



## CROWDSTRIKE FALCON: IL NUOVO STANDARD NELLA PROTEZIONE DEGLI ENDPOINT

LA SICUREZZA DEGLI ENDPOINT BASATA  
SU UN APPROCCIO SEMPLICE, MA POTENTE



L'agente a basso impatto di CrowdStrike Falcon e un potente cloud lavorano assieme e senza interruzioni per fornire protezione e visibilità in tempo reale: **sempre, anche quando l'agente non è collegato a internet.** CrowdStrike Falcon garantisce una prevenzione efficace dalle minacce grazie all'intelligenza artificiale (AI), al Machine Learning (ML), a funzioni di rilevamento e risposta avanzate e all'integrazione con la threat intelligence: il tutto tramite una console di gestione altamente intuitiva.

### PERCHÉ CROWDSTRIKE FALCON?

#### PROTEZIONE COMPLETA

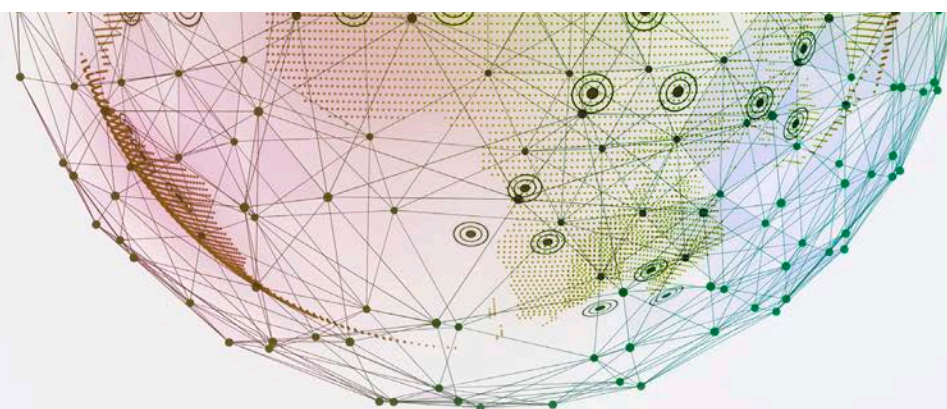
Prevenzione e rilevamento immediati ed efficaci di tutti i tipi di attacchi, sia in presenza che in assenza di malware, indipendentemente dal fatto che siate online oppure offline

#### VISIBILITÀ IMPAREGGIABILE

Un "DVR" per il vostro endpoint a cui non gli sfugge nulla. Scoprite in pochi secondi le attività correnti dei vostri endpoint ed investigate su quelle passate

#### MASSIMA FACILITÀ DI UTILIZZO

Una piattaforma basata sul cloud rende facile la distribuzione, la configurazione e la manutenzione: il tutto usando un unico agente a basso impatto



#### CROWDSTRIKE: PROVATO, TESTATO, GARANTITO

Con CrowdStrike, potete essere sicuri che la vostra organizzazione è finalmente protetta dagli attacchi informatici, che siano noti o sconosciuti, sia quando utilizzano malware che quando non. Ma non fidatevi solo delle nostre parole, guardate che cosa dicono gli esperti a proposito di CrowdStrike Falcon:

### "VISIONARIO"

- Quadrante Magico per le piattaforme di protezione degli endpoint  
di Gartner - gennaio 2017

### "STRONG PERFORMER"

- Forrester Wave: Sicurezza degli endpoint - ottobre 2016

### "APPROVED BUSINESS SECURITY PRODUCT"



- AV Comparatives - dicembre 2016

SEDE CENTRALE 15440 Laguna Canyon Road, Suite 250 Irvine,  
California 92618, U.S.A. | +1 (888) 512-8906 | info@crowdstrike.com  
sales@crowdstrike.com | crowdstrike.com

SEDE ITALIANA +39 0282 952 424

Vittima di un attacco? Contattateci al numero +1 (855) 276-9347 o all'indirizzo  
e-mail services@crowdstrike.com



