Malwarebytes

SCHEDA DELLA SOLUZIONE

Malwarebytes Incident Response

Il sistema di eliminazione delle minacce più affidabile e completo al mondo

VANTAGGI PRINCIPALI

- Eliminazione automatica, precisa e completa delle minacce
- Superamento delle distanze tra i diversi silos operativi
- Riduzione del tempo di permanenza dei malware
- Risoluzione dei problemi di carenza di personale e competenze
- Riduce i costi e la complessità legati alla gestione degli interventi di risposta

PREMI

Forbes — Azienda più promettente degli Stati Uniti

CRN — Prodotto dell'anno

V3 — Innovazione di sicurezza dell'anno

Il numero e il tipo di eventi di sicurezza che devono affrontare i team responsabili di risolvere gli incidenti informatici (CIRT) è in costante aumento, come lo sono il costo e la complessità dei processi di eliminazione delle minacce.

Infatti, la correzione di oltre il 60 percento degli attacchi richiede più di 9 ore.[1] Considerate le risorse limitate e la frequenza delle minacce, oggi più che mai le organizzazioni devono passare da processi di risposta agli incidenti reattivi a processi automatizzati.

Malwarebytes Incident Response è una soluzione affidabile per l'eliminazione accurata e completa delle minacce, in grado di ottimizzare l'efficienza e l'efficacia degli interventi di risposta. Il nostro approccio automatico consente di rafforzare il modello di sicurezza impiegato e di superare le distanze tra i diversi silos operativi.

Funzionalità chiave

Eliminazione automatica

Il nostro sistema di eliminazione automatica consente ai team CIRT di evitare interventi mirati e manuali per la pulizia e il ripristino dei dispositivi in seguito a un'infezione malware, con un notevole risparmio di tempo e risorse. Le operazioni automatiche avvengono più velocemente e con maggiore precisione, riducendo il tempo di permanenza dei malware.

Eliminazione completa

La maggior parte delle soluzioni si limita a eliminare i componenti malware attivi ma ciò non costituisce un'eliminazione completa. Linking Engine di Malwarebytes applica un approccio proprietario che rileva e rimuove anche i componenti dinamici e quelli collegati. Il nostro motore applica tecniche di sequenziamento che garantiscono la rimozione dei meccanismi di persistenza dei malware rendendone permanente l'eliminazione. La nostra avanzata metodologia di eliminazione consente alle aziende di identificare ed eliminare i malware in modo rapido e completo.

