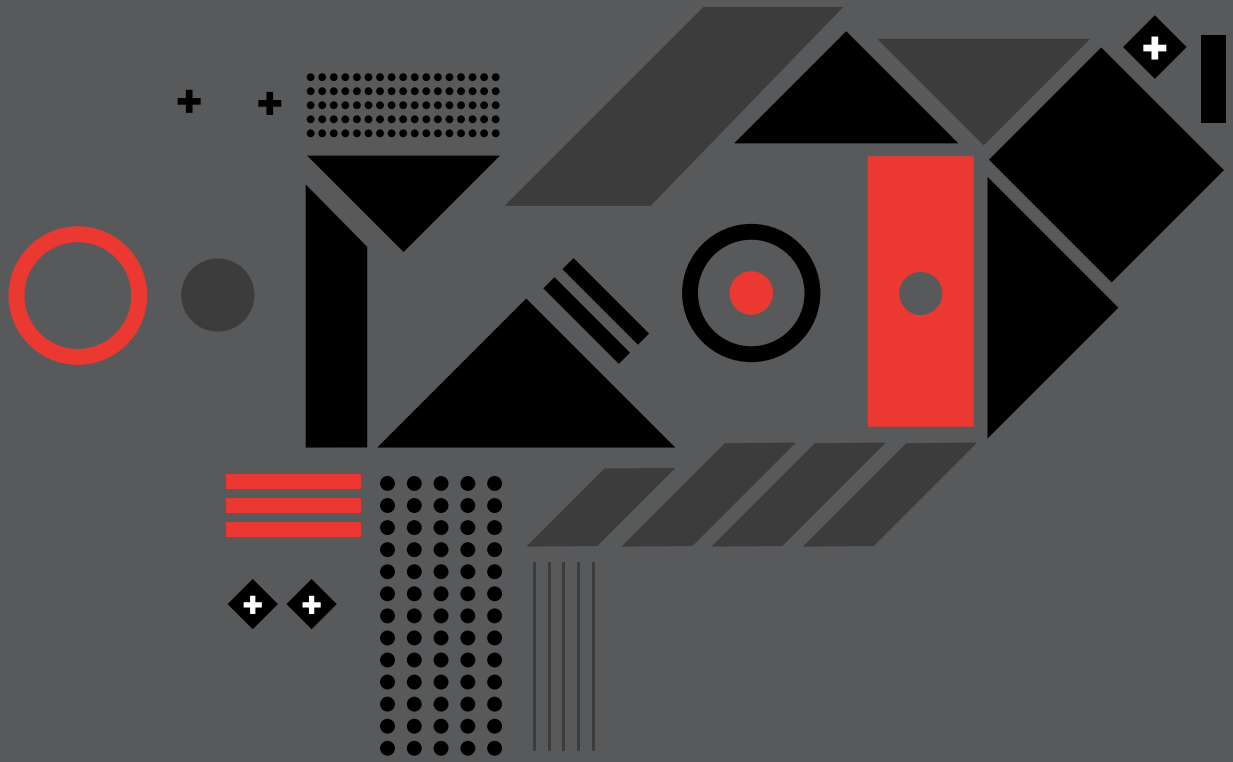
eBook

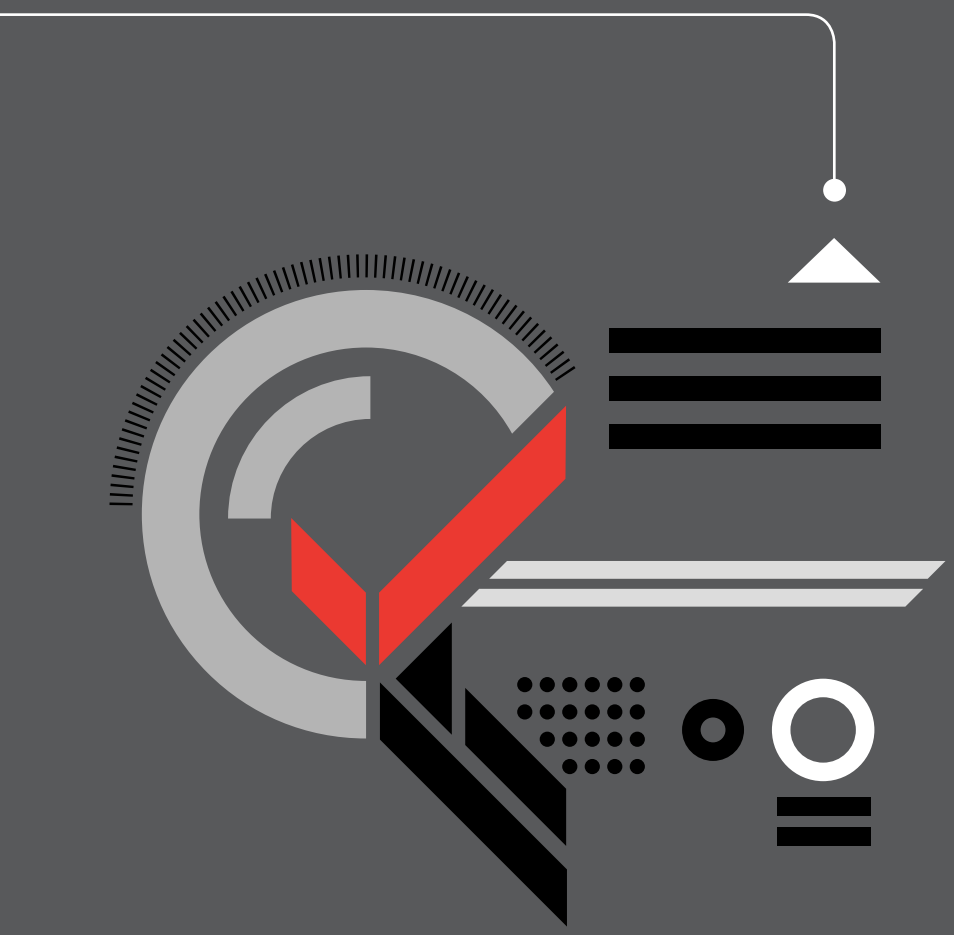


LAVORA DA QUALSIASI LUOGO E SEMPRE IN SICUREZZA

PROTEGGI I COLLABORATORI CHE LAVORANO IN MODO IBRIDO, TUTELA I TUOI DATI E RAFFORZA LA RESILIENZA AZIENDALE CON LA PIATTAFORMA CROWDSTRIKE FALCON SU AMAZON WORKSPACES

CROWDSTRIKE | aws

SOMMARIO

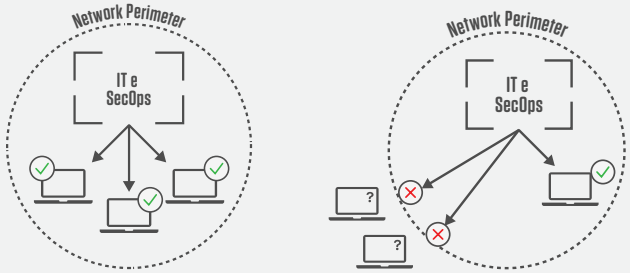


IL PERSONALE IN REMOTO SFIDA I PARAMETRI DI SICUREZZA

Lavorare da remoto è una tendenza che non finirá presto. Il modello che si sta affermando è quello ibrido, in cui alcuni dipendenti lavorano completamente in remoto, altri tornano in ufficio e altri ancora scelgono un mix delle due opzioni, andando in ufficio solo alcuni giorni della settimana. In questo mondo in cui si lavora da qualsiasi luogo, le sfide per mantenere la sicurezza e garantire la resilienza aziendale si moltiplicano, in un momento in cui la maggior parte delle aziende sta ancora lottando per fare sempre di più con meno.

L'accelerazione dell'adozione del cloud sposa il crescente modello di lavoro ibrido

Con la transizione al lavoro agile, molte aziende sono state costrette ad accelerare l'adozione delle tecnologie cloud per stare al passo, spostando i loro modelli di sicurezza informatica da soluzioni on-premise a soluzioni cloud. Ora che il lavoro ibrido è il nuovo standard, queste aziende stanno scoprendo che gli approcci adottati per necessità in condizioni di massima pressione per tempi e operatività non sono sufficienti a salvaguardare i loro lavoratori ibridi, o i rispettivi dati, a lungo termine.



