CROWDSTRIKE

# CrowdStrike Falcon Cloud Security su AWS

aws PARTNER

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



eBook CrowdStrike

# Sommario

# Introduzione

In tutto il mondo, la tecnologia cloud sta alimentando organizzazioni di ogni dimensione e, sempre più spesso, le aziende si affidano o scelgono di migrare ad Amazon Web Services (AWS). I requisiti aziendali come flessibilità, innovazione e TCO spingono CTO e CIO ad adottare le tecnologie AWS. Questi Executive si affidano ad AWS affinché consenta loro di rispondere ai cambiamenti con velocità e sicurezza, dimensionare in modo efficace e promuovere la crescita dell'attività.

Man mano che le aziende si evolvono, devono evolversi anche le strategie di sicurezza per essere sempre un passo avanti alle minacce. Poter contare precocemente su una strategia di sicurezza per il cloud è fondamentale per essere pronti a tutto, visto che la tecnologia e i gli attacchi informatici diventano sempre più sofisticati.

Sia che la tua azienda sia stata costruita sul cloud o sia che ti trovi in mezzo al tuo percorso di adozione del cloud, riflettere sulla strategia di sicurezza è fondamentale. A prescindere dalla fase in cui ti trovi, la sicurezza del tuo computer deve essere un'esigenza primaria.

Nel panorama in evoluzione della tecnologia cloud in cui i cambiamenti sono una costante, c'è una cosa che possiamo garantire: gli avversari conoscono i rischi di sicurezza del cloud. E tu?

**52%**

**La percentuale di organizzazioni nordamericane che prevedono che almeno il 41% dei loro workload sarà gestito nel cloud nei prossimi 24 mesi.**

# Come rimanere protetti durante la migrazione al cloud

La tecnologia cloud ha favorito il rapido lancio di nuove imprese. Ha aiutato le aziende attuali a gettare le basi per l'innovazione e ha dato vita a una nuova serie di parametri di sicurezza e di minacce. Ma l'innovazione può anche includere rischi come lo sviluppo decentralizzato e l'implementazione delle policy, le lacune di visibilità tra le varie tecnologie e gli endpoint e il sempre pericoloso fattore umano: in altre parole, lo Shadow IT, l'architettura mal concepita e la mancanza di conoscenze e competenze.

Per le aziende che utilizzano la tecnologia cloud per creare infrastrutture e dimensionare a piacimento, la sicurezza significa garantire la protezione in un ambiente in costante evoluzione. Le app e le soluzioni esternalizzate costruite da terzi con standard di sicurezza e architetture diversi possono lasciare delle lacune nella sicurezza. Per questo, implementare precocemente una strategia di sicurezza è il modo migliore per mantenere una visibilità centralizzata sui vari componenti e servizi cloud.

Per chi sta migrando verso il cloud da tecnologie legacy, i rischi per la sicurezza sono presenti sia nei sistemi nuovi che in quelli precedenti. Le soluzioni ibride durante un processo di migrazione sono particolarmente vulnerabili, così come i sistemi e i database più vecchi accantonati, qualora non vengano smaltiti correttamente. La maggior parte delle migrazioni comporta anche la riqualificazione o l'assunzione di nuovi dipendenti e un cambiamento nella cultura aziendale. Se da un lato questo genera un fondamento valido per gestire i futuri cambiamenti tecnologici, dall'altro può anche causare problemi. Pertanto, mantenere una visione top-down della sicurezza nel bel mezzo di un'importante transizione tecnologica è fondamentale.

# L'approccio strategico alla sicurezza di CrowdStrike

Un metodo per proteggere i propri sistemi cloud è quello di rivolgersi a un partner di sicurezza come CrowdStrike. Con Falcon Cloud Security e il supporto di un team di esperti di sicurezza informatica, riceverai una protezione end-to-end, dall'host al cloud e in ogni punto intermedio, per workload e container su AWS.

## L'approccio CrowdStrike

- Focus sull'avversario
- Riduzione dell'esposizione
- Monitoraggio della superficie di attacco
- Protezione in fase di runtime
- Integrazione nella pipeline CI/CD

Gli avversari hanno adattato attacchi comuni in altri punti del panorama IT, come l'escalation delle autorizzazioni, il ransomware e lo sniffing di dati e pacchetti, al cloud. È probabile che emergano anche nuove tecniche di attacco cloud native. Le soluzioni di sicurezza cloud di CrowdStrike dispongono di alert e report in tempo reale su oltre 200 avversari direttamente integrati, quindi quando emergono nuove minacce, si sarà pronti a rispondere.

Per quanto riguarda la sicurezza del cloud, ridurre l'esposizione e la superficie di attacco significa segmentare i workload, risolvere le questioni in sospeso (soprattutto per chi abbandona i vecchi sistemi) e assicurarsi che la sicurezza sia la prima considerazione nell'utilizzo del cloud, detto anche shifting left. Una volta definita la superficie di attacco, il monitoraggio ad alta visibilità è il modo migliore per difendersi dai potenziali aggressori. Falcon Cloud Security offre analisi automatizzate, protezione runtime e a riposo, indicatori di attacco (IOA) cloud native e machine learning per una maggiore velocità di indagine.

