PERCHÉ TI SERVE L'EDR

Guida per le piccole e medie imprese

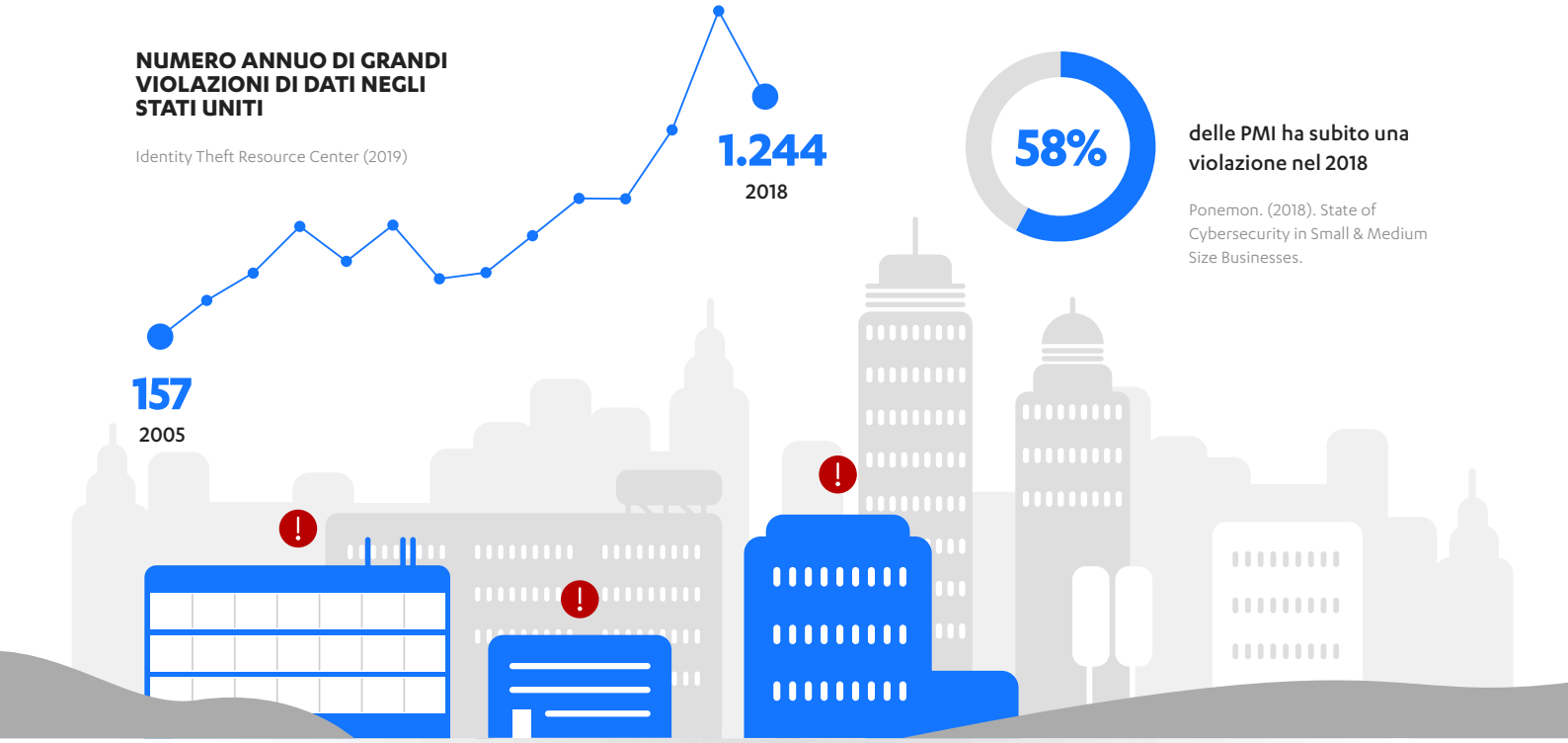
F-Secure

SOMMARIO

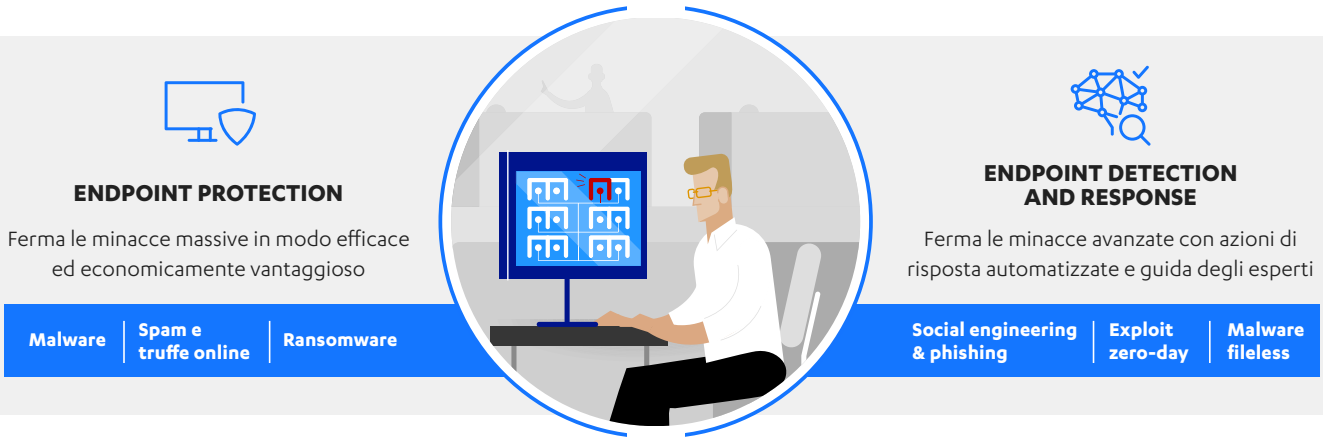
PERCHÉ TI SERVE UNA SOLUZIONE EDR

Nella tua rete è presente un attaccante in questo momento?
Nonostante l'incremento degli investimenti nella cyber security, la maggior parte dei leader IT non riesce ancora a dare una risposta definitiva a questa domanda. Ci sono tantissimi aspetti da tenere sotto controllo, come utenti, dispositivi, applicazioni, avvisi, vulnerabilità, patch e non solo. I team IT, soprattutto quelli delle aziende più piccole, non hanno il tempo di monitorare le reti 24/7.
A oggi, quasi due terzi delle organizzazioni globali hanno subito una violazione[1] e il 56% di queste violazioni viene rilevato a distanza di mesi o più[2]. E più a lungo una violazione rimane inosservata, più costosa diventa; il costo della risposta, infatti, aumenta rapidamente, addirittura nell'ordine di migliaia di euro ogni giorno.
Questi attacchi prendono di mira anche le piccole imprese. Nel 2018 circa il 58% delle PMI ha subito una violazione[3]. Per queste imprese le conseguenze sono ancora più gravi: secondo le stime della National Cyber Security Alliance, il 60% delle PMI è costretto a chiudere i battenti nei sei mesi successivi a un incidente[4].
