UN PASSO AVANTI RISPETTO ALLE MENTI CRIMINALI

F-Secure Rapid Detection & Response

F-Secure

PROTEGGI IL BUSINESS E I SUOI DATI DAGLI ATTACCHI AVANZATI

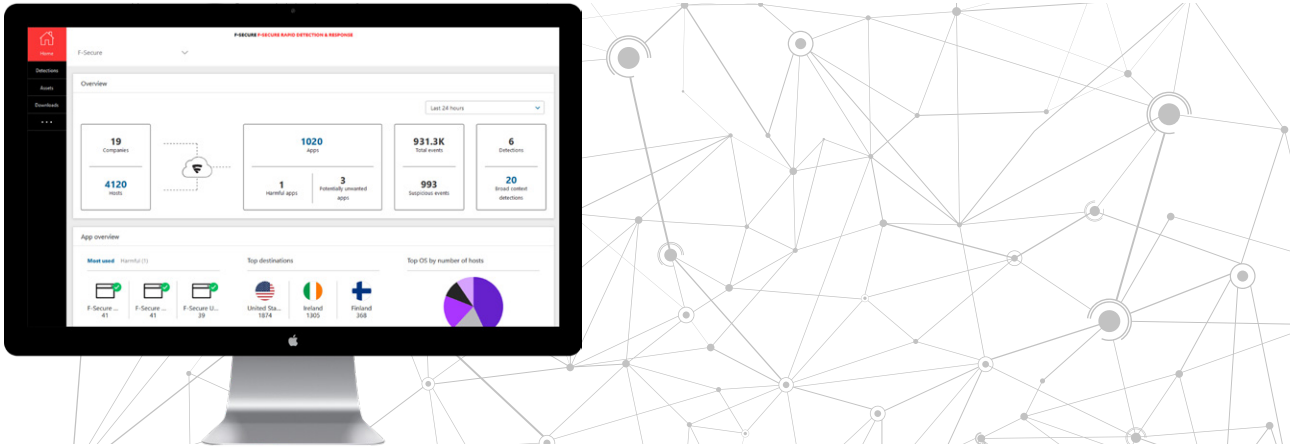
La prevenzione efficace delle minacce prima che provochino danni è il fulcro della cyber security, ma non si può fare affidamento unicamente sulle misure preventive per tenere al sicuro il business e i suoi dati dalle tattiche, tecniche e procedure (TTP) utilizzate negli attacchi mirati.

La rapida evoluzione del panorama delle minacce e dei requisiti normativi, ad esempio il GDPR, impone che le aziende siano preparate a rilevare le violazioni dopo una compromissione e investano in strategie di risposta rapida agli attacchi avanzati.

La soluzione F-Secure Rapid Detection & Response, creata da un team di esperti nella ricerca delle minacce, consente al tuo team IT o a un service provider certificato di proteggere la tua organizzazione dalle minacce avanzate. Con il supporto degli esperti di cyber security di F-Secure, i tuoi specialisti IT saranno in grado di rispondere agli incidenti in modo rapido ed efficace. Se invece affidi a un service provider la gestione delle attività di rilevamento e risposta per la tua azienda, potrai focalizzare l'attenzione sul core business e contare sulla guida degli esperti in caso di attacco.

