Malwarebytes

GEGEVENSBLAD

Malwarebytes Incident Response

Gecentraliseerde detectie en verwijdering van bedreigingen

TECHNISCHE KENMERKEN

Incident Response-engine
Snelle, supereffectieve scan van bedreigingen met on demand, geplande en geautomatiseerde opties

Meerdere scanmodi
Hyper-, Threat- en Custom-scans worden op de achtergrond uitgevoerd

Linking Engine
Signature-loze technologie die alle kwaadaardige objecten die aan de primaire bedreiging zijn gerelateerd herkent en grondig verwijdert

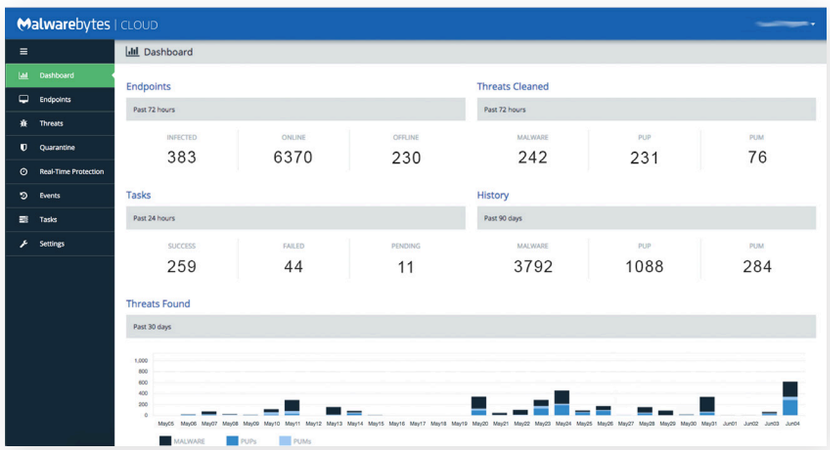
Het cloud-platform van Malwarebytes
Cloud-gebaseerde beheerconsole garandeert een makkelijk, gecentraliseerd beheer van het beveiligingsbeleid, de uitvoering ervan en het rapporteren van bedreigingen

Middelenbeheer
Bevat de benodigde gegevens over het eindsysteem, met inbegrip van geheugenobjecten, geïnstalleerde software, opstartprogramma's, enz

Forensic Timeliner
Haalt Windows-loggebeurtenissen op en zet deze in een chronologisch overzicht

Moderne aanvallers worden steeds slimmer in het benaderen en misleiden van hun slachtoffers en in het uitvoeren van hun cyberaanvallen. Kwaadaardige bedreigingen blijven de verdediging van netwerken en eindsystemen omzeilen, ondanks dat bedrijven, scholen en overheidsinstanties miljarden aan de versterking van hun beveiligingsstacks uitgegeven hebben. En het kost veel tijd en moeite om op deze incidenten[1] te reageren, waarbij het vaak 6 tot 8 uren duurt voordat één enkel eindsysteem hersteld of een systeemkopie teruggezet is. Volgens onderzoek van Ponemon Institute duurt het gemiddeld 229 dagen voordat kwaadaardige of strafbare datalekken vastgesteld worden, en 82 dagen voordat ze gedicht zijn[2]. Bedrijven moeten hun beveiligingsteams uitrusten met de krachtigste telemetrie en de beste verwijderingstools.

Malwarebytes Incident Response is een tool die bedreigingen detecteert en verwijdert en berust op een uiterst schaalbaar, cloudgebaseerd beheerplatform. Hij scant eindsystemen in een netwerk op geavanceerde bedreigingen, zoals malware, PUP's en adware, en verwijdert deze grondig. Malwarebytes Incident Response verbetert uw detectie van bedreigingen en uw reactiesnelheid op aanvallen. Bovendien is deze tool ook nog eens schaalbaar, flexibel en volautomatisch.



Malwarebytes-cloudconsole dashboard

Referenties

[1] *Bij maatregelen tegen incidenten gaat het meestal over de tools, de processen, en het talent die door organisaties worden gebruikt voor het aanpakken en verhelpen van een cyberaanval zodra deze is herkend.*