La situazione sembra desolante, con gli attaccanti che bypassano in ogni modo le difese delle organizzazioni. Cosa può fare un leader IT, che ha risorse limitate, ma responsabilità infinite?

Qui entra in gioco la tecnologia **EDR** (**Endpoint Detection and Response**). Le soluzioni EDR sono pensate per incrementare **la protezione degli endpoint** (anti-malware aziendale, filtro antispam e simili) con funzionalità di rilevamento e risposta più efficaci.
Se paragoniamo la protezione degli endpoint a una recinzione, il sistema EDR potrebbe essere il team di sicurezza che la sorveglia costantemente, sempre in guardia per identificare eventuali tentativi di intrusione. È il livello di sicurezza successivo quando le difese preventive non riescono a intercettare un attacco avanzato o quando in uno dei dispositivi manca una patch importante. Anche se un attaccante riesce a entrare, non tutto è perduto, puoi comunque rilevare e bloccare la minaccia.
L'EDR sta diventando sempre più importante nella lotta contro i cyber attacchi, ma molti professionisti IT hanno difficoltà a quantificarne i benefici per la loro azienda. Per aiutarti, abbiamo creato questa guida, che ti spiega come funziona l'EDR, perché è necessario per rilevare gli attacchi e come utilizzarlo per migliorare il profilo di sicurezza complessivo della tua organizzazione. Abbiamo incluso anche alcune informazioni utili sulla valutazione dei vendor di soluzioni EDR, con riferimenti ai dati di test indipendenti.