PRIMA DELLA COMPROMISSIONE

DOPO LA COMPROMISSIONE



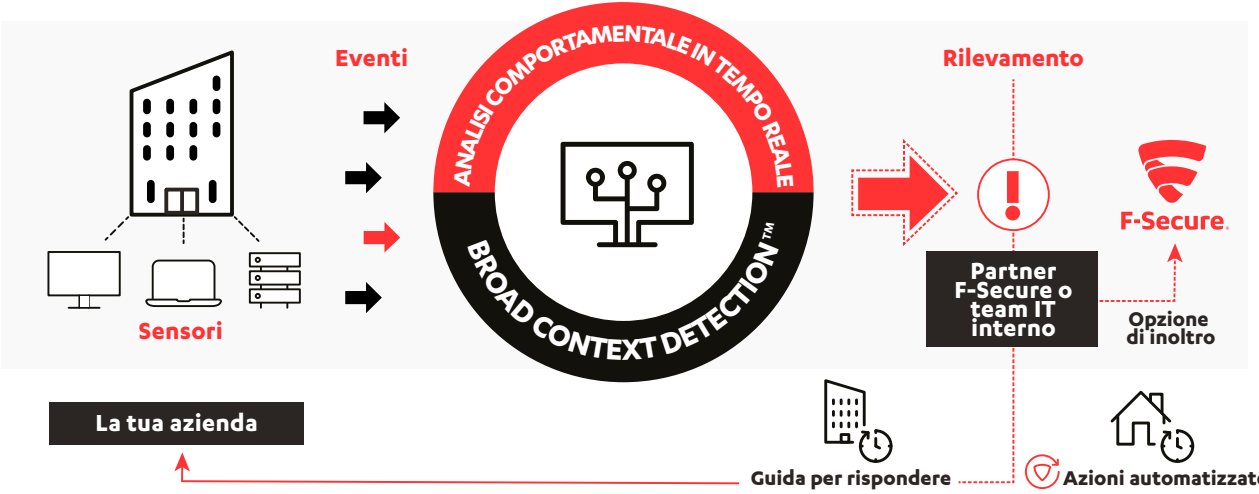
FERMA RAPIDAMENTE GLI ATTACCHI MIRATI CON LA GUIDA DEGLI ESPERTI

Per contrastare le cyber minacce avanzate ti serve il meglio della tecnologia e dell'esperienza umana.

La soluzione di Endpoint Detection & Response (EDR) di F-Secure ti offre visibilità contestuale sulle minacce avanzate, permettendoti di rilevare e rispondere agli attacchi mirati con l'automazione e la guida degli esperti.

Quando si verifica una violazione, un semplice avviso non basta. Per pianificare la miglior risposta possibile occorre comprendere tutte le specifiche dell'attacco. I nostri meccanismi Broad Context Detection™, insieme a fornitori di servizi certificati e all'automazione integrata, fermeranno rapidamente l'attacco e ti offriranno consigli utili su altre azioni correttive.

COME FUNZIONA



La tecnologia di F-Secure al tuo servizio

1. I sensori monitorano gli eventi comportamentali generati dagli utenti e li inviano nel nostro cloud in tempo reale.

2. L'analisi comportamentale in tempo reale e i meccanismi Broad Context Detection™ riducono il volume dei dati, distinguendo i modelli di comportamento malevoli da quelli normali degli utenti, per identificare rapidamente gli attacchi reali.

3. Gli avvisi con ampie informazioni di contesto e descrizioni sull'attacco consentono di confermare un rilevamento in modo più facile, sia da parte di un Partner F-Secure che da parte del team IT aziendale, con possibilità di inoltrare le indagini più complesse a F-Secure.

4. Una volta confermato un rilevamento, il servizio propone i passaggi necessari per contrastare e correggere la minaccia.

COME FUNZIONA

CERCARE UN AGO IN UN PAGLIAIO – UN ESEMPIO CONCRETO

Rilevare le minacce avanzate individuando i piccoli eventi singoli che gli attaccanti mettono in atto è come cercare un ago in un pagliaio.

In un'installazione presso un cliente con 325 nodi, i nostri sensori hanno raccolto circa 500 milioni di eventi nell'arco di un mese. L'analisi dei dati grezzi nei nostri sistemi back end ha ridotto quel numero a 225.000 eventi.

Gli eventi sospetti sono stati ulteriormente analizzati dai nostri meccanismi Broad Context Detection™ per restringere il numero di rilevamenti ad appena 24. Infine, quei 24 rilevamenti sono stati esaminati in dettaglio e solo 7 di essi sono risultati essere minacce reali.

Permettendo ai team IT e di sicurezza di focalizzare l'attenzione su meno ma più accurati rilevamenti è possibile mettere in atto risposte più rapide ed efficaci in caso di un cyber attacco reale.

500 MILIONI
EVENTI AL MESE
raccolti da 325 sensori endpoint

225 000
EVENTI SOSPETTI
dopo l'analisi comportamentale in tempo reale degli eventi

24
RILEVAMENTI
dopo la contestualizzazione degli eventi sospetti

7
MINACCE REALI
dopo la conferma dei rilevamenti come minacce reali

VANTAGGI

VISIBILITÀ

Ottieni visibilità immediata sullo stato della sicurezza e dell'ambiente IT

- Migliora la visibilità sullo stato della sicurezza e dell'ambiente IT grazie all'inventario delle applicazioni e degli endpoint
- Identifica le attività sospette raccogliendo e correlando gli eventi comportamentali oltre il malware commodity
- Fornisce avvisi con ampie informazioni di contesto e criticità degli asset, semplificando la risposta agli incidenti

RILEVAMENTO

Proteggi il tuo business e i suoi dati sensibili rilevando rapidamente le violazioni

- Rileva e ferma rapidamente gli attacchi mirati per minimizzare le interruzioni di attività e l'impatto negativo sul brand
- Configura il servizio entro poche ore, per essere immediatamente pronto in caso di violazione
- Rispetta i requisiti normativi di PCI, HIPAA e GDPR che prevedono la notifica delle violazioni entro 72 ore

