LÖSUNGSBESCHREIBUNG

Malwarebytes for Business

MALWAREBYTES ENDPOINT DETECTION AND RESPONSE

ÜBERSICHT

Sicherheitsexperten in Unternehmen aller Größenordnungen kämpfen gegen immer ausgeklügeltere Schadsoftware und Ransomware, wobei Angriffe mittlerweile alle elf Sekunden erfolgen. Trotz der von vielen Unternehmen unternommenen Anstrengungen zur Erkennung und Verhinderung von Cyberangriffen sind 69 Prozent der Unternehmen Opfer eines Ransomware-Angriffs geworden, und fast 60 Prozent der Endpunkte beherbergen versteckte Bedrohungen wie schädliche Trojaner, Rootkits und verschleierte Schadsoftware. Diese Bedrohungen sind verbreitet, hartnäckig und schaffen es oft, selbst dem besten Endpunktschutz zu entgehen. Das ist der Grund, warum mehr als die Hälfte aller Unternehmen angeben, dass sie nicht die Fähigkeit haben, fortschrittliche Attacken effektiv zu erkennen und mit diesen umzugehen. Demzufolge zahlen Firmen durchschnittlich ein Lösegeld von $ 240.000 und übermäßig viele falsch positive Sicherheitsbenachrichtigungen nehmen inzwischen mehr als 25 Prozent der Zeit und Arbeitsleistung von IT- und Sicherheitsteams für Untersuchungen und Analysen in Anspruch.

Um diese zunehmenden Sorgen zu adressieren, wurden die Richtlinien und Rahmenbedingungen des National Institute of Standards and Technology (NIST) und ähnlichen Einrichtungen durch kürzliche Updates an den Cybersicherheits-Rahmenbedingungen strikter, aber auch schwieriger umzusetzen. Was Unternehmen nun brauchen, ist die Fähigkeit, bekannte und unbekannte Bedrohungen an Endpunkten effizient zu entdecken, in Echtzeit zu reagieren, diese gründlich zu isolieren und zu untersuchen. Sollten Daten beeinträchtigt werden, verloren gehen oder für Lösegeldforderungen zurückgehalten werden, benötigen die Firmen einen resilienteren Endpoint Detection and Response (EDR), um das Problem zu beheben, einen Rollback durchzuführen und das System schnell und vollständig wiederherzustellen.

EDR-HERAUSFORDERUNGEN

Ransomware
Angriffe erfolgen inzwischen alle 11 Sekunden und verursachen im Durchschnitt einen Schaden von mehr als $ 240.000.

Komplexität
Mehr als 61 % der Unternehmen geben an, dass Komplexität und begrenzte Personalkapazitäten eine wesentliche EDR-Herausforderung darstellen.

Compliance
Die neuen NIST- und ähnlichen Richtlinien sind strikter und erschweren die Compliance.

Quellen: 2021 Studie, Cybersecurity Ventures; 2020 EDR-Studie, Ponemon Institute; 2021 Umfrage, IDC; 2019 Umfrage, CyberEdge/Statista

IDENTIFIZIEREN
Scannen & Evaluieren von Endpunkten

SCHÜTZEN
Abwehr von Einbrüchen

ERKENNEN
Abwehr vor der Ausführung

REAGIEREN
Isolierung & Bedrohungsjagd

WIEDERHERSTELLEN
Beseitigung IR & Wiederherstellung

Übernommen vom National Institute of Standards and Technology 800-171

INTUITIV

Malwarebytes Endpoint Detection and Response verwendet ein einzigartiges Machine-Learning-Konzept zur Anomalie-Erkennung, das nicht nur bekannte, sondern auch unbekannte Bedrohungen erkennt. Malwarebytes EDR überzeugt durch höhere Genauigkeit, daher haben wir eine der niedrigsten Raten falsch positiver Ergebnisse in der Branche. Unsere granulare Isolierung und resilienten Beseitigungsmöglichkeiten helfen dabei, eine laterale Ausbreitung der Schadsoftware zu verhindern, die schließlich zur Ausführung von Ransomware führen kann.