COME FUNZIONA L'EDR



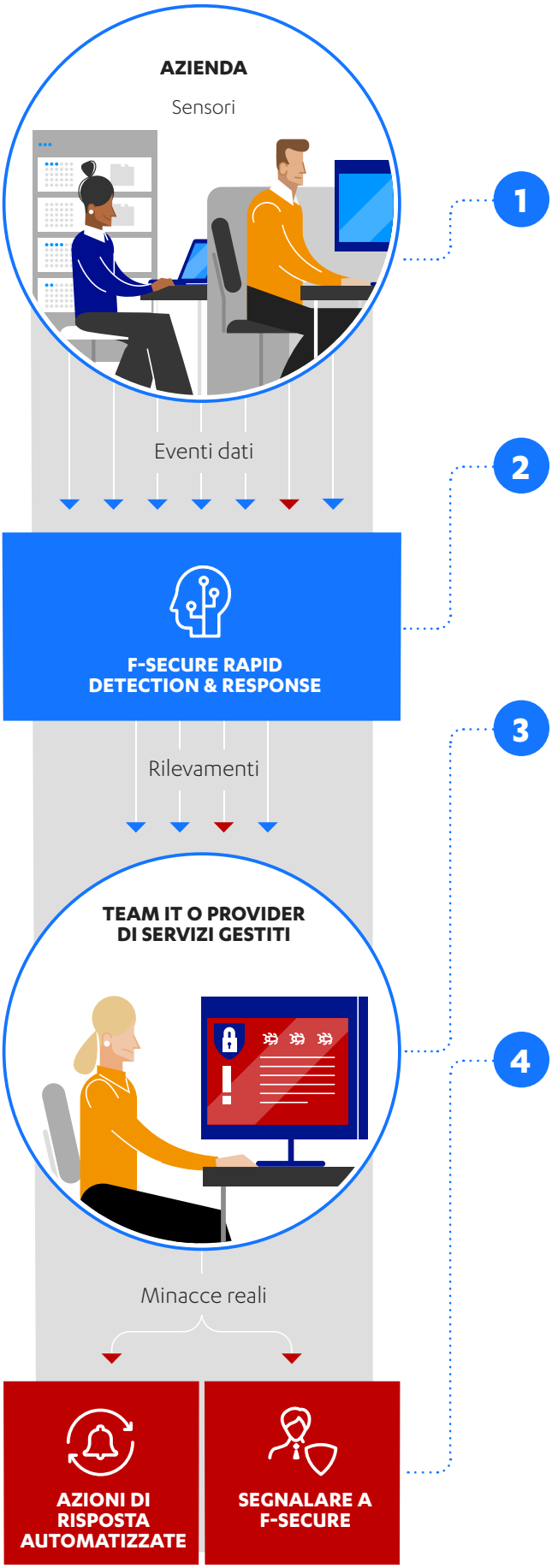
L'EDR raccoglie un numero enorme di eventi comportamentali relativi ai dati (come esecuzioni di processi, connessioni di rete e operazioni sui file) dalle workstation e dai server dell'organizzazione attraverso sensori endpoint leggeri. Questi dati sono estremamente preziosi per il rilevamento degli attacchi ma, se sono troppi, diventano impossibili da gestire per gli analisti umani. Ritrovarsi con milioni o miliardi di informazioni, tra le quali si annidano solo alcune minacce reali, è davvero come cercare un ago nel pagliaio.
Utilizzando strumenti di analisi avanzata con il supporto del machine learning, l'EDR è in grado di analizzare questi dati e intercettare gli indicatori di attacco cui corrispondono minacce sia note che nuove. A questo scopo, confronta il comportamento accettabile degli utenti con i dati raccolti e identifica le azioni anomale.
Ecco alcuni esempi concreti di ciò che l'EDR può fare:

- Rilevare attacchi malware fileless distribuiti da siti web che contengono codice malevolo, documenti PDF caricati sui browser o macro incorporate in file di MS Office
- Identificare altri processi insoliti avviati dalle workstation aziendali
- Rilevare nuovi tipi di malware nell'ambiente, anche senza firme esistenti.
- Individuare i dipendenti che utilizzano applicazioni sconosciute o dannose.
- Isolare dalla rete i computer e i server compromessi, per evitare che un cyber attacco si diffonda ulteriormente.

Anziché segnalare una miriade di falsi positivi, l'EDR è in grado di evidenziare solo i risultati rilevanti, in modo rapido e preciso. Nel caso di un particolare cliente, la soluzione F-Secure ha rilevato un totale di 2 miliardi di eventi correlati agli endpoint in un mese e ha individuato i 15 incidenti che rappresentavano minacce effettive. Una volta identificate le minacce, l'EDR ti aiuta anche a eseguire ulteriori indagini e a rispondere con azioni automatizzate e raccomandazioni. Questo è un aspetto importantissimo per le piccole imprese, che solitamente non dispongono delle risorse e delle competenze necessarie per gestire autonomamente i cyber incidenti di un certo rilievo. Con una soluzione EDR come F-Secure Rapid Detection & Response, non solo puoi scoprire se ci sono problemi sulla tua rete IT, ma ottieni anche un aiuto concreto per risolverli.

ESEMPIO

Un laptop appartenente a un dipendente junior del reparto marketing sta caricando dati su un server sconosciuto su Internet. L'EDR rileva questo comportamento in pochi minuti, isola automaticamente il computer dal resto della rete e avvisa il team IT perché indaghi. Con l'aiuto dell'EDR, il team stabilisce rapidamente che si tratta effettivamente di un attacco (il computer del dipendente è stato compromesso) e ne ricerca l'origine. Scopre che tutto è partito da un processo che è stato avviato da un allegato email malevolo. Il team IT corregge il problema sul dispositivo compromesso, aggiorna le impostazioni della soluzione antispam per evitare che i dipendenti ricevano di nuovo lo stesso allegato pericoloso in futuro, modifica le regole del firewall in modo da bloccare le connessioni al dominio interessato e informa gli utenti del rischio a cui è esposta l'organizzazione.
In questa situazione di esempio non è stato trovato un malware tradizionale e non c'era nulla che la piattaforma di protezione degli endpoint dovesse prevenire. Senza l'EDR, l'azienda avrebbe lottato contro un nemico invisibile.



Questo è il processo alla base della nostra soluzione EDR, F-Secure Rapid Detection & Response:

I sensori installati nei computer Windows, nei computer Mac e nei server monitorano il comportamento degli utenti all'interno dell'organizzazione. Gli eventi dati raccolti vengono inviati al nostro database in cloud per l'analisi in tempo reale. I sensori sono invisibili agli utenti finali e il team IT non deve svolgere altre operazioni per monitorare l'ambiente IT.

