

Malwarebytes Incident Response

Zentralisierte Erkennung und Beseitigung von Bedrohungen

Moderne Angreifer gehen immer raffinierter vor, wenn sie auf Informationen abzielen, Informationen über ihre Opfer sammeln und ihre Cyberangriffe durchführen. Schädliche Bedrohungen dringen nach wie vor in die Netzwerk- und Endpunkt-Abwehrvorkehrungen ein, auch wenn Unternehmen, Bildungseinrichtungen und Behörden Milliarden dafür aufgewendet haben, ihre Sicherheits-Stacks zu verstärken. Der Zeit- und Arbeitsaufwand, um auf Vorfälle zu reagieren¹, ist immens und zieht sich oft sechs bis acht Stunden hin, nur um etwas wiederherzustellen oder ein Image für einen einzelnen Endpunkt zu erstellen. Laut den Untersuchungen des Ponemon Institute dauert es durchschnittlich 229 Tage, um schädliche oder kriminelle Angriffe zu identifizieren, und 82 Tage, um sie unter Kontrolle zu bringen². Unternehmen müssen ihre Sicherheitsteams mit der informationstechnisch besten Telemetrie und den besten Wiederherstellungsmethoden ausrüsten.

Malwarebytes Incident Response ist ein Tool zur Erkennung von Bedrohungen und zur Wiederherstellung, das auf einer hoch skalierbaren, cloudbasierten Managementplattform basiert. Es scannt vernetzte Endpunkte auf erweiterte Bedrohungen wie Schadsoftware, PUPs und Adware und entfernt sie gründlich. Malwarebytes Incident Response verbessert Ihre Erkennung von Bedrohungen und verkürzt die Reaktionszeit auf einen Angriff aufgrund der zusätzlichen Vorteile der Skalierbarkeit, Flexibilität und Automatisierung.



Dashboard der Cloud-Konsole von Malwarebytes

Referenze

¹ Unter den Begriff der Vorfallsreaktion fallen allgemein die Tools, Prozesse und Mitarbeiter, die Organisationen einsetzen, um identifizierte Cyberangriffe zu bekämpfen und deren Auswirkungen zu mindern.

²Quelle: Ponemon Institute, 2016 Cost of Data Breach Study, Juni 2016.

TECHNISCHE MERKMALE

INCIDENT RESPONSE

Incident Response-Engine

Schnelle und extrem effektive Suche nach Bedrohungen mit bedarfsorientierten, geplanten und automatisierten Optionen

Verschiedene Scan-Modi

Scan-Modi Hyper, Threat und Custom ohne Unterbrechung der Endbenutzer

Linking-Engine

Signaturfreie Technologie erkennt alle mit dem primären Bedrohungs-Payload verbundenen Bedrohungsartefakte und entfernt diese gründlich

Malwarebytes-Cloudplattform

Cloudbasierte Managementkonsole zur einfachen und zentralisierten Verwaltung von Sicherheitsrichtlinien, Bereitstellungen und Berichten zu Bedrohungen

Asset-Management

Liefert praktische Daten zum Endpunktsystem, einschließlich zu Speicherobjekten, installierter Software, Start-up-Programmen und mehr

Forensic Timeliner

Erfasst und organisiert Windows-Protokollereignisse in einer einzigen chronologischen Ansicht

Wichtigste Vorteile

Automatisierung

Sie können Malwarebytes Incident Response vorab auf Ihren Endpunkten bereitstellen, um über eine fortschrittliche Erkennung und Beseitigung von Bedrohungen mit einem Klick zu verfügen. Das Programm lässt sich auch in Ihr vorhandenes Endpunktmanagement, SIEM und Ihre Tools zur Erkennung von Bedrohungen integrieren, um automatisch auf Vorfälle zu reagieren. Durch die Automatisierung von Reaktionen auf Bedrohungen können Unternehmen ihre Incident Response-Workflows beschleunigen und die Dauer der Angriffe verkürzen.

Flexibilität

Malwarebytes Incident Response verwendet einen einzigen persistenten Agenten und beinhaltet auch Optionen für nicht persistente Agenten (Breach Remediation). Dadurch erhalten Sie flexible Bereitstellungsoptionen für verschiedene IT-Geschäftsumgebungen. Zusammen mit einer einfachen Integration in Ihren vorhandenen Sicherheits-Stack erfüllt Malwarebytes Ihre Anforderungen in Bezug auf das Betriebssystem (Windows und Mac OS X) und die Infrastruktur.

Skalierbarkeit

Malwarebytes Incident Response wird über die neue cloudbasierte Endpunktmanagementplattform von Malwarebytes bereitgestellt. Durch die Malwarebytes-Cloudplattform verringert sich die Komplexität. Malwarebytes Incident Response und andere Lösungen von Malwarebytes können mühelos bereitgestellt und verwaltet werden, sei es für einen einzigen Endpunkt oder eine Million Endpunkte. Dank dieser zentralen Cloud-Konsole ist es nicht mehr notwendig, vor Ort installierte Hardware zu erwerben und zu warten.

SYSTEMANFORDERUNGEN

Composants inclus

Zugehörige Komponenten
 Malwarebytes-Cloudplattform
 Malwarebytes Incident Response
 (persistente Agenten für Windows und Mac OS X)
 Breach Remediation (nicht persistente Agenten für Windows CLI, Mac GUI, Mac CLI)
 Forensic Timeliner – Windows
 E-Mail- und Telefonsupport

Hardwareanforderungen

Windows

CPU: 1 GHz
 RAM: 1 GB (Clients); 2 GB (Server)
 Speicherplatz: 100 MB (Programm + Protokolle)

Aktive Internetverbindung

Mac

Jedes Apple Mac-Gerät, das Mac OS X (ab Version 10.10) unterstützt
 Aktive Internetverbindung

Unterstützte Betriebssysteme

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® mit SP3 (nur 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® (nur 32 Bit)
 Mac OS X (ab Version 10.10)

Bitte beachten Sie, dass Windows Server, bei denen das Serverkerninstallationsverfahren verwendet wird, ausdrücklich ausgeschlossen sind.

Die Integration von Windows Action Center wird für Windows-Server- Betriebssysteme nicht unterstützt.



malwarebytes.com/business



corporate-sales@malwarebytes.com



1.800.520.2796

Malwarebytes ist das Internetsicherheitsunternehmen der nächsten Generation, dem Millionen Anwender weltweit vertrauen. Malwarebytes schützt Menschen und Unternehmen proaktiv vor gefährlichen Bedrohungen wie Schadsoftware, Ransomware und Exploits, die von herkömmlichen Antivirenprogrammen nicht erkannt werden. Das führende Produkt des Unternehmens kombiniert eine fortschrittliche Heuristik zur Bedrohungserkennung mit signaturfreien Technologien, um Cyberangriffe zu erkennen und zu stoppen, bevor Schäden entstehen. Mehr als 10.000 Unternehmen auf der ganzen Welt nutzen, vertrauen und empfehlen Malwarebytes. Das im Jahr 2008 gegründete Unternehmen mit Hauptgeschäftssitz in Kalifornien verfügt über Standorte in Europa und Asien und beschäftigt ein global agierendes Team von Bedrohungs- und Sicherheitsexperten.