Malwarebytes

GEGEVENSBLAD

Malwarebytes Breach Remediation

Geavanceerde verwijdering van bedreigingen

TECHNISCHE KENMERKEN

- Geavanceerde malwareverwijdering met antirootkitscans
- Intelligente scanengine op basis van heuristiek en definities
- Geautomatiseerde ontdekking en verwijdering van malware op afstand
- Weergave van forensische gebeurtenissen op tijdlijn
- Aangepaste OpenIOC-bedreigingsindicatoren (XML-indeling)
- Vier typen systeemscans (volledig, bedreiging, hyper, pad)
- Optionele modi voor scannen-en-verwijderen of alleen-scannen
- Quarantainebeheer van gedetecteerde bedreigingen
- Verslaglegging van gebeurtenissen op centrale locatie (CEF-indeling)
- Geen blijvend ruimtebeslag op eindsysteem
- Specifieke scanengine voor Mac-malware en -adware
- Uitbreidbaar platform ondersteunt flexibele implementatieopties

De huidige incidentmedewerkers worden in hun werk belemmerd door traditionele inbreukdetectiesystemen die duizenden waarschuwingen per dag genereren maar de malware niet volledig kunnen verwijderen en zo niet kunnen voorkomen dat het terugkomt of zich lateraal verspreidt. Deze reactieve benadering vereist handmatig onderzoek naar het betreffende lek, waardoor kwaadaardige aanvallen gemiddeld 205 tot 229 dagen ongehinderd hun gang kunnen gaan.* Zodra malware op een laptop of server wordt ontdekt, kan een IT-beheerder wel zes huur kwijt zijn aan de imaging van elk geïnfecteerd apparaat.

Malwarebytes Breach Remediation is een volgende generatie platform voor geavanceerde detectie en verwijdering van bedreigingen dat bedoeld is voor kleine, middelgrote en grote bedrijven. Met Malwarebytes Breach Remediation kunnen organisaties proactief jacht maken op malware en incidenten op afstand oplossen, in plaats van dat ze fysiek naar elke geïnfecteerde computer gaan en het apparaat herstellen of imagen. Het is een onafhankelijk platform dat gemakkelijk geïntegreerd kan worden in de bestaande beveiligings- en beheertools van het bedrijf. Malwarebytes Breach Remediation biedt de unieke mogelijkheid om malware gelijktijdig te detecteren en te verwijderen. Hierdoor neemt het risico op aanhoudende bedreigingen grotendeels af.

Belangrijkste voordelen

Verwijdert malware grondig

Verwijdert alle sporen van infecties en gerelateerde artefacten, niet alleen de primaire belasting of infecterende instantie. Elimineert het risico op nieuwe aanvallen of laterale bewegingen die kapitaliseren op overgebleven sporen van malware. Malwarebytes is de feitelijke marktleider in malwareverwijdering—vertrouwd door miljoenen en getest door AV-Test.org.

Reduceert stilstandtijd aanzienlijk

U kunt uw aandacht richten op projecten die geld opleveren, in plaats van talloze uren te spenderen aan het handmatig oplossen van malwaregerelateerde incidenten en het maken van nieuwe hardware-images in de hele onderneming.

**Gartner Security & Risk Management Summit Presentation, Defending Endpoints From Persistent Attack, Peter Firstbrook, 8-11 juni 2015*

Ponemon Institute, 2016 Cost of Data Breach Study, juni 2016.

Werkt proactief, niet reactief

Maakt gebruik van automatische verwijdering die proactief detecteert en gelijktijdig incidenten oplost. Het lijkt op de installatie van een sprinklerinstallatie om kleine branden te blussen voordat ze zich verspreiden. U bent de held, omdat u het probleem op kunt lossen in plaats van op duizenden beveiligingswaarschuwingen per dag te hoeven reageren.

Jaagt op malware

Ontdekt nieuwe en onopgemerkte malware en kwaadaardige activiteiten en verwijdert deze snel. Gebruikt naast de IOC's (indicators of compromise) inbreukdetectietools en -bibliotheken van derden de gedragsregels en heuristiek van Malwarebytes.

Extraheert forensische gebeurtenissen

Spoort forensische gebeurtenissen op via de gepatenteerde Forensic Timeliner-functie, zodat uw team beveiligingslekken of onveilig gebruikersgedrag kan aanpakken. Verzamelt systeemgebeurtenissen vóór en tijdens een infectie en presenteert gegevens op een handige tijdlijn voor een uitgebreide analyse van vector- en aanvalsketens. Tot de afgedekte gebeurtenissen behoren bestands- en registerwijzigingen, bestandsuitvoering en bezochte websites.

Verhoogt waarde van bestaande investeringen

Integreert eenvoudig met bestaande beveiligingsinformatie- en gebeurtenisbeheertools (bijv. Splunk, ArcSight en QRadar), inbreukdetectiesystemen (bijv. Lastline, Mandiant en Fidelis) en eindsysteembeheerplatforms (bijv. Tanium, ForeScout en Microsoft SCCM). U kunt implementatie en verwijdering via uw eindsysteembeheerplatform activeren op basis van waarschuwingen die u ontvangt uit uw SIEM en automatisch oplossingsdetails terugvoeren in uw SIEM.

Dicht beveiligingslek van Apple

Verwijdert malware en adware snel van Mac-eindsystemen. Schoont OS X-systemen in minder dan één minuut helemaal op. Afzonderlijke GUI- en opdrachtregelprogramma's maken flexibel gebruik van populaire Mac-beheeroplossingen mogelijk (bijv. Apple Remote Desktop, Casper Suite en Munki). Maakt geautomatiseerd gebruik op afstand mogelijk via shell- of AppleScript-opdrachten. Systeembeheerders en incidentmedewerkers kunnen systeeminformatie verzamelen via gebruiksvriendelijke Snapshot-opdracht.

SYSTEEMVEREISTEN

Ga naar malwarebytes.com/business/breachremediation voor alle technische specificaties en systeemvereisten.

Opgenomen componenten:
CLI-programma voor Windows
Programma Forensic Timeliner voor Windows
GUI-programma voor Mac
CLI-programma voor Mac

Eindsystemen
Ondersteunde besturingssystemen:
Windows 10, 8.1, 8, 7, Vista, XP
Windows Server 2012, 2008, 2003
Mac OS X (10.8 en hoger)

malwarebytes.com/business corporate-sales@malwarebytes.com 1.800.520.2796

Malwarebytes beschermt particuliere klanten en bedrijven tegen gevaarlijke bedreigingen, zoals malware, ransomware en exploits die aan de detectie van traditionele antivirusoplossingen ontsnappen. Malwarebytes Anti-Malware, het paradepaardje van het bedrijf, heeft een uiterst geavanceerde heuristische detectie-engine. Deze engine heeft wereldwijd al meer dan vijf miljard kwaadaardige bedreigingen van computers verwijderd. Wereldwijd vertrouwen meer dan 10.000 kleine, middelgrote en grote bedrijven de beveiliging van hun gegevens toe aan Malwarebytes. Het bedrijf is opgericht in 2008 en heeft zijn hoofdkantoor in Californië. Het heeft vestigingen in Europa en wordt ondersteund door een mondiaal team van onderzoekers en deskundigen.