Il nostro backend in cloud esamina i dati raccolti, distinguendo gli eventi sospetti dalle normali attività degli utenti. Questo avviene con l'analisi comportamentale, reputazionale e dei Big Data in tempo reale, in associazione al machine learning. L'analisi è completamente autonoma e non richiede l'intervento del team IT.

Sulla dashboard viene visualizzato un elenco filtrato di avvisi, con una grafica chiara e informazioni sugli attacchi. Puoi vedere facilmente tutti gli host interessati e gli eventi correlati su una linea temporale. Gli avvisi vengono anche contestualizzati, tenendo conto dell'importanza degli host coinvolti, del panorama delle minacce e dei livelli di rischio attuali. Avendo a disposizione tutte queste informazioni, saprai esattamente dove focalizzare subito l'attenzione.

Le minacce reali vengono isolate dalla rete. A questo punto hai due possibilità:

a) Puoi esaminare il problema e rispondere mediante il team IT aziendale, utilizzando le azioni di risposta automatizzate e le indicazioni fornite dalla soluzione. Se la sicurezza è affidata a uno dei nostri provider di servizi certificati, saranno loro a eseguire le azioni necessarie per conto della tua azienda.

b) Puoi inoltrare il problema agli esperti di F-Secure in materia di risposta agli incidenti grazie alla funzionalità integrata "Segnalare a F-Secure". Essi eseguiranno un'indagine approfondita sulla minaccia e consiglieranno le misure appropriate per correggerla, prima che possa danneggiare il business.

COME FUNZIONANO GLI ATTACCHI AVANZATI

Per capire in che modo l'EDR può proteggere l'organizzazione dalle minacce mirate e avanzate, dobbiamo esaminare il modus operandi consueto degli attaccanti. Chi intende violare i livelli di sicurezza preventiva di un'azienda, di solito inizia utilizzando una di queste tattiche:

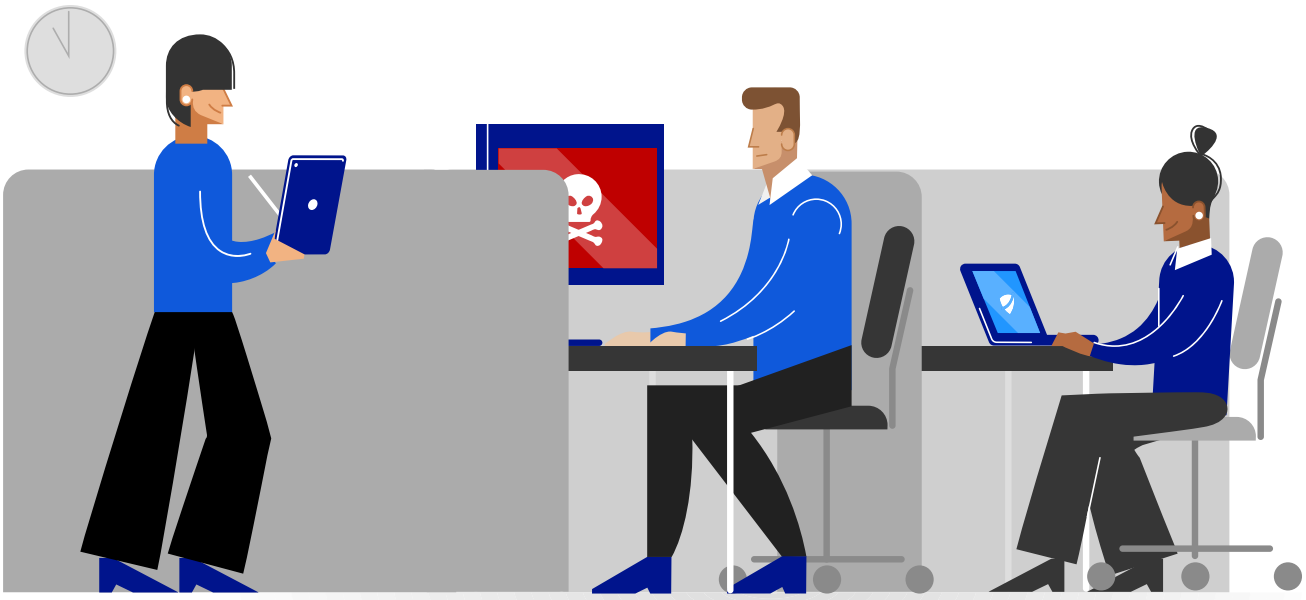
1. **Sfruttamento di una vulnerabilità:** i punti deboli della sicurezza nei sistemi esposti al pubblico sono un'attraente via di attacco. Il 57% delle violazioni deriva da vulnerabilità note che avrebbero potuto essere corrette[5]. In una situazione in cui ogni anno emergono più di 16.000 nuove vulnerabilità, la maggior parte delle aziende fatica a tenere aggiornata l'intera l'infrastruttura[6]. Grazie ai moderni strumenti di automazione, gli attaccanti opportunisti sono in grado di scansionare la rete pubblica alla ricerca di una qualsiasi di queste vulnerabilità comuni, trovando migliaia di dispositivi privi delle patch necessarie.