Le aziende lungimiranti stanno adottando un approccio alla sicurezza informatica cloud native basato su un framework che protegge chiunque, ovunque.

Protezione in tempo reale

Previeni le minacce, rileva le attività sospette e rispondi agli incidenti informatici – il tutto in tempo reale, indipendentemente da dove si trovano i tuoi utenti o i tuoi dispositivi.

Protezione degli endpoint

Elimina la complessità, semplifica le operazioni di sicurezza e esegui il deploy in tempi record. Attiva immediatamente il Vulnerability Management e l'IT Hygiene con Falcon Spotlight™ e Falcon Discover™.

Per tutti i dispositivi

L'architettura basata su un unico agent Falcon molto leggero funziona ovunque, anche nei carichi di lavoro cloud e nei data center, e protegge gli utenti sia sui dispositivi di proprietà dell'azienda che su quelli personali.

Sei fattori chiave che supportano la sicurezza informatica dei lavoratori in remoto

1. Assicurati di disporre di una policy di sicurezza informatica aggiornata che includa norme per il lavoro da remoto.
2. Pianifica la connessione dei dispositivi personali dei dipendenti BYOD (bring your own device) al sistema aziendale.
3. Ricorda sempre che si potrebbe accedere a dati sensibili da reti Wi-Fi non sicure.
4. La visibilità e l'Hygiene della sicurezza informatica sono elementi critici.
5. È estremamente importante che gli utenti restino continuamente aggiornati e informati e che i lavoratori remoti abbiano la possibilità di contattare tempestivamente il personale IT in caso di problemi.
6. I piani di gestione delle crisi e di risposta agli incidenti devono essere attuabili dalla forza lavoro remota.

PROTEGGI I COLLABORATORI CHE LAVORANO IN MODO IBRIDO CON FALCON E AMAZON WORKSPACES

Proteggere identità e dati dei dipendenti

Con Amazon WorkSpaces, i dipendenti che lavorano da qualsiasi luogo hanno a disposizione una soluzione desktop-as-a-service sicura che consente loro di accedere ai propri desktop ovunque si trovino. Installare il sensore CrowdStrike Falcon in un ambiente Amazon WorkSpaces migliora ulteriormente la postura di sicurezza e contribuisce a mitigare i rischi derivanti dalle minacce alla sicurezza informatica.

Amazon WorkSpaces fornisce una soluzione desktop-as-a-service per i lavoratori ibridi

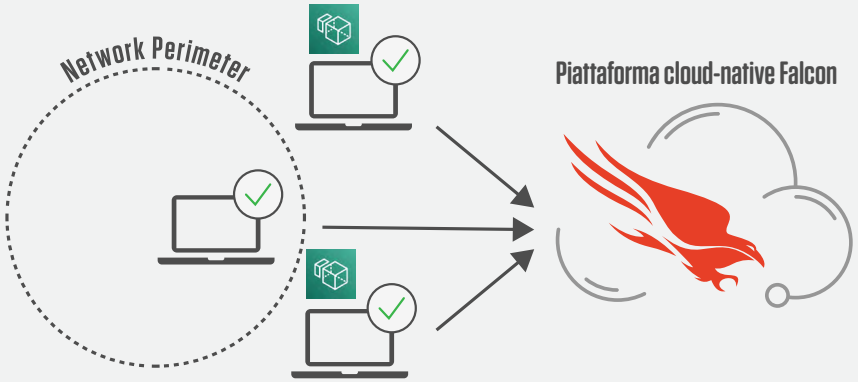
- Offri un desktop in cloud accessibile ovunque esista una connessione Internet
- Operatività su un'ampia gamma di dispositivi, tra cui PC, Mac e iPad
- Elimina le attività amministrative come il provisioning, il deploying e la manutenzione dei desktop

La piattaforma CrowdStrike Falcon blocca le compromissioni offrendo una protezione degli endpoint nativa in cloud e senza attriti.

