

# FALCON HORIZON GESTIONE DELLA STRATEGIA DI SICUREZZA CLOUD

Blocca le compromissioni dei sistemi multicloud in tempo reale grazie a visibilità unificata, rilevamento delle minacce, monitoraggio continuo e gestione della conformità

## VEDERE DI PIÙ PER FARE DI PIÙ

Il passaggio al cloud ha trasformato radicalmente il modo in cui le aziende sviluppano le applicazioni e le immettono sul mercato. Il moderno ciclo di sviluppo delle applicazioni valuta sopra tutto la velocità di commercializzazione. Gli sviluppatori che lavorano per il cloud devono costruire applicazioni cloud native supportate da un'infrastruttura programmabile che consenta alle aziende di rimodulare e riconfigurare l'infrastruttura cloud al volo.

Dal momento che questa accelerazione fa emergere nuove sfide, i responsabili della sicurezza faticano a stare al passo. Il risultato? Visibilità e controllo insufficienti sulle risorse cloud, processi frammentari per il rilevamento e la prevenzione degli errori di configurazione, più incidenti informatici e incapacità di mantenere la conformità.

Falcon Horizon ottimizza la gestione della sicurezza degli ambienti cloud proteggendo l'intero ciclo di sviluppo delle applicazioni e permettendo di distribuire le applicazioni in tutta sicurezza, rapidamente ed efficacemente. La piattaforma cloud CrowdStrike Falcon® assicura visibilità sull'intera infrastruttura cloud, ricerca ininterrottamente gli errori di configurazione e svolge attività di rilevamento delle minacce consentendo ai team DevSecOps di correggere prontamente i problemi.

## PRINCIPALI VANTAGGI

Offre visibilità completa sugli ambienti multicloud e rappresenta un punto di riferimento unico per le risorse cloud

Previene automaticamente gli errori di configurazione e le vulnerabilità delle applicazioni

Valuta la sicurezza degli account cloud ed elimina le violazioni di conformità

Riduce il sovraccarico di avvisi di sicurezza e accelera la risposta agli incidenti

Migliora la qualità del codice e abbrevia i cicli di rilascio

Offre una protezione nativa per il cloud senza agent

# FUNZIONALITÀ PRINCIPALI

## RILEVAMENTO E VISIBILITÀ

Funzioni di rilevamento delle risorse e visibilità sull'infrastruttura cloud:

- Punto di riferimento affidabile per le risorse e le configurazioni di sicurezza di account e ambienti multicloud.
- Rilevamento automatico delle risorse implementate con dettagli quali errori di configurazione, metadati, dati di rete, informazioni di sicurezza, controllo degli accessi e modifiche. Servizi supportati:

AWS		
ACM	EKS	RDS
API Gateway v1	ElastiCache	Redshift
CloudTrail	ELB	Route 53
CloudFront	EMR	S3
CloudFormation	GuardDuty	SES
Config	IAM	SNS
DynamoDB	Kinesis	SQS
EBS	KMS	SSM
EC2	Lambda	VPC
ECR	NLB/ALB	

Azure	
Active Directory (AD)	Servizio Kubernetes
Servizio app	Bilanciamento del carico
Registro Container	Monitoraggio di Azure
Disco	Gruppi di sicurezza di rete
File di Azure	PostgreSQL
Identità	SQL Server nelle macchine virtuali
Key Vault	Account di archiviazione

- Gestione delle policy dei gruppi di sicurezza per account, progetti, regioni e reti virtuali utilizzando un'unica console.
- Visibilità su tutte le richieste di controllo alle API e ricerca dei rischi per la sicurezza dei cluster Kubernetes gestiti.
- Identificazione delle risorse cloud non protette da Falcon Horizon.

## RILEVAMENTO E CORREZIONE DEGLI ERRORI DI CONFIGURAZIONE

Elimina i rischi legati alla sicurezza e accelera il processo di distribuzione:

- Confronto delle configurazioni delle applicazioni cloud con riferimenti riconosciuti per rilevare le violazioni e correggerle in tempo reale.
- Correzione dei problemi che comportano un'esposizione delle risorse cloud – come errori di configurazione, porte IP aperte e modifiche non autorizzate – tramite procedure di correzione guidate e salvaguardie che prevengono errori gravi da parte degli sviluppatori.
- Monitoraggio delle risorse di archiviazione per verificare che le autorizzazioni di accesso siano protette e non accessibili pubblicamente.
- Individuazione e correzione automatiche dei rischi legati alle identità in Azure per prevenire attività pericolose da parte degli utenti aziendali.
- Utilizzo dei nuovi report di analisi delle identità **Identity Analyzer** per verificare che i gruppi, gli utenti e le app di Azure AD dispongano delle giuste autorizzazioni.
- Risoluzione rapida dei problemi e riduzione del sovraccarico di avvisi grazie alla nuova procedura di gestione delle policy migliorata per account, regioni o risorse cloud specifiche.
- Monitoraggio delle istanze del database – con verifica dell'abilitazione di disponibilità elevata, backup e crittografia – e dei gruppi di sicurezza per limitare le esposizioni.