2. **Spear Phishing:** comunicazioni ingannevoli mirate progettate per indurre qualcuno nell'organizzazione a condividere informazioni sensibili o ad aprire un file eseguibile. Gli attacchi di tipo spear phishing sono estremamente comuni ed estremamente efficaci: nel rapporto annuale sulle minacce di Verizon si stima che il 32% delle violazioni comporti questa tattica [2].

3. **Watering Hole:** gli attaccanti cercano eventuali vulnerabilità nei siti Web abitualmente utilizzati dai dipendenti. Poi inseriscono codice malevolo nella base JavaScript o HTML di questi siti, che indirizza gli utenti bersaglio verso un altro sito compromesso in cui è in agguato un malware. Quando qualcuno nell'organizzazione usa il sito Web comune e popolare, scatta la trappola.

4. **Man-in-the-Middle:** l'attaccante intercetta le tue comunicazioni e le inoltra solo dopo averle esaminate o addirittura modificate, dando l'impressione che l'interlocutore sia un soggetto attendibile. Gli attacchi di tipo man-in-the-middle vengono compiuti in prossimità tramite reti Wi-Fi non crittografate o da remoto tramite malware.

5. **Buying Access:** le organizzazioni criminali commissionano così tanti attacchi in crowdsourcing ai danni di così tanti sistemi, che, prima o poi, una certa percentuale di questi sistemi verrà inevitabilmente compromessa. In molti casi, gli attaccanti possono risparmiare tempo e fatica semplicemente acquistando l'accesso a un'azienda già compromessa. La tua azienda è stata violata in passato? Se è così, l'accesso ai tuoi sistemi potrebbe essere in vendita per pochi spiccioli.



Quando un attaccante riesce a superare il perimetro, per prima cosa inizia ad aggirarsi nel sistema, armato delle peggiori intenzioni. Potrebbe aggiungere nuovi utenti locali o modificare gli account utente esistenti per elevarne i privilegi, cercare le password dell'amministratore di dominio con uno strumento di memory-scraping o spostarsi lateralmente da un sistema all'altro alla ricerca di qualcosa di interessante.

Ovviamente l'obiettivo è non farsi scoprire, quindi gli aggressori esperti di solito usano componenti legittimi del sistema operativo per radicarsi stabilmente nella rete aziendale e nascondersi nel traffico normale. I firewall e i prodotti tradizionali per la protezione degli endpoint non sono in grado di rilevare la presenza di un attaccante a questo punto del processo.

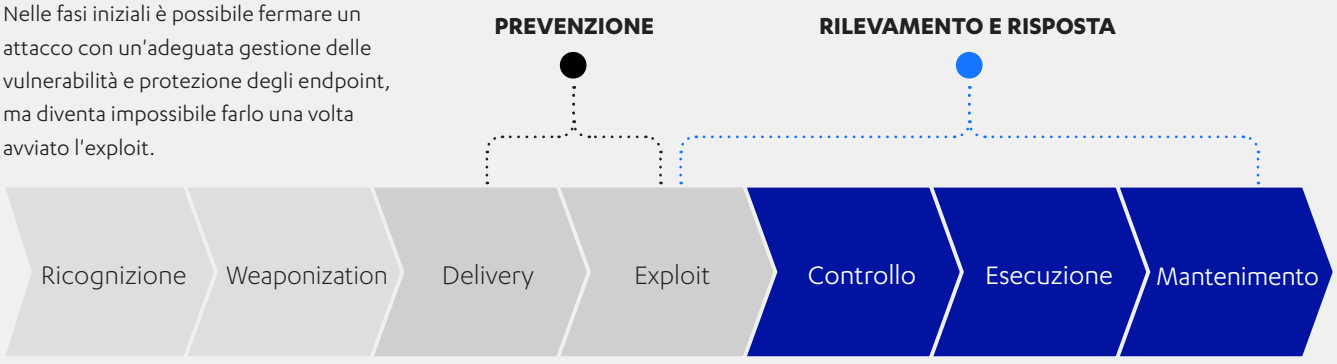
Infine, l'attaccante utilizzerà gli strumenti di amministrazione IT dell'azienda stessa, sfruttando PowerShell, Service Commands o Windows Remote Management per mettere le mani su ciò che gli interessa, come i dati dei clienti o la proprietà intellettuale. Quando l'attaccante sottrae i dati, il processo viene camuffato abilmente in modo da farlo sembrare il comportamento di un utente normale e da non destare allarmi. Ora i tuoi beni più preziosi sono sul mercato nero, a disposizione del miglior offerente.

Gli attacchi sofisticati come questo, da cui nessuna organizzazione può considerarsi immune, non possono essere fermati solamente con metodi di difesa statici. Proprio per questo, gli obiettivi privilegiati della maggior parte dei cyber criminali sono le piccole e medie imprese, che di solito hanno meno difese e un numero inferiore di addetti alla sicurezza IT rispetto alle grandi aziende. Inoltre, le PMI spesso fanno parte della catena di approvvigionamento delle grandi aziende e rappresentano quindi una via di attacco praticabile quando l'intento è violare queste società con metodi di spear phishing o di altro tipo.