CROWDSTRIKE

# COSTRUITO PER BLOCCARE LE COMPROMISSIONI

Protezione degli endpoint basata sul cloud



## CROWDSTRIKE FALCON: RENDERE POSSIBILE L'IMPOSSIBILE

È stato detto che era impossibile realizzare una protezione completa degli endpoint usando un unico agente a basso impatto sugli utenti e sulle prestazioni dei sistemi. Abbiamo dimostrato che non è vero. Grazie alle capacità senza precedenti di visibilità, protezione e risposta in tempo reale di CrowdStrike Falcon **è ora possibile:**

- Prevenire sia gli attacchi commodity che quelli sofisticati, sia quando vengono usati dei malware che quando no, senza differenze se i vostri endpoint sono online oppure offline.
- Ottenere visibilità dettagliata e in tempo reale delle applicazioni e dei processi in esecuzione nel vostro ambiente, garantendo che nulla sia tralasciato e che sia possibile intervenire nel caso sia richiesta una attività di risposta.
- Dare la caccia proattivamente alle attività di attacco più avanzate, in maniera più rapida ed efficace di prima.
- Proteggere gli endpoint per tutte le principali piattaforme, inclusi Windows, OS X e Linux, i server dei data center, le macchine virtuali e le piattaforme cloud come AWS, Azure e Google.
- Sostituire il vostro antivirus inefficace per distribuire una soluzione di nuova generazione, testata e certificata da enti indipendenti come capace di rimpiazzare efficacemente gli antivirus.





## Panoramica delle soluzioni CrowdStrike

### FALCON DISCOVER

#### IT Hygiene

Falcon Discover identifica i sistemi non autorizzati e le applicazioni presenti in tutta la vostra infrastruttura in tempo reale, permettendo una remediation rapida che aumenta il vostro livello di sicurezza.

### FALCON PREVENT

#### Next-Generation Antivirus (NGAV)

Falcon Prevent protegge da tutti gli attacchi, sia quando utilizzano malware che non, ed è inoltre stato testato e certificato da enti indipendenti per la sostituzione dei loro antivirus.

### FALCON INSIGHT

#### Endpoint Detection & Response (EDR)

Falcon Insight offre visibilità continua e completa degli endpoint, che include funzionalità di detection, response e forensic, garantendo che non venga tralasciato nulla e che eventuali compromissioni possano essere bloccate sul nascere.

### FALCON OVERWATCH

#### Managed Threat Hunting

Il team Falcon OverWatch lavora senza interruzione 24x7 per moltiplicare gli sforzi dei vostri team interni di sicurezza al fine di individuare le attività malevoli il prima possibile, bloccando subito gli avversari.