## ELIMINA I PUNTI CIECHI DELLA SICUREZZA CON FALCON HORIZON

**Unifica la visibilità e il controllo negli ambienti multicloud:** Falcon Horizon assicura un rilevamento continuo delle risorse cloud e una visibilità ininterrotta sull'ambiente cloud fornendo preziose informazioni di contesto sullo stato di sicurezza complessivo e sugli interventi necessari per prevenire potenziali incidenti di sicurezza.

**Previene gli errori di configurazione del cloud ed elimina le violazioni di conformità:** Falcon Horizon esegue un monitoraggio intelligente delle risorse cloud grazie al quale rileva in anticipo errori di configurazione, vulnerabilità e rischi di sicurezza e propone interventi di remediation guidati per eliminare i rischi, evitare che gli sviluppatori commettano errori costosi e garantire il rispetto della conformità negli ambienti multicloud.

**Riduce il sovraccarico di avvisi di sicurezza grazie al rilevamento mirato delle minacce:** Falcon Horizon cerca ininterrottamente anomalie e attività sospette, si integra alla perfezione con le soluzioni SIEM, consente ai team di sicurezza di ottenere visibilità, classificare le minacce in base alla gravità, ridurre il sovraccarico di avvisi eliminando quelli ininfluenti e di affrontare e risolvere i problemi più rapidamente.

**FALCON HORIZON**  
**GESTIONE DELLA STRATEGIA DI SICUREZZA CLOUD**

## RILEVAMENTO DELLE MINACCE IN TEMPO REALE

Rilevamento immediato delle minacce lungo l'intero ciclo di sviluppo delle applicazioni:

- Individuazione degli avvisi di sicurezza significativi dell'ambiente multicloud grazie all'approccio mirato volto a identificare e gestire le minacce.
- Riduzione drastica del numero di avvisi esaminato considerando gli ambiti che gli attaccanti hanno maggiore probabilità di colpire.
- Definizione della priorità delle vulnerabilità in base all'ambiente e analisi del codice per evitare che le vulnerabilità entrino in produzione.
- Ricerca continua di attività malevole, comportamenti e accessi non autorizzati alle risorse cloud tramite il rilevamento delle minacce in tempo reale.

## MONITORAGGIO CONTINUO DELLA CONFORMITÀ

Valuta la sicurezza degli account cloud ed elimina le violazioni di conformità:

- Monitoraggio continuo della stato di conformità di tutte le risorse cloud utilizzando un'unica console.
- Controllo di conformità con generazione di report dettagliati che permettono di valutare se gli account cloud sono conformi alle linee guida CIS di Docker e Kubernetes.
- Rilevamento delle violazioni delle policy e richiesta di intervento immediato dell'utente per ripristinare la conformità.

## INTEGRAZIONE DELLE OPERAZIONI DI SVILUPPO E SICUREZZA

La gestione della sicurezza cloud nativa e agentless consente di ridurre i costi e di eliminare attriti e complessità per gli account e i provider multicloud:

- Visibilità e controllo gestiti centralmente su tutte le risorse cloud affinché i responsabili di sicurezza e sviluppo (DevOps) possano fare riferimento a una fonte di informazioni unica.
- I responsabili della sicurezza sono autorizzati a bloccare le risorse compromesse impedendo che vengano immesse nel ciclo di produzione delle applicazioni.
- Grazie all'integrazione con SIEM, migliore visibilità per le operazioni di sicurezza, disponibilità di più dati contestuali sugli errori di configurazione e sulla violazione delle policy e risposta agli incidenti più rapida.
- Un'unica API facilita l'integrazione e le operazioni di remediation tra DevOps e gli strumenti di collaborazione già in uso, tra cui e-mail, Slack e PagerDuty.
- L'utilizzo di report e dashboard favorisce maggiore allineamento e collaborazione tra team di sicurezza, DevOps e responsabili delle infrastrutture.

## 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.

Per maggiori informazioni, visita [www.crowdstrike.com/it](http://www.crowdstrike.com/it)

