Malwarebytes

SCHEDA DATI

Malwarebytes Incident Response

Rilevamento e correzione centralizzata delle minacce

FUNZIONALITÀ TECNICHE

Motore di Incident Response
Scansione delle minacce veloce ed estremamente efficace su richiesta, programmata e automatica

Varie modalità di scansione
Le modalità di scansione Hyper, Threat, e Custom non comportano interruzioni dell'operatività degli utenti finali

Linking Engine
Tecnologia senza firma che identifica e rimuove completamente tutte le minacce collegate al payload primario

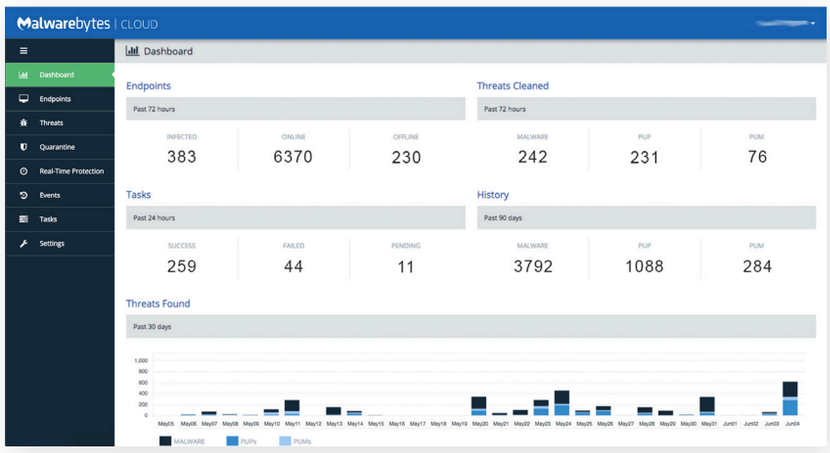
Piattaforma cloud di Malwarebytes
La console di gestione basata su cloud offre gestione della politica di sicurezza, installazioni e reporting sulle minacce semplici e centralizzati

Asset Management
Fornisce dati utili sul sistema di endpoint, tra cui oggetti in memoria, software installati, programmi di avvio e molto altro

Forensic Timeliner
Raggruppa e organizza gli eventi del log di Windows in un unico ordine di visualizzazione cronologico

Gli hacker moderni usano tecniche sempre più sofisticate per puntare le vittime, ottenere informazioni e sferrare i loro attacchi informatici. Le minacce continuano a fare breccia nelle difese di reti ed endpoint, nonostante i miliardi spesi da aziende, scuole e agenzie governative per la sicurezza. Il tempo e gli sforzi necessari per far fronte alle conseguenze degli attacchi[1] sono notevoli, richiedendo spesso dalle 6 alle 8 ore per correggere o effettuare il re-imaging di un singolo endpoint. Secondo una ricerca del Ponemon Institute, l'identificazione degli attacchi criminali o dannosi richiede in media 229 giorni, mentre il contenimento altri 82 giorni[2]. Le aziende devono rafforzare i team di sicurezza adottando i migliori sistemi di telemetria e correzione.

Malwarebytes Incident Response è uno strumento per il rilevamento e la correzione delle minacce, creato su una piattaforma di gestione altamente scalabile e basata su cloud. Effettua la scansione degli endpoint di rete per rilevare minacce avanzate tra cui malware, PUP e adware, per poi rimuoverli completamente. Malwarebytes Incident Response migliora il rilevamento delle minacce e ottimizza il tempo necessario a rispondere a un attacco, con i benefici aggiunti di scalabilità, flessibilità e automazione.



Console cloud di Malwarebytes – Dashboard

Riferimenti

[1] Quando si parla di "risposta agli incidenti", ci si riferisce in genere agli strumenti, ai processi e alle capacità impiegate dalle organizzazioni per far fronte e mitigare un attacco informatico dopo averlo identificato.

[2] Fonte: Ponemon Institute, Studio sui costi associati alla violazione dei dati, giugno 2016.