- Installa rapidamente dal cloud attraverso una soluzione SaaS per mantenere protetti tutti i dispositivi, indipendentemente dalla loro posizione
- Utilizza la soluzione in modo trasparente per proteggere l'intera gamma di potenziali modelli di lavoro senza sacrificare le performance
- Riduci la complessità con una soluzione SaaS in cloud che non richiede hardware e aiuta a ridurre i costi di esercizio

L'APPROCCIO ALLA SICUREZZA DI CROWDSTRIKE PROTEGGE DALLE COMPROMISSIONI

Il sensore leggero Falcon si installa facilmente nell'ambiente WorkSpaces dell'utente finale, per un set up sicuro da qualsiasi luogo si lavori. Insieme, queste soluzioni cloud-native consentono di mantenere la continuità aziendale assicurando la protezione dalle minacce emergenti, abilitando una soluzione ibrida sicura e tagliando i costi grazie alla riduzione delle spese di esercizio.



80%
le violazioni dovute a credenziali compromesse

Sconfiggi gli avversari piú temibili

Con le nuove minacce che prendono di mira le vulnerabilità dei dipendenti ibridi, la sicurezza di Amazon Virtual Private Network (VPC) unita alla protezione degli endpoint offerta della piattaforma Falcon sono fondamentali. Proteggi il tuo personale ibrido con una soluzione di sicurezza informatica che unisce machine learning, intelligenza artificiale e threat hunting proattivo.

Rispondi, recupera e ripristina da remoto

Falcon abilita la protezione da remoto per tutelare i dati, i workload e i dispositivi del tuo personale, indipendentemente da dove lavorino. Ripristina rapidamente gli host remoti con una potente soluzione cloud native.

Compensa i costi per promuovere la resilienza

I desktop-as-a-service tramite WorkSpaces e l'architettura cloud native di Falcon riducono significativamente l'hardware e la necessità di fornire dispositivi e software. Adotta un approccio completamente gestito per ridurre le spese di esercizio e migliorare la resilienza aziendale.

DIFENDITI DAGLI AVVERSARI PIÙ AUDACI

Dietro ogni attacco si cela un avversario in carne e ossa. Questi autori delle minacce sono in continua evoluzione e utilizzano eventi rilevanti per mascherare i loro attacchi.

CrowdStrike è sempre aggiornata sulle minacce emergenti e ha progettato il sensore Falcon per garantire una visibilità approfondita delle vulnerabilità. Come sensore integrato in Amazon WorkSpaces, Falcon ti consente di mantenerti all'erta per proteggere sia i tuoi lavoratori ibridi che i dati nel cloud.

Protezione completa: dal cloud in su

Il deployment degli Amazon WorkSpaces avviene all'interno dei VPC di Amazon, che forniscono a ciascun utente l'accesso a volumi di archiviazione persistenti e crittografati nel Cloud AWS e si integrano con AWS Key Management Service. I dati degli utenti non vengono memorizzati sul dispositivo locale, il che migliora la sicurezza dei dati utente e riduce al minimo la superficie di rischio anche per i lavoratori ibridi.

Detection e prevenzione in tempo reale

Grazie alle informazioni ricavate dal Threat Graph Intelligence, Falcon offre la detection e il rilevamento in tempo reale delle minacce note e sconosciute, tra i piú efficaci sul mercato. Gli endpoint sono protetti dagli avversari 24 ore su 24, 7 giorni su 7.

Falcon si concentra su qualcosa di più del malware e adotta un approccio ai criminali informatici che non solo identifica gli indicatori di compromissione, ma anche gli indicatori di attacco.

LE BEST PRACTICE DELLA SICUREZZA INFORMATICA PER UN MONDO IBRIDO

La sicurezza informatica in un mondo in cui si lavora da qualsiasi luogo richiede un approccio diverso. I sistemi che proteggono gli utenti di un ufficio richiedono una scansione ad elevata ampiezza di banda per identificare i sistemi, valutare le patch e visualizzare le vulnerabilità. In uno scenario di lavoro ibrido, questa configurazione non è più fattibile. I lavoratori che entrano ed escono dall'ufficio, e che accedono ai dati aziendali su dispositivi gestiti e non gestiti, creano enormi punti ciechi per il team di sicurezza IT, oltre a introdurre rischi che possono rallentare i tentativi di porre rimedio alle minacce.