Con l'EDR, mandi completamente in frantumi questo piano. Anche se un attaccante dovesse riuscire a superare le tue misure di sicurezza preventiva, non gli sarebbe facile nascondersi nel normale traffico di rete. Qualsiasi comportamento insolito viene rilevato prima che l'azienda venga danneggiata. In molti casi, il solo fatto di eseguire una soluzione EDR costituisce un forte deterrente contro i cyber criminali opportunistici.

CICLO DI VITA DI UN CYBER ATTACCO

Il "ciclo di vita di un cyber attacco" è una versione semplificata della sequenza di passaggi eseguiti per violare una rete. Nelle fasi iniziali è possibile fermare un attacco con un'adeguata gestione delle vulnerabilità e protezione degli endpoint, ma diventa impossibile farlo una volta avviato l'exploit.



QUALI SONO I VANTAGGI DELL'EDR PER I LEADER IT

L'EDR assicura molti vantaggi ai responsabili della cyber security aziendale:

1. **Se ti chiedono informazioni sullo stato della sicurezza, potrai fornire una risposta chiara, sicura e accurata:** la cyber security non è più un argomento IT di nicchia, ma è diventata un problema di gestione del rischio a tutto campo. Sempre più spesso ai manager IT viene chiesto di segnalare lo stato della sicurezza ai vertici aziendali, compreso il consiglio di amministrazione. Quando ti viene posta l'inevitabile domanda "Qual è il nostro livello di sicurezza in questo momento?", l'EDR ti consente di rispondere in modo esaustivo e sincero. Con il supporto dei dati provenienti dalle piattaforme di gestione delle vulnerabilità e di protezione degli endpoint, potrai spiegare chiaramente qual è il grado di protezione, quali tipi di attacchi sono stati riscontrati nei sistemi, se i dipendenti stanno seguendo le linee guida per la sicurezza IT e così via.

2. **Puoi contare sul fatto che qualsiasi tentativo di attacco sarà rilevato e segnalato rapidamente, senza spendere l'intero budget IT per la sicurezza:** come abbiamo già detto innumerevoli volte in questa guida, la sola prevenzione degli attacchi non è più sufficiente. Ma sviluppare capacità di rilevamento e risposta efficaci non è facile, né economico, quando si deve partire da zero. Una soluzione EDR chiavi in mano è un'ottima scelta per le piccole e medie imprese, in quanto offre tutte le funzionalità principali di rilevamento e risposta a un costo non paragonabile a quello dei servizi completamente gestiti. Infatti, alcune soluzioni come F-Secure Rapid Detection & Response consentono anche di accedere ai professionisti della sicurezza solitamente riservati alle soluzioni premium. Con la funzionalità **Segnalare a F-Secure**, i rilevamenti di minacce più gravi o complesse possono essere inoltrati direttamente agli esperti del nostro centro specializzato nella risposta agli incidenti, le stesse persone che gestiscono quotidianamente la cyber security dei clienti enterprise.

3. **Quando viene rilevata una minaccia, sarai in grado di rispondere e porvi rimedio in modo molto più rapido**: oltre ai rilevamenti, l'EDR offre anche strumenti e consigli pratici per affrontare diversi problemi di sicurezza. Isolamento degli host, comunicazione diretta con gli utenti, azioni di risposta da remoto... la soluzione EDR ti propone il modo migliore per risolvere un determinato incidente di sicurezza nel più breve tempo possibile. Anche se l'obiettivo resta comunque quello di prevenire un attacco, questi strumenti si rivelano preziosi nel momento in cui bisogna affrontare una minaccia attiva.

4. **Se si verifica una violazione, sarai in grado di vedere e capire esattamente cosa è successo, per evitare che si ripeta in futuro:** rilevare e fermare un attacco è fondamentale, ma è altrettanto importante capire come è avvenuto. Per migliorare significativamente il profilo di sicurezza dell'azienda, è necessario procedere a ritroso e identificare i metodi che sono riusciti a eludere le difese aziendali. Attraverso la raccolta di tutti i dati forensi rilevanti, l'EDR consente di analizzare come è stato eseguito un attacco, di trarne un insegnamento e di rafforzare la sicurezza contro eventuali tentativi simili in futuro. È anche importante raccogliere i dati relativi ai tentativi di attacco non riusciti poiché da questi può emergere che l'azienda è nel mirino di un cyber criminale persistente.

5. **Il Regolamento generale sulla protezione dei dati (GDPR) prevede l'obbligo di notificare le violazioni dei dati entro 72 ore. Anziché preoccuparti dell'adeguamento, saprai con certezza che la tua azienda è conforme ai requisiti:** sono già state comminate le prime sanzioni previste dal GDPR alle aziende che hanno subito una violazione dopo l'entrata in vigore del regolamento. L'EDR ti aiuta a rispettare il GDPR su due fronti: in primo luogo, potrai dimostrare alle autorità di avere adottato le misure basilari per proteggere l'ambiente IT. In secondo luogo, qualora un attaccante riuscisse a penetrare la tua linea difensiva, puoi raccogliere informazioni sufficienti per segnalarlo alle autorità entro la scadenza delle 72 ore.

