security Hub, aiuta a velocizzare i tempi di detection, indagine e remediation per bloccare un maggior numero di compromissioni. Un servizio integrato per una completa sicurezza significa un team più efficiente che dedica meno tempo alla gestione di flussi di lavoro distinti. Massimizza la potenza di AWS Security Hub per aggregare gli eventi sfruttando la threat intelligence e l'architettura semplificata di CrowdStrike.

Semplifica le architetture AWS

Altri fornitori di sicurezza richiedono spesso routing complessi per le applicazioni legacy che devono essere inserite nel flusso dei pacchetti e numerosi agent di workload per fornire antivirus, EDR e sicurezza dei container che vengono installati e gestiti separatamente. Questo può aggiungere complessità agli ambienti AWS e aumentare i tempi di inattività. Falcon, come agent singolo, offre lo stesso livello di sicurezza con meno spese.

Accelera i tempi di risposta

Gli incidenti prioritari all'interno di AWS Security Hub aiutano a semplificare il processo di triage, consentendo al tuo team di affrontare per primo le minacce più critiche.

Aumenta l'efficienza per risparmiare sui costi

La possibilità di acquistare Falcon Cloud Security nel Marketplace di AWS ti permette di sfruttare i vantaggi del conteggio e della fatturazione integrati, ottimizzando al contempo la spesa per i workload elastici.

100.000 nodi
in un giorno per un deployment immediato

75%
più efficiente

Il DevOps può iniziare più in fretta

- Integra sicurezza e remediation con un sensore per endpoint
- Salta l'installazione: CrowdStrike si collega a una console basata su SaaS
- Promuovi un unico servizio di sicurezza per una protezione totale

Il Cloud architect ottimizzano i progetti

- Consolida l'architettura per costruzioni più semplici
- Dimensionamento in base all'espansione dei workload nel cloud, senza bisogno di infrastruttura aggiuntiva
- Potenti API rendono possibile l'automazione di tutte le aree funzionali per la difesa in profondità

Operare con eccellenza

La sicurezza informatica non è solo un problema tecnologico: per proteggere i workload AWS servono anche persone e processi efficaci. Ignorare le operazioni di sicurezza può comportare danni e attività di remediation che rallentano DevOps e riducono il tempo di attività delle applicazioni critiche.
Un simile impatto si potrebbe evitare se le tecnologie di sicurezza fossero opportunamente configurate e mantenute aggiornate e se gli alert di sicurezza venissero prontamente classificati, analizzati e risolti.

Molte organizzazioni si scontrano con questo aspetto operativo della sicurezza perché il personale qualificato necessario per eseguire la cybersecurity 24/7/365 può essere difficile da reperire e costoso da assumere.

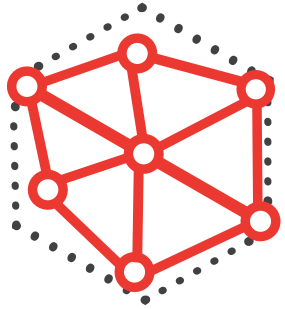
Amplia il tuo team con la detection e la risposta gestiti
CrowdStrike Falcon Complete è un servizio di detection e risposta gestiti (MDR) che accresce l'efficacia della piattaforma Falcon con l'efficienza di un team dedicato di professionisti della sicurezza. Falcon Complete si concentra sulla gestione e sul monitoraggio della sicurezza di endpoint e workload e risponde alle minacce con velocità e precisione, affinché non debba farlo tu.

I team DevOps subiscono meno interruzioni

- Il monitoraggio ininterrotto e la remediation chirurgica eliminano rapidamente le minacce senza intaccare il workload sottostante.

I team di sicurezza acquisiscono competenze ed efficacia immediate

- Messa a punto continua delle politiche di sicurezza per garantire massima efficacia
- Minacce identificate e debellate in pochi minuti
- Serenità supportata da una garanzia in caso di compromissione



Lo schema 1-10-60 è la tempistica ideale che consigliamo alle aziende di rispettare per essere più veloci degli avversari:

< 1 minuto
per rilevare le minacce

< 10 minuti
per comprendere le minacce

60 minuti
per eliminare le minacce

Inizia subito a utilizzare CrowdStrike su AWS

Per ulteriori informazioni sulle soluzioni CrowdStrike e AWS, visita:

- **CrowdStrike Falcon Cloud Security**
- **CrowdStrike page in the AWS Marketplace**
- **Approfondisci la tua postura di sicurezza con l'Analisi del rischio per la sicurezza del cloud**