Gruppo Credem: come gestire efficacemente la sicurezza di diecimila endpoint

CREDEM

ITALY
6,500+ DIPENDENTI
SERVIZI FINANZIARI

Il Gruppo Credem è una delle principali realtà bancarie italiane. Fondato nel 1910 su iniziativa di alcuni imprenditori reggiani, oggi è presente a livello nazionale in 19 regioni tramite quasi 600 filiali e centri imprese, a cui vanno aggiunti 800 promotori finanziari con uffici dedicati.

L'esigenza di garantire i massimi livelli di cybersecurity, oltre a essere dettata da normative ad hoc, come ad esempio la Direttiva europea NIS2 e il Regolamento DORA, deriva dalla specificità del comparto.

> **Per le banche la cybersecurity è importante perché ormai, da una quindicina d'anni, i servizi vengono erogati in ambito digitale: la banca è digital.**

Francesco Puccioni
Head of Cybersecurity Operations

SFIDE

- **Crescita esponenziale dell'ecosistema IT**
- **Complessità di gestione e aggiornamento di sistemi di protezione separati (EDR e Antivirus)**
- **Tempistica nell'analisi e individuazione delle minacce + Elevato numero di falsi positivi**

SOLUZIONI

- **Consolidamento di EDR e Antivirus in unica piattaforma**
- **Blocco proattivo di ~150 eventi malevoli l'anno**
- **Maggiore velocità nell'individuazione del problema**

© 2026 CROWDSTRIKE, INC.

Un'evoluzione che è coincisa, nel corso del tempo, con la crescita esponenziale dell'ecosistema IT da «mettere sotto sorveglianza». Di questo ecosistema fanno parte gli endpoint, che nel Gruppo sono diecimila, e le interconnessioni tra vari servizi, compresi quelli forniti da terzi in ambito di application e service management, senza dimenticare le nuove sfide poste dall'adozione massiccia dell'Intelligenza Artificiale generativa. Il moltiplicarsi di questi fattori fa sì che gli "eventi" da analizzare non crescano più in modo lineare, ma in maniera esponenziale. Un tale volume di dati pone un limite alle capacità di analisi puramente umane degli operatori; si tratta di un lavoro che oggi non può essere svolto senza una strategia combinata di integrazione e automazione.

Perché Gruppo Credem ha scelto CrowdStrike

L'adozione delle soluzioni CrowdStrike, da parte del Gruppo Credem, è avvenuta tra il 2023 e il 2024 alla naturale scadenza della soluzione precedente di endpoint detection and response (EDR). «È stato un percorso lineare. Secondo noi - spiega Puccioni - CrowdStrike è il partner best of breed per affiancarci nella protezione di tutti i potenziali eventi malevoli che possono verificarsi sui nostri endpoint. L'adozione è stata frutto di un'attenta analisi e valutazione di diversi aspetti. Inizialmente la scelta si è concentrata sull'individuazione del miglior sistema antimalware e EDR per tutti gli endpoint di Gruppo Credem. Successivamente, l'analisi si è estesa fino a includere la valutazione e l'adozione del modulo di Device Control. Una roadmap strategica che ha sempre tenuto conto dei rigorosi requisiti richiesti dalle Authority in materia di cybersecurity e resilienza».

Credem Group ha scelto di potenziare la propria postura di sicurezza attraverso la piattaforma CrowdStrike, focalizzandosi su strumenti di monitoraggio EDR, protezione preventiva degli endpoint, gestione delle policy dei firewall, controllo degli accessi ai dispositivi fisici e mobili.

> **Consideriamo CrowdStrike il partner best of breed ideale per affiancarci nella protezione dei nostri endpoint da qualsiasi potenziale criticità.**
>
> FRANCESCO PUCCIONI
>
> Head of Cybersecurity Operations di Credem

© 2026 CROWDSTRIKE, INC.

Se Falcon Insight endpoint detection and response (EDR), Falcon Prevent e Falcon Firewall Management rappresentano strumenti fondamentali nell'individuazione di possibili malware, Falcon Device Control permette di evidenziare e prevenire eventuali esfiltrazioni di dati sui device. In sostanza, consente di effettuare un'analisi e di implementare policy di blocco sulle periferiche di archiviazione installate o collegate ai vari endpoint.

I benefici operativi e strategici della piattaforma Falcon

L'adozione della piattaforma Falcon di CrowdStrike ha permesso a Gruppo Credem di unire in un'unica soluzione l'EDR con ciò che un tempo veniva definito "antivirus". Il primo beneficio immediato di questa convergenza tecnologica è stato di natura operativa: l'azienda non deve più aggiornare periodicamente un sistema di protezione separato e semplifica notevolmente la gestione dell'endpoint detection and response.

Avere un unico sensore leggero si è tradotto in una maggiore efficienza complessiva, derivante dall'ampia visibilità e dalla correlazione di eventi provenienti da fonti differenti all'interno di un'unica interfaccia. In precedenza, infatti, il Security Operation Center (SOC) aveva l'onere di svolgere queste attività di correlazione senza automatismi, un approccio che esponeva gli operatori al rischio di sbagliare l'analisi a causa del "rumore di fondo" generato durante la concitazione di un potenziale attacco.