- Die granulare Isolierung verhindert, dass Lateralbewegungen einzelne Server, Subnetze oder Gruppen enthalten
- MITRE ATT&CK-Zuordnung mit wenigen Benachrichtigungen für falsch positive Ergebnisse
- Die resiliente Linking Engine zur Beseitigung von Schadsoftware entfernt Programmdateien, Artefakte und Modifikationen

EFFEKTIV

Malwarebytes EDR ist unterbrechungsfrei und kann innerhalb weniger Minuten über einen einfachen Endpunkt-Agenten angewendet werden. Unsere Nebula Cloud-Konsole gewährleistet einfaches und intuitives Management.

- Die intuitive, cloud-native Nebula-Managementkonsole spart Zeit, Kosten und Aufwand für IT-Dienste
- Unterbrechungsfreier, rollenbasierter Zugriff und ein leichtgewichtiger Agent
- Robuste SIEM, SOAR, ITSM* Integrationen automatisieren Support-Tickets, Scans und die Beseitigung von Schadsoftware

INKLUSIVE

Malwarebytes EDR bietet Ransomware-Rollback für Windows und verwendet zur Vermeidung von Leistungseinbußen einen Leightweight Agent, der im Gegensatz zu vielen anderen Lösungen mit nur drei Hintergrundprozessen auskommt.

- Geführte Bedrohungsjagd und sichere Bedrohungsanalyse mittels Cloud-Sandbox
- 72-Stunden-Ransomware-Rollback für Windows-Server
- Umfasst den Schutz vor Brute-Force-Angriffen über Remote Desktop Protocol (RDP)

INTEGRIERTER ENDPUNKTSCHUTZ

Das Machine Learning-Konzept von Malwarebytes EDR erkennt nicht nur bekannte Bedrohungen, sondern findet auch unbekannte „Zero-Day“ Bedrohungen, verschleierte Schadsoftware, Rootkits, und verdächtige Verhaltensweisen, die von anderen oft nicht erkannt werden. Die Erkennung verdächtiger Aktivitäten alarmiert bei Bedrohungen und liefert handlungsorientierte Erkenntnisse. Im Gegensatz zu mehr reaktiven, signaturbasierten Lösungen, bei denen die Schadsoftware ausgeführt werden kann, findet und blockiert unser Endpunktschutz Bedrohungen bereits vor einer Infizierung der Server. Durch die intuitive und cloud-native Malwarebytes Nebula-Managementkonsole können Sie Schadsoftware mit ein paar Klicks besiegen, nicht mit einem Dutzend Scripts. Ihr Sicherheitsteam kann vom globalen Dashboard aus innerhalb weniger Sekunden zu den erkannten Bedrohungen und den in die Quarantäne verschobenen Geräten navigieren.

MULTIMODALE ISOLIERUNG

Malwarebytes EDR ist die erste Lösung, die zur Endpunktisolierung mehrere miteinander kombinierte Funktionen bietet. Bei einem Angriff auf einen Endpunkt kann einfach verhindert werden, dass Schadsoftware sich verbreitet, Schaden anrichtet und während des Angriffs Unterbrechungen bei IT und Benutzern verursacht.

- **Netzwerkisolierung** schränkt die Geräte-Kommunikation ein, damit Angreifer ausgesperrt bleiben und Schadsoftware nicht „nach Hause telefonieren“ kann.
- **Prozessisolierung** begrenzt, welche Prozesse ausgeführt werden dürfen und hält so Schadsoftware auf, während die Benutzer produktiv bleiben können.
- **Desktopisolierung** für Windows-Workstations warnt Benutzer vor Bedrohungen und blockiert vorübergehend den Zugriff, während das Gerät für eine Analyse online bleibt.

*SIEM: Sicherheitsinformations- und Ereignismanagement
SOAR: Security Orchestration, Automation and Response
ITSM: IT Service Management

SCHUTZ VOR BRUTE-FORCE-ANGRIFFEN

Durch Telearbeit hat die Nutzung des Remote Desktop Protocol (RDP) weiter zugenommen, welches eines der primären Ransomware-Angriffsvektoren ist. Der Malwarebytes-Schutz vor Brute-Force-Angriffen für RDP ist leicht zu konfigurieren, in wenigen Minuten einsatzbereit, verhindert das Eindringen von RDP, verbessert die Erkennung, blockiert verdächtige Anmeldungen, und schützt vor Exploits wie gebündelte/polymorphe Schadsoftware.