RISPOSTA

Rispondi rapidamente con la guida degli esperti se sei sotto attacco

- Automazione e intelligence incorporate aiutano il tuo team a concentrarsi solo sugli attacchi reali
- Gli avvisi includono una guida per la risposta adeguata, con possibilità di automatizzare le azioni di risposta su base continuativa
- Colma le lacune di competenze o risorse rispondendo agli attacchi con un fornitore di servizi certificato supportato da F-Secure

CARATTERISTICHE

Sensori endpoint

Strumenti di monitoraggio leggeri e discreti, progettati per funzionare con qualsiasi soluzione di protezione degli endpoint

- Sensori leggeri vengono implementati in tutti i computer rilevanti nell'organizzazione
- Infrastruttura di gestione a client singolo con le soluzioni F-Secure per la sicurezza degli endpoint
- I sensori raccolgono i dati comportamentali dai dispositivi endpoint senza compromettere la privacy degli utenti

Broad Context Detection™

La tecnologia di rilevamento proprietaria di F-Secure consente di comprendere facilmente l'ambito di un attacco mirato

- Analisi comportamentale, reputazionale e dei Big Data in tempo reale con machine learning
- Contestualizzazione automatica dei rilevamenti, con visualizzazione su una linea temporale
- Include i livelli di rischio, la criticità degli host interessati e il panorama delle minacce prevalente

Visibilità delle applicazioni

Acquisire visibilità sullo stato della sicurezza e dell'ambiente IT non è mai stato così facile

- Identifica tutte le applicazioni dannose o altrimenti indesiderate e le destinazioni esterne di vari servizi cloud
- Sfrutta i dati reputazionali di F-Secure per identificare le applicazioni potenzialmente dannose
- Limita le applicazioni potenzialmente dannose e i servizi cloud ancora prima che si verifichi una violazione dei dati

Guida degli esperti

Ti prepara ad affrontare i cyber attacchi più avanzati con le risorse di cui disponi

- Guida passo passo integrata per la risposta e azioni da remoto per fermare gli attacchi
- Guida e supporto di service provider certificati per le azioni di risposta
- Eccezionale funzionalità di inoltro a F-Secure per l'analisi delle minacce e servizio di guida da parte di esperti

Risposta automatizzata

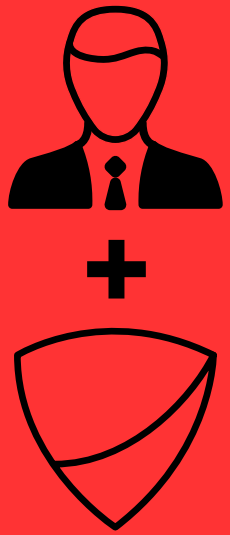
Riduzione dell'impatto dei cyber attacchi mirati automatizzando le azioni di risposta 24 ore su 24

- Azioni di risposta automatizzate in base a criticità, livello di rischio e pianificazioni predefinite
- I livelli di rischio e di criticità forniti dal servizio consentono di definire le priorità per le azioni di risposta
- Contenimento rapido degli attacchi anche se il team interno è disponibile solo negli orari lavorativi

PER VEDERE IL VIDEO VAI SU

www.f-secure.com/RDR

INFORMAZIONI SU F-SECURE



www.f-secure.com
www.twitter.com/fsecure_it
www.facebook.com/f-secure

UN PASSO AVANTI RISPETTO ALLE MENTI CRIMINALI

Come si rileva un attacco sofisticato? Con le tecnologie più avanzate di analisi e machine learning. Ma non basta. Bisogna pensare come un attaccante.

Gli esperti di sicurezza di F-Secure hanno partecipato a più indagini su crimini informatici in Europa di qualunque altra società. Con i nostri esperti sempre al corrente di ciò che accade nel panorama dei cyber attacchi potrai avvalerti della threat intelligence più recente.

Nessuno conosce la cyber security come F-Secure. Per tre decenni, F-Secure ha guidato l'innovazione nella cyber security, difendendo decine di migliaia di aziende e milioni di persone. Con un'esperienza insuperabile nella protezione degli endpoint, così come nel rilevamento e risposta, F-Secure difende aziende e privati da attacchi informatici avanzati, violazioni di dati e dalle diffuse infezioni ransomware. La sofisticata tecnologia di F-Secure combina la forza del machine learning con l'esperienza umana degli esperti presenti nei suoi rinomati laboratori di sicurezza con un approccio singolare chiamato Live Security. Gli esperti di sicurezza di F-Secure hanno partecipato a più investigazioni sul cyber crime in Europa di qualsiasi altra azienda sul mercato e i suoi prodotti sono venduti in tutto il mondo attraverso oltre 200 operatori di banda larga e telefonia mobile e migliaia di rivenditori. Fondata nel 1988, F-Secure è quotata al NASDAQ OMX Helsinki Ltd.

F-Secure