### Falcon Cloud Security per DevSecOps e monitoraggio

Per chi crea su più ambienti, Falcon Cloud Security semplifica la gestione della postura con un'unica fonte di verità per tutte le risorse cloud e le configurazioni di sicurezza. Tutto ciò che devi vedere, in un unico posto. Grazie alla protezione IOA e al ripristino guidato basato su machine learning integrata direttamente nel piano di controllo, Falcon Cloud Security aiuta i team a gestire la compliance e a implementare in sicurezza le integrazioni AWS con maggiore efficienza.

### Falcon Cloud Security per la prevenzione delle compromissioni più completa

Mentre costruisci o sostituisci i sistemi con tecnologia cloud, Falcon Cloud Security assicura una protezione completa contro le compromissioni in ambienti privati, pubblici, ibridi e multi-cloud, consentendo ai clienti di adottare e proteggere rapidamente la tecnologia su qualsiasi workload. Con Falcon Cloud Security, puoi creare, eseguire e proteggere le applicazioni con velocità e sicurezza.

# Protezione dei container su AWS

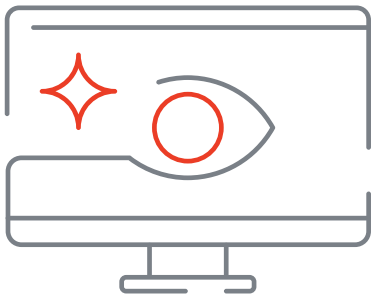
Garantire la protezione dei container è un altro elemento chiave di una strategia di sicurezza cloud efficace. Isolati e indipendenti per natura, i container limitano la visibilità. Spesso sono creati in base alla mentalità "imposta e dimentica" e lasciano in secondo piano la compliance alla sicurezza nel lungo termine. Ma anche con le migliori pratiche di monitoraggio, i container possono causare problemi nell'analisi della sicurezza a causa dell'enorme quantità di dati che producono nella scansione delle vulnerabilità.

Falcon Cloud Security affronta direttamente questi problemi. Il lightweight agent di CrowdStrike offre una visibilità completa sui container, sia che si tratti di implementazioni on-premise che in cloud. Il monitoraggio continuo e l'integrazione della pipeline CI/CD semplificano il controllo dei container e il loro ripristino se necessario. Inoltre, il monitoraggio di Falcon Cloud Security e la detection automatica continua delle minacce forniscono un'analisi agile dei dati sulle vulnerabilità AI/ML su grande scala e una protezione runtime con alert in tempo reale.

# La protezione del computing su AWS è semplice e facile con Falcon

Le organizzazioni che si affidano ad AWS conoscono il valore della tecnologia cloud per la migrazione di sistemi obsoleti e la creazione di applicazioni moderne. Sanno anche bene quale sia il valore delle partnership con aziende all'avanguardia tecnologica per alimentare i propri sistemi e far crescere la propria attività.

CrowdStrike Falcon Cloud Security si integra perfettamente con AWS Security Hub, è costruito con servizi AWS come Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Container Service (Amazon ECS) e Amazon Linux 2 e si distribuisce tramite AWS Systems Manager. I clienti AWS che collaborano con CrowdStrike sono operativi in pochi minuti e hanno immediatamente accesso a informazioni e analisi di tutti i loro servizi in un'unica console centrale. Inoltre, CrowdStrike Falcon Cloud Security opera con un ingombro minimo e ha zero impatto sulle prestazioni di runtime anche durante le attività di analisi, ricerca e investigazione.



## Dove AWS e CrowdStrike collaborano

### CrowdStrike e i servizi di computing AWS

- Workload di container
- Istanze Amazon EC2, incluso Graviton
- Amazon WorkSpaces
- Amazon Elastic Kubernetes Service
- Amazon Elastic Container Service
- AWS Fargate
- AWS Outposts

### CrowdStrike e integrazioni dei servizi AWS Cloud

- Accesso verificato da AWS
- AWS Account Factory Customization
- AWS Control Tower
- AWS Security Hub
- AWS Systems Manager
- AWS PrivateLink
- Amazon GuardDuty
- Firewall di rete AWS
- AWS CloudEndure Disaster Recovery

# Il momento di creare una strategia di sicurezza per il cloud è arrivato

Quando si tratta di sicurezza cloud, collaborare con un esperto che capisca i tuoi avversari, cosa cercano e come attaccano è il modo migliore per difendere la tua azienda. Come leader del settore della sicurezza informatica, CrowdStrike ha una comprovata esperienza nella prevenzione delle compromissioni.

## Per ulteriori informazioni sulle soluzioni CrowdStrike e AWS, visita:

- **CrowdStrike Falcon per AWS ›**
- **Prossimi eventi CrowdStrike e AWS ›**
- **CrowdStrike and AWS partner page ›**
- **CrowdStrike su AWS Marketplace ›**