Per affrontare le sfide della sicurezza informatica nel nuovo assetto del mondo del lavoro, gli esperti di CrowdStrike propongono le seguenti best practice:

Responsabilizza i lavoratori e sfrutta la tecnologia

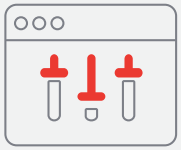
Per pianificare una strategia di sicurezza informatica completa ed efficace occorre iniziare dalla considerazione delle policy, dei processi e delle tecnologie di ogni funzione aziendale. Le strategie di sicurezza informatica più efficaci fondono le risorse umane con soluzioni tecnologiche avanzate, come l'intelligenza artificiale, il machine learning e altre forme di automazione intelligente per rilevare meglio le attività anomale e aumentare i tempi di risposta e ripristino.

Scegli attentamente il tuo cloud

Non tutti i cloud sono uguali quando si tratta di assicurarsi i vantaggi di questa tecnologia senza compromettere la sicurezza. Amazon Web Services (AWS) è stato creato con i più alti standard di sicurezza dei dati, con controlli di identità e accesso dettagliati per una visibilità superiore. Le funzionalità di prevenzione e rilevamento offerte da CrowdStrike per Amazon Workspaces supportano i dipendenti in remoto senza compromettere la continuità aziendale.

Abilita la risposta, il recupero e il ripristino da remoto

Gli attacchi e le intrusioni non si fermeranno ed è tuo compito assicurarti di poter disporre delle risorse e delle capacità per rispondere da qualsiasi luogo al fine di proteggere la tua azienda. L'architettura basata sul cloud di Amazon WorkSpaces e Falcon ti permette di proteggere ogni workload ovunque, anche al di fuori di firewall, fornendo funzionalità di sicurezza in tempo reale.



Semplifica l'erogazione del desktop

Come servizio cloud, Amazon WorkSpaces assicura un minor carico hardware da gestire e non richiede complessi deployment di infrastrutture desktop virtuali che non si possono dimensionare. Amazon WorkSpaces è disponibile in 13 regioni AWS e consente di accedere a desktop cloud ad alte prestazioni ovunque i tuoi team lavorino.

LA CREAZIONE DI UNA RETE PROTETTIVA INIZIA CON LA GESTIONE DEI COSTI

Le aziende di tutto il mondo sono alle prese con l'incertezza. Nel tentativo di potenziare la resilienza aziendale, le imprese hanno interrotto temporaneamente le iniziative di crescita, bloccato i budget e iniziato ad accumulare riserve in cash. Con Amazon WorkSpaces e Falcon, le aziende dispongono di un metodo per abilitare in modo sicuro le operazioni aziendali e mantenere bassi i costi.

Cloud architecture conveniente

Le funzionalità di gestione centralizzata di Amazon Workspaces per i lavoratori in remoto aiutano a dimensionare l'accesso ai desktop cloud. Mentre continui a supportare il tuo personale ibrido, non è più necessario pianificare, preparare e fornire hardware e software per stare al passo, risparmiando tempo e denaro. Inoltre, Amazon WorkSpaces elimina la necessità di acquistare risorse per desktop e laptop in eccesso fornendo accesso on-demand a desktop cloud che includono una gamma di risorse di cloud computing, memoria e archiviazione per soddisfare le esigenze lavorative del tuo personale ibrido. La piattaforma CrowdStrike Falcon esegue la scansione di tutti gli endpoint per garantirne la protezione a prescindere dalla loro ubicazione e senza alcun impatto sulle prestazioni.