COME VALUTARE I VENDOR

Finora abbiamo cercato di illustrare nel modo più chiaro possibile quali sono i principi generali di funzionamento e i benefici dell'EDR. Ma come si fa a sapere qual è la soluzione giusta per la tua organizzazione?
Per valutare i diversi fornitori di EDR, il campo è molto più sgombro rispetto all'AV tradizionale. La regola d'oro la fornisce un programma sviluppato dall'organizzazione no profit statunitense MITRE, che esamina le soluzioni EDR a fronte del framework "ATT&CK" messo a punto dall'organizzazione stessa, un set di tattiche, tecniche e procedure utilizzate dai cyber criminali, costantemente aggiornato. Offre risultati imparziali per valutare le performance dei vari vendor di soluzioni EDR, con approfondimenti sui tipi di telemetrie, avvisi, interfacce e output che puoi aspettarti da ognuno di essi. Le valutazioni di MITRE sono molto utilizzate da varie autorità del settore, come ad esempio Gartner e Forrester.
Le funzionalità di rilevamento dell'EDR di F-Secure sono state testate da MITRE nell'estate del 2019.

Abbiamo ottenuto risultati eccellenti che dimostrano che F-Secure è in grado di rilevare anche gli attacchi nation-state più sofisticati. La valutazione MITRE non è un'analisi competitiva e non vengono assegnati punteggi ai vari fornitori. Forrester, tuttavia, ha pubblicato uno script di valutazione che conta e valuta i risultati allo scopo di misurare le performance dei diversi fornitori. Usando questa semplice metrica, F-Secure ha raggiunto il punteggio massimo.
In breve: con F-Secure, puoi contare sulla migliore tecnologia EDR possibile. Se vuoi saperne di più sul framework MITRE ATT&CK e su come interpretare i risultati dei test, siamo a tua disposizione.
La valutazione MITRE è un ottimo punto di partenza ma occorre considerare anche altri fattori oltre alle prestazioni di rilevamento. Quando parli con i vendor delle loro soluzioni EDR, poni almeno queste domande. Abbiamo fornito le nostre risposte per darti alcuni esempi.

DOMANDE PER LA VALUTAZIONE DEI VENDOR EDR

La soluzione EDR è complessa e lunga da eseguire? F-Secure Rapid Detection & Response è progettato per essere gestito anche dagli analisti IT junior, con un'interfaccia utente e dashboard immediate. Dato che la soluzione visualizza tutte le attività in corso sugli endpoint, il team riuscirà facilmente a comprendere quando e come si verifica un attacco. Con le nostre azioni di risposta automatica e la guida integrata, inoltre, puoi rispondere agli attacchi senza essere un esperto certificato nella risposta agli incidenti.

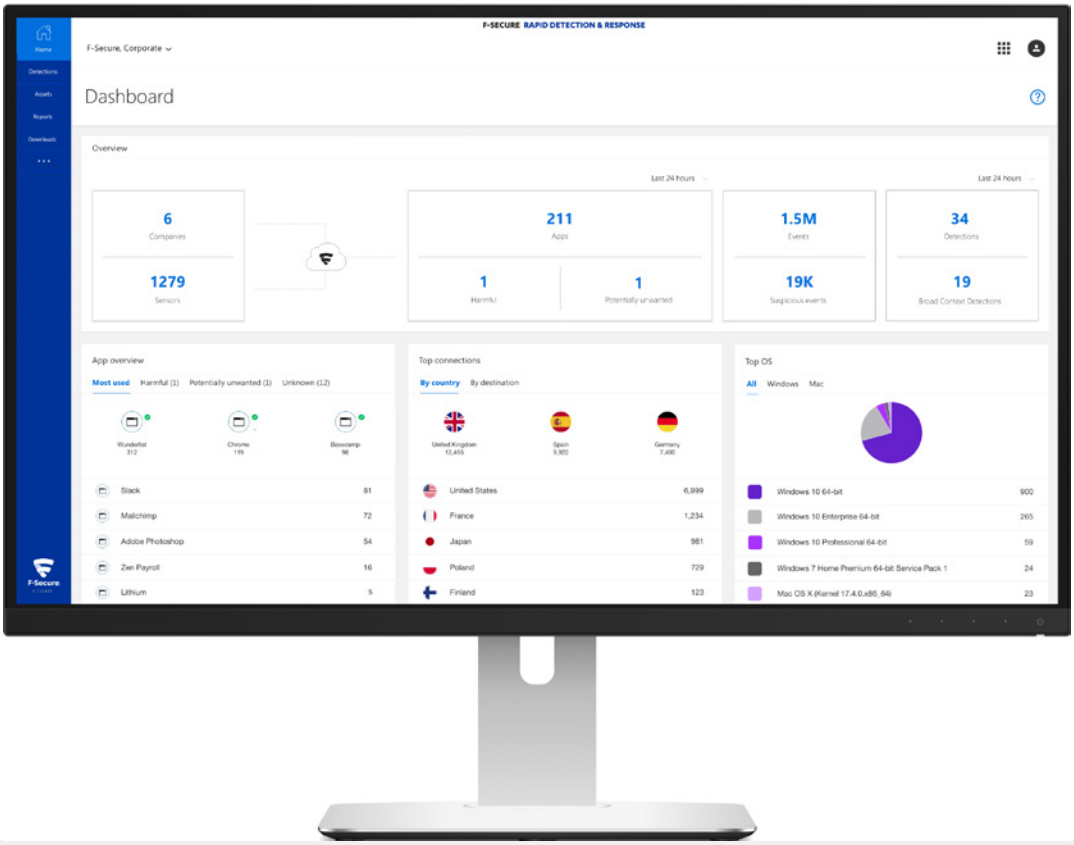
La soluzione può essere integrata con altri prodotti di sicurezza? F-Secure Rapid Detection & Response interagisce con tutte le altre piattaforme di protezione degli endpoint. Inoltre, è completamente integrato con la nostra pluripremiata soluzione di sicurezza degli endpoint, F-Secure Protection Service for Business. Con questo pacchetto per endpoint è possibile prevenire, rilevare e rispondere a tutte le minacce in modo efficace, nonché gestire entrambe le soluzioni all'interno dello stesso portale utente.