[2] *Bron: Ponemon Institute, 2016 Cost of Data Breach Study, juni 2016.*

Belangrijkste voordelen

Automatisering

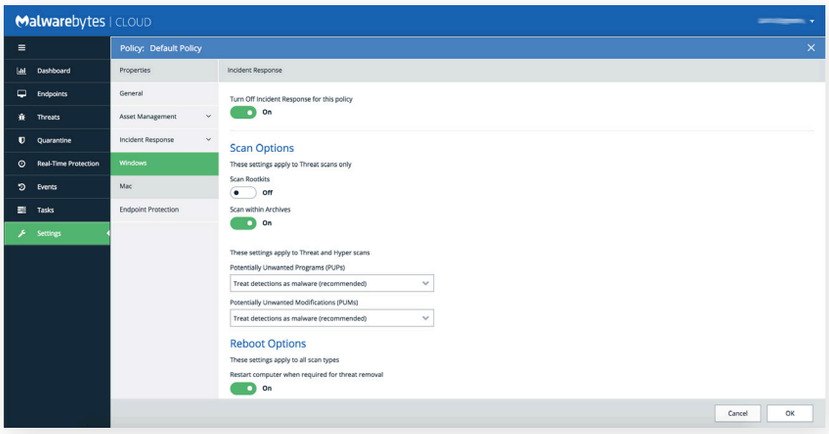
U kunt Malwarebytes Incident Response al op uw eindsystemen installeren, zodat u met één muisklik beschikt over geavanceerde mogelijkheden voor het detecteren en verwijderen van bedreigingen. U kunt dit ook integreren met uw bestaande SIEM-systeem, detectietools en beheerplatform voor eindsystemen, zodat er automatisch gereageerd kan worden op meldingen van incidenten. Door het automatiseren van tegenmaatregelen kunnen bedrijven de reactietijd en beveiligingsworkflows versnellen en downtime als gevolg van cyberaanvallen minimaliseren.

Flexibiliteit

Malwarebytes Incident Response gebruikt een permanente gezamenlijke agent en bevat ook niet-permanente agentopties (Breach Remediation). Hierdoor biedt hij flexibele gebruiksmogelijkheden voor uiteenlopende zakelijke IT-omgevingen. Malwarebytes kan eenvoudig worden geïntegreerd met uw bestaande beveiligingsoplossingen, is geschikt voor uw besturingssysteem (Windows en Mac OS X) en voldoet aan de eisen van uw infrastructuur.

Schaalbaarheid

Malwarebytes Incident Response wordt geleverd via ons Malwarebytes cloud-gebaseerde beheerplatform voor eindsystemen. Het Malwarebytes-cloudplatform vermindert de complexiteit, waardoor Malwarebytes Incident Response en andere oplossingen van Malwarebytes gemakkelijk gebruikt en beheerd kunnen worden, of u nu één of een miljoen eindsystemen hebt. Door deze gecentraliseerde cloud-console hoeft er geen eigen hardware aangeschaft en onderhouden te worden.



Malwarebytes Incident Response beveiligingsbeleid instellingen

SYSTEEMVEREISTEN

Opgenomen componenten

- Het cloud-platform van Malwarebytes
- Malwarebytes Incident Response (permanente Windows en Mac OS X agents)
- Breach Remediation (niet-permanente Windows CLI, Mac GUI, Mac CLI agents
- Forensic Timeliner (Windows)
- Ondersteuning via e-mail en telefoon

Hardwarevereisten

Windows
Processor: 1 GHz
RAM: 1 GB (clients); 2 GB (servers)
Schijfruimte: 100 MB (programma + logboeken)
Actieve internetverbinding

Mac
Elke Apple Mac die Mac OS X (10.10 of hoger) ondersteunt
Actieve internetverbinding

Ondersteunde besturingssystemen

Windows 10® (32-bits, 64-bits)
Windows 8.1® (32-bits, 64-bits)
Windows 8® (32-bits, 64-bits)
Windows 7® (32-bits, 64-bits)
Windows Vista® (32-bits, 64-bits)
Windows XP® met SP3 (alleen 32-bits)

* Windows Server 2016® (32-bits, 64-bits)
* Windows Server 2012/2012R2® (32-bits, 64-bits)
* Windows Small Business Server 2011
* Windows Server 2008/2008R2® (32-bits, 64-bits)
* Windows Server 2003® (alleen 32-bits)

Mac OS X (10.10 of hoger)

Merk op dat Windows servers die het Server Core-installatieproces gebruiken nadrukkelijk zijn uitgesloten.

* *Integratie van Windows Action Center is niet ondersteund voor Windows Server besturingssystemen.*

malwarebytes.com corporate-sales@malwarebytes.com 1.800.520.2796

Malwarebytes richt zich met methodes van de nieuwste generatie op het beveiligen van computers en heeft miljoenen klanten over de hele wereld. Malwarebytes beschermt particulieren en bedrijven proactief tegen gevaarlijke bedreigingen, zoals malware, ransomware en exploits die de detectie van traditionele antivirusoplossingen weten te omzeilen. Het topproduct combineert een geavanceerde heuristische detectie van bedreigingen met signature-loze technologieën voor het opsporen en tegenhouden van een cyberaanval voordat deze schade kan aanrichten. Meer dan 10.000 bedrijven over de hele wereld vertrouwen op en bevelen Malwarebytes aan. Het bedrijf is in 2008 in Californië opgericht en heeft vestigingen in Europa en Azië met een internationaal team van beveiligingsexperts en onderzoekers van bedreigingen.