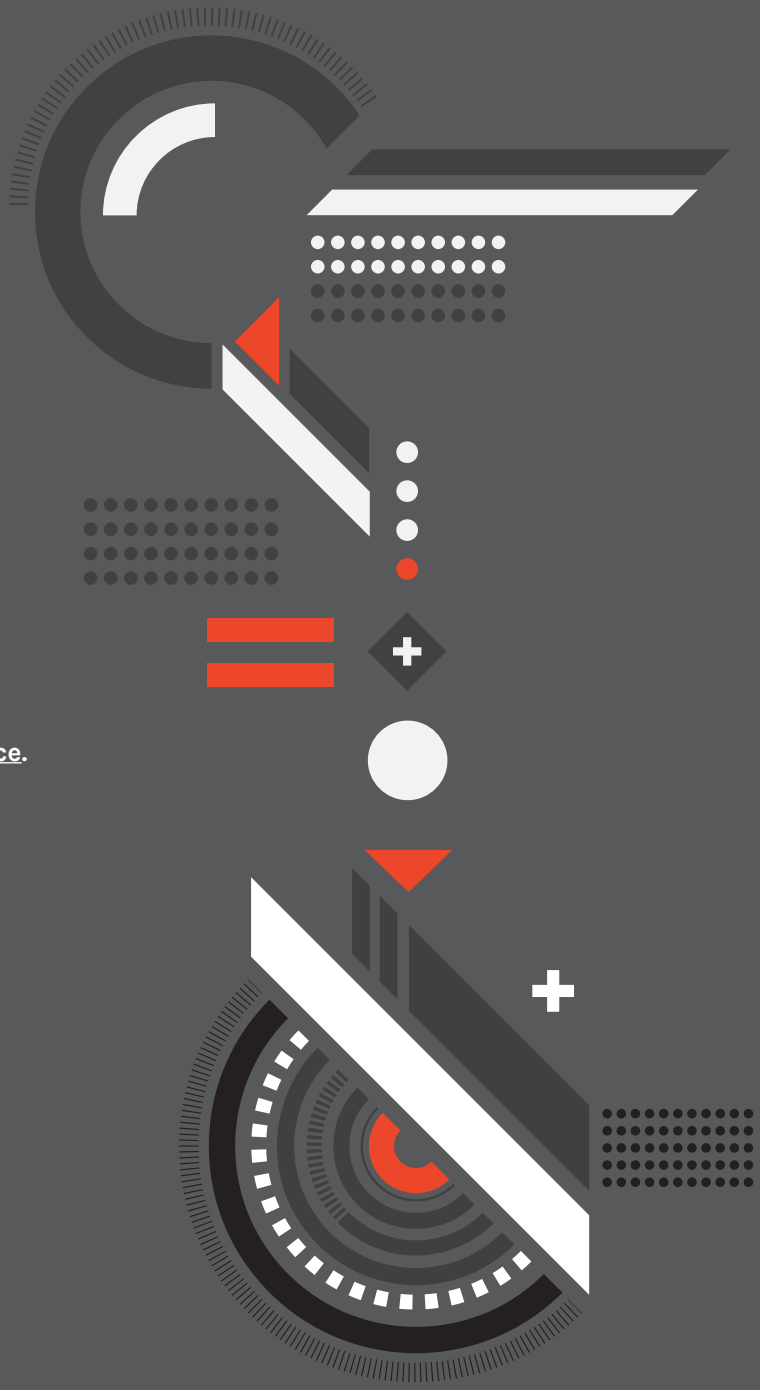
Completamente gestito per ridurre le spese di esercizio

Le organizzazioni hanno la possibilità di intensificare i loro sforzi in ambito di sicurezza informatica implementando la protezione degli endpoint di Falcon come servizio completamente gestito. Questa soluzione "scaccia pensieri" ti permette di affidare l'implementazione, la gestione e la risposta agli incidenti informatici degli endpoint al collaudato team di esperti di sicurezza di CrowdStrike. Il risultato è una postura di sicurezza istantaneamente ottimizzata senza l'onere, le spese e i costi di gestione interna di un programma completo di sicurezza degli endpoint.

È ORA DI PROTEGGERE IL TUO MONDO IN CUI SI LAVORA DA QUALSIASI LUOGO

Con CrowdStrike è facile iniziare. Per saperne di più sull'implementazione della piattaforma CrowdStrike Falcon e/o su Amazon Workspaces, **scarica la nostra prova gratuita valida 15 giorni**.

Per maggiori informazioni sulle soluzioni CrowdStrike e AWS, visita **CrowdStrike** o **AWS Marketplace**.



aws marketplace