Delegando questo compito alla piattaforma, Gruppo Credem ha ottenuto una drastica accelerazione nell'identificazione dei problemi, passando da tempistiche di analisi di interi giorni a pochi minuti, a seconda dell'evento posto sotto la lente. A questa rapidità d'azione, si aggiunge la vitale capacità di contenimento: nel momento in cui individua una minaccia, Falcon permette di isolare immediatamente la macchina colpita. Questo evita che l'infezione si propaghi all'intero ecosistema con effetti potenzialmente devastanti per il business, garantendo di fatto quella resilienza operativa oggi fortemente richiesta da normative come NIS2 e DORA.

Naturalmente, per mantenere questa efficienza a livelli ottimali, è essenziale mitigare il volume degli alert. Tenuto conto che l'evoluzione delle tecniche di cui si servono le nuove campagne malware è costantemente in divenire, qualsiasi sistema richiede un tuning continuo. Grazie a questo costante lavoro di affinamento, la piattaforma ha registrato una notevole riduzione dei falsi positivi, con risultati concreti e quantificabili: su una proiezione annuale di 4.525 eventi potenzialmente malevoli rilevati, Falcon è intervenuta in maniera proattiva su soli 149 eventi conclamati. Questo si traduce nell'attivazione automatica dell'EDR su circa un evento critico ogni due giorni, sventando la minaccia in modo silente prima ancora che potesse trasformarsi in un vero e proprio incidente informatico.

Infine, la protezione offerta da CrowdStrike non si limita alle sole minacce esterne, ma si focalizza su un'ulteriore priorità vitale per il comparto bancario: l'abbattimento del rischio di data breach. «Falcon Device Control ci aiuta ad avere un controllo pieno dei dati in transito da e per i sistemi di archiviazione di massa, siano essi storage portatili, chiavette USB o qualsiasi tipo di altra periferica - sottolinea Puccioni -. Inoltre, si presta all'implementazione di policy che garantiscono di "marcare stretto" il dato aziendale onde evitare violazioni della privacy e dei dati sensibili».

© 2026 CROWDSTRIKE, INC.

Le sfide future di Gruppo Credem

Quanto vale la sicurezza in generale e per un gruppo bancario in particolare? È vero, la sicurezza non genera business dal punto di vista del ROI. Però è anche vero che proteggere il business è garanzia certa di risparmio dai contenziosi che dovessero derivare a causa di data breach o incidenti che coinvolgono partner o clienti.

Grazie alla piattaforma Falcon gli eventi malevoli potenziali sono stati individuati e bloccati in maniera proattiva prima che diventassero conclamati.

> **Siamo molto soddisfatti della collaborazione con CrowdStrike. Non solo della loro soluzione, ma anche dell'azienda che sta dietro alla soluzione sia in termini di assistenza sia di capacità tempestiva di remediation.**

Francesco Puccioni
Head of Cybersecurity Operations

Oggi, in un ecosistema sempre più ampio, occorre anche rafforzare i controlli a livello di cloud workload security, container security e SaaS security e messa in sicurezza dell'Infrastructure as Code (IaC). «In questi ambiti - conclude Francesco Puccioni - abbiamo già delle soluzioni di cybersecurity, ma poiché la preoccupazione non è mai troppa, vogliamo investire in attività progettuali e in tecnologia che ci permettano di ampliare il set di controlli. Siamo certi che, anche in questa circostanza, un partner come CrowdStrike porterà grande valore».

CROWDSTRIKE SOLUTIONS

Falcon platform

© 2026 CROWDSTRIKE, INC.

Informazioni su CrowdStrike

CrowdStrike (Nasdaq: CRWD), leader globale della cybersecurity, ha ridefinito la sicurezza moderna con la piattaforma cloud-native più avanzata al mondo per proteggere le aree critiche del rischio aziendale: endpoint e cloud workload, identità e dati.

Alimentata dal CrowdStrike Security Cloud e da AI di classe mondiale, la piattaforma CrowdStrike Falcon® sfrutta indicatori di attacco in tempo reale, threat intelligence, tattiche degli avversari in evoluzione e telemetria arricchita proveniente da tutta l'azienda per fornire rilevamenti iper-accurati, protezione e remediation automatizzate, threat hunting d'élite e osservabilità prioritizzata delle vulnerabilità.

Progettata appositamente nel cloud con un'architettura a singolo agente leggero, la piattaforma Falcon offre deployment rapido e scalabile, protezione e prestazioni superiori, ridotta complessità e time-to-value immediato.

CrowdStrike: Fermiamo le violazioni.

Per saperne di più : www.crowdstrike.com

Seguici: Blog | X | LinkedIn | Facebook | Instagram

© 2026 CrowdStrike, Inc. Tutti i diritti riservati. CrowdStrike, il logo del falco, CrowdStrike Falcon® e CrowdStrike Threat Graph sono marchi di proprietà di CrowdStrike, Inc. e registrati presso l'United States Patent and Trademark Office e in altri paesi. CrowdStrike possiede altri marchi commerciali e marchi di servizio e può utilizzare i marchi di terze parti per identificare i loro prodotti e servizi.

Inizia oggi la tua prova gratuita.

PROVA GRATIS ›