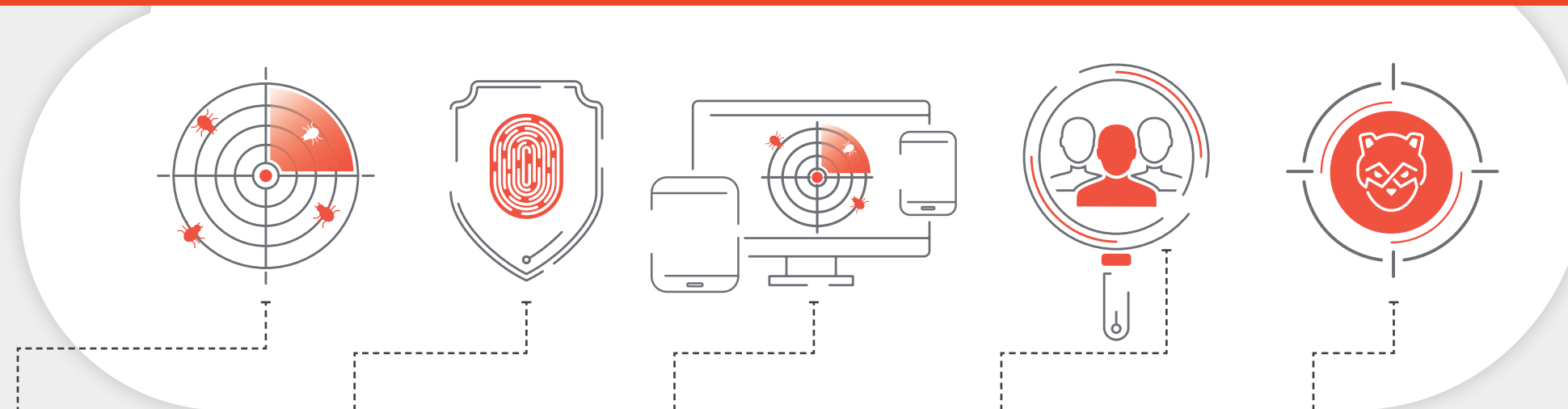
### FALCON INTELLIGENCE

#### Threat Intelligence

Falcon Intelligence monitora le attività degli avversari a livello globale, fornendo report personalizzati e analisi di immediata utilità per i team operativi, aiutando a migliorare il livello di sicurezza della vostra azienda.

# PROTEZIONE DEGLI ENDPOINT BASATA SUL CLOUD

## PIATTAFORMA FALCON



#### IT HYGIENE

Dovete essere pronti per affrontare qualsiasi tipo di attacco, ma non potete rimediare a ciò che non vedete. Le organizzazioni necessitano una visibilità completa in tempo reale di tutto il loro ambiente, di identificare tutti gli endpoint gestiti e non, di avere un inventario delle applicazioni installate, il tutto con l'obiettivo di effettuare azioni immediate per migliorare la loro sicurezza.

#### NEXT GENERATION ANTIVIRUS (NGAV)

Per proteggervi dagli attacchi sia in presenza che in assenza di malware, avete bisogno di un antivirus di nuova generazione di efficacia testata che combini molteplici tecnologie di prevenzione, come il machine learning, le funzioni di exploit blocking e analisi comportamentale avanzata con gli Indicatori di Attacco (IOA).

#### ENDPOINT DETECTION & RESPONSE (EDR)

Soluzione EDR completa che registra continuamente gli eventi degli endpoint permettendo di scoprire e indagare ogni attività in meno di 5 secondi, fornendo dettagli di cosa sta accadendo nei vostri sistemi e garantendo che gli attaccanti non abbiano posti dove nascondersi.

#### MANAGED THREAT HUNTING

Utilizzare le tecnologie di difesa più avanzate può essere non sufficiente. Per sconfiggere gli avversari più sofisticati è necessario un team dedicato che lavora 24x7 dando proattivamente la caccia a comportamenti sospetti e sfruttando la "forza del gruppo" per identificare minacce nuove ed emergenti.

#### THREAT INTELLIGENCE

Non potete proteggervi da un rischio che non conoscete. Le informazioni di Threat Intelligence vi permettono di comprendere le motivazioni dei vostri avversari, anticipare le loro tecniche e applicare azioni efficaci per evitare che riescano a compromettere la vostra organizzazione.



## Servizi di CrowdStrike:



### SERVIZI DI INCIDENT RESPONSE

I servizi completi di risposta (IR) prima e dopo gli incidenti sono disponibili 24x7 per assistere prima, durante e dopo aver subito un attacco. Questi team altamente specializzati forniscono le capacità necessarie per difendere la vostra azienda da compromissioni o supportarvi nella risposta di incidenti già riscontrati, prevenendo le compromissioni e migliorando la vostra velocità nel porvi rimedio.



### SERVIZI PROATTIVI

Il team di assistenza di CrowdStrike può lavorare con voi per anticipare le minacce, preparando la vostra rete a contrastare le intrusioni e migliorando la capacità del vostro personale nel prevenire i danni dovuti ad eventuali attacchi informatici. I servizi proattivi comprendono compromise assessment, penetration test "next-gen" ed esercizi simulati, nonché programmi di sviluppo delle capacità di IR e del SOC (Security Operations Center).