Qual è l'impatto della soluzione sugli endpoint in termini di prestazioni? I sensori endpoint di F-Secure Rapid Detection & Response sono leggeri e discreti, con un impatto prestazionale estremamente basso sugli endpoint. Come ci hanno confermato molti clienti, sono praticamente invisibili per l'utente finale, il che dovrebbe essere l'obiettivo di qualsiasi soluzione di cyber security.

In che modo la soluzione rileva le minacce? F-Secure Rapid Detection & Response utilizza la nostra tecnologia proprietaria Broad Context Detection™ per il rilevamento delle minacce. Utilizza l'analisi comportamentale, reputazionale e dei Big Data in tempo reale con machine learning per inserire automaticamente i rilevamenti in un contesto più ampio, che include i livelli di rischio, la criticità degli host interessati e il panorama delle minacce prevalente.

Che tipo di supporto offre il vendor? In caso di attacco o di rilevamento di minacce complesse, la nostra soluzione offre una funzionalità integrata chiamata Segnalare a F-Secure. Basta un clic su un pulsante per ottenere aiuto dai nostri esperti nella risposta agli incidenti, che hanno esperienza pratica nella gestione di innumerevoli cyber attacchi. Inoltre, si può decidere di acquistare F-Secure Rapid Detection & Response come servizio gestito, fornito da uno dei nostri rivenditori certificati. In questo modo potrai concentrarti sulle tue attività IT fondamentali, delegando la sicurezza agli esperti.

Per le organizzazioni più grandi e particolarmente interessanti per gli attaccanti, una soluzione ottimale può essere il servizio di threat hunting completamente gestito di F-Secure, che consente di bloccare in pochi minuti anche gli attacchi nation-state più complessi, con il supporto 24/7 dei nostri esperti in indagini sulle minacce e risposta agli incidenti.



F-SECURE RAPID DETECTION & RESPONSE

- Ottieni visibilità immediata sull'ambiente IT
- Rileva i cyber attacchi e i problemi IT in pochi minuti
- Rispondi alle minacce con automazione e guida
- Chiedi aiuto a F-Secure per i rilevamenti di minacce più complessi

Prenota una demo gratuita

NOTE DI CHIUSURA

1 451 Group. (2019). Thales Data Threat Report.

2 Verizon. (2019). Data Breach Investigations Report.

3 Ponemon. (2018). State of Cybersecurity in Small & Medium Size Businesses.

4 National Cyber Security Alliance. Cyberthreats and solutions for small and midsize businesses.

5 Ponemon. (2018). Cost of a Data Breach.

6 CVE Details (2019). Number of New CVEs Published Each Year.

INFORMAZIONI SU F-SECURE

Nessuno può vantare una visibilità sui cyber attacchi reali maggiore di F-Secure. Stiamo colmando il divario tra rilevamento e risposta, impiegando l'impareggiabile threat intelligence di centinaia dei migliori consulenti tecnici del settore, milioni di dispositivi che eseguono il nostro pluripremiato software e innovazioni incessanti nell'intelligenza artificiale. Le maggiori banche, compagnie aeree e imprese si affidano a noi per il nostro impegno volto a sconfiggere le minacce più potenti del mondo.

Insieme alla nostra rete costituita dai più importanti partner di canale e da oltre 200 service provider, il nostro obiettivo è fare in modo che ognuno disponga della cyber security di livello enterprise di cui tutti noi abbiamo bisogno. Fondata nel 1988, F-Secure è quotata sul listino NASDAQ OMX Helsinki Ltd.

f-secure.com/business | twitter.com/fsecure_it | linkedin.com/f-secure

F-Secure