Vantaggi principali

Automazione

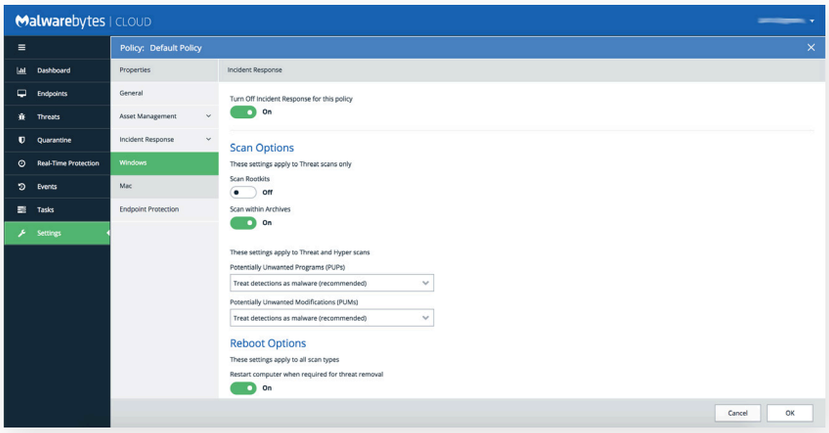
Puoi effettuare una pre-installazione di Malwarebytes Incident Response sui tuoi endpoint per il rilevamento e la correzione avanzati delle minacce a portata di clic. Malwarebytes Incident Response si integra inoltre con i sistemi di gestione dei tuoi endpoint, i SIEM e gli strumenti per il rilevamento delle minacce per rispondere automaticamente alle notifiche di incidenti. L'automatizzazione delle risposte alle minacce aiuta le aziende ad accelerare la risposta agli incidenti, riducendo i tempi di permanenza degli attacchi.

Flessibilità

Malwarebytes Incident Response si avvale di un agente persistente unificato e comprende inoltre opzioni con agenti non-persistenti (Breach Remediation). Ciò consente opzioni di implementazione flessibili in base ai diversi ambienti IT. Malwarebytes si integra facilmente nelle tecnologie di sicurezza esistenti, adattandosi al sistema operativo (Windows e Mac OS X) e ai requisiti dell'infrastruttura.

Scalabilità

Malwarebytes Incident Response viene fornito mediante la nuova piattaforma di gestione degli endpoint basata su cloud Malwarebytes, che riduce la complessità, rendendo semplice l'installazione e la gestione di Malwarebytes Incident Response e di altre soluzioni Malwarebytes a prescindere dal numero di endpoint. La console su cloud centralizzata elimina inoltre la necessità di acquisire e manutenere componenti hardware in loco.



Malwarebytes Incident Response – impostazioni della politica di sicurezza

REQUISITI DI SISTEMA

Componenti inclusi

- Piattaforma cloud di Malwarebytes
- Malwarebytes Incident Response (agenti Windows e Mac OS X persistenti)
- Breach Remediation (agenti Windows CLI, Mac GUI, Mac CLI non-persistenti)
- Forensic Timeliner (Windows)
- Assistenza telefonica e via e-mail

Requisiti hardware

Windows
CPU: 1 GHz
RAM: 1 GB (client); 2 GB (server)
Spazio su disco: 100 MB (programma + log)
Connessione internet attiva

Mac
Qualsiasi dispositivo Apple in grado di supportare Mac OS X (versione 10.10 o successiva)
Connessione internet attiva

Sistemi operativi supportati

Windows 10® (32 bit, 64 bit)
Windows 8.1® (32 bit, 64 bit)
Windows 8® (32 bit, 64 bit)
Windows 7® (32 bit, 64 bit)
Windows Vista® (32 bit, 64 bit)
Windows XP® con SP3 (solo 32 bit)
* Windows Server 2016® (32 bit, 64 bit)
* Windows Server 2012/2012R2® (32 bit, 64 bit)
* Windows Small Business Server 2011
* Windows Server 2008/2008R2® (32 bit, 64 bit)
* Windows Server 2003® (solo 32 bit)
Mac OS X (10.10 o versioni successive)

Notare che i server Windows che utilizzano il processo di installazione Server Core sono specificamente esclusi.

* *Integrazione Windows Action Center non supportata per i sistemi operativi Windows Server.*

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.