Telemetria di livello superiore

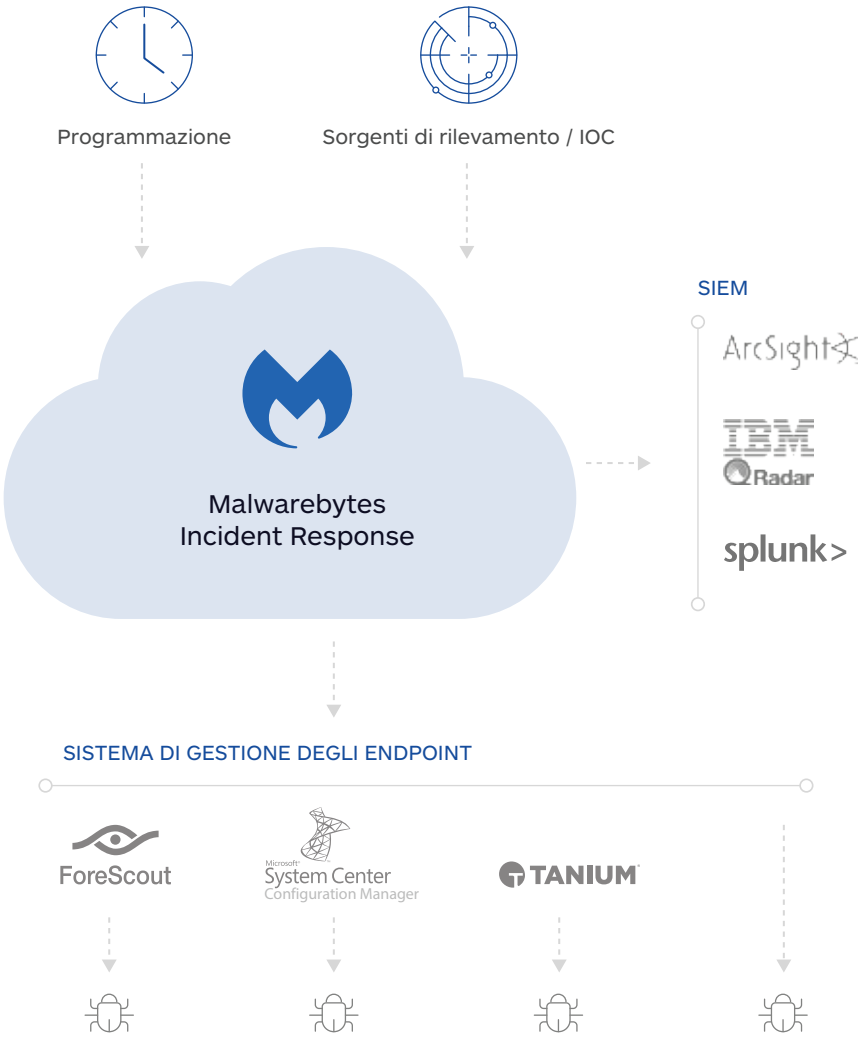
La nostra esperienza e le innumerevoli informazioni a cui possiamo attingere ci consentono di comprendere a fondo il problema degli attacchi ai dispositivi aziendali. Grazie ai nostri sistemi di analisi dei Big Data e a ricerche approfondite, riusciamo a correggere oltre 3 milioni di endpoint al giorno. Questa preziosa telemetria sul malware 0-day rende la nostra tecnologia più reattiva nei confronti delle minacce emergenti, aiutandoci a prevenire i malware futuri.

Individuazione proattiva

Le minacce sono sempre in agguato, in qualunque ambiente. Dopo essere riusciti a infettare un endpoint, i criminali tendono spesso ad allargare l'area colpita infettando altri dispositivi. Malwarebytes consente alle aziende di eseguire scansioni programmate che mirano all'individuazione proattiva dei più recenti indicatori di compromissione (IOC). La nostra soluzione permette di implementare facilmente una procedura di ricerca dei dispositivi compromessi che aumenta enormemente il livello di sicurezza.

Implementazione flessibile e predisposizione all'integrazione

Malwarebytes propone soluzioni flessibili, da implementare a seconda delle esigenze, scegli il nostro agente endpoint gestito da cloud persistente o l'agente endpoint non-persistente (Breach Remediation). L'agente non-persistente facilita inoltre l'integrazione nei SIEM e nei sistemi di gestione degli endpoint esistenti. La nostra soluzione può intervenire in tempo reale sugli IOC rilevati in rete dal sistema SIEM. Ad esempio, Malwarebytes è in grado di rispondere a un incidente sulla base di un avviso inviato da soluzioni Splunk o ForeScout.



Risorse web

Per ulteriori informazioni su Malwarebytes Incident Response, visita: malwarebytes.com/business/incidentresponse/
Ultime notizie: blog.malwarebytes.com/
Per richiedere un periodo di prova: malwarebytes.com/business/licensing

Riferimenti

[1] *Understanding the Depth of the Global Ransomware Problem*, Osterman Research

Santa Clara, CA | malwarebytes.com | corporate-sales@malwarebytes.com | 1.800.520.2796

Malwarebytes è l'azienda per la sicurezza informatica di prossima generazione a cui si affidano milioni di persone in tutto il mondo. Malwarebytes protegge in maniera proattiva i privati e le aziende da minacce pericolose quali malware, ransomware ed exploit che sfuggono al rilevamento degli antivirus convenzionali. Il principale prodotto dell'azienda combina la rilevazione euristica e avanzata delle minacce con le tecnologie senza firma per rilevare e arrestare un attacco informatico prima che possa danneggiare i sistemi. Oltre 10.000 aziende in tutto il mondo utilizzano, si affidano e consigliano Malwarebytes. Fondata nel 2008, la sede principale dell'azienda è in California, con uffici in Europa e Asia e conta su un team globale di ricercatori ed esperti della sicurezza.