AUTOMATISIERTE BESEITIGUNG VON SCHADSOFTWARE

Unsere automatisierte Herangehensweise macht manuelle Eingriffe bei der Problembeseitigung von Angriffen überflüssig und setzt wertvolle Zeitressourcen frei. Typische Schadsoftware-Infektionen können mehr als 100 Artefakte zurücklassen, einschließlich Dateien, Ordner und Registrierungsschlüssel, die sich auf andere Systeme Ihres Netzwerks ausbreiten können. Die meisten Lösungen beseitigen nur aktive Schadsoftware-Komponenten, beispielsweise Programmdateien, die Systeme einer Neuinfektion aussetzen (z. B. potenziell unerwünschte Programme oder Modifikationen (PUPs oder PUMs). Malwarebytes proprietäre Linking Engine erkennt und entfernt dynamische und zugehörige Artefakte, Modifikationen und Prozessänderungen. Unsere Engine setzt verknüpfte Sequenzierung ein, um eine gründliche Beseitigung der Schadsoftware zu gewährleisten.

SANDKASTEN IN DER CLOUD

Wir setzen bei der tiefgreifenden Analyse leistungsstarke Threat Intelligence in unserem Sandkasten in der Cloud ein, um die Präzision der Bedrohungserkennung zu steigern und Ihnen eine Vorabanalyse verfolgbarer IOCs (Indicators of Compromise) zu bieten. Potenziell gefährliche Schadsoftware kann im Sandkasten in der Cloud für eine Evaluierung und Analyse aktiviert werden.

GEFÜHRTE BEDROHUNGSJAGD

Die Bedrohungsjagd ermöglicht geplantes und bedarfsgesteuertes Scannen von Endpunkten zum Auffinden individueller IOC-Bedrohungen, vom Benutzer initiierte Bereinigungs-Scans über die Integration mit vorhandenen Werkzeugen für das Management von IT-Systemen und eine kontinuierliche Überwachung zum Schutz vor verdächtigen Dateien und Prozessereignissen, Netzwerkverbindungen und Registry-Aktivitäten. Asset-Management-Funktionen sammeln Endpunktdaten und zeigen sie an, inklusive Informationen zu installierter Software, Updates und Startprogrammen.

Visuelle Grafiken helfen Ihnen bei der Untersuchung von Prozessen, die von einer Bedrohung erzeugt wurden, und bei der Bestimmung, wohin sich die Prozesse lateral bewegt haben. Eine integrierte Incident-Response-Funktion sorgt dafür, dass Sie alle Spuren einer Bedrohung isolieren und beseitigen oder ungefährliche Aktivitäten global ausschließen können – und das alles mit einigen einfachen Klicks anstatt mit komplexen Skripten. Malwarebytes EDR erfasst detaillierte Bedrohungsinformationen des Servers und stellt eine MITRE ATT&CK-Zuordnung für die Analyse und Untersuchung bereit, damit Organisationen eine Zero Trust Architecture (ZTA) an Endpunkten umsetzen können.

RANSOMWARE-ROLLBACK

Für Windows-Plattformen umfasst Malwarebytes EDR eine einzigartige 72-Stunden-Ransomware-Rollback-Technologie, die die Zeit zurückdrehen und Ihr Unternehmen schnell wieder in einen gesunden Zustand bringen kann. Anders als bei weniger effektiven Dateisicherungsstrategien kann Malwarebytes, falls sich ein Angriff auf Benutzerdateien auswirkt, diese Modifikationen leicht wieder rückgängig machen, um Dateien wiederherzustellen, die bei einem Ransomware-Angriff verschlüsselt, gelöscht oder modifiziert wurden. Der Umfang der Datenspeicherung wird durch die Nutzung unserer unternehmenseigenen dynamischen Ausschlusstechnologie minimiert.

KONTINUIERLICHE ÜBERWACHUNG

Die fortschrittliche Flight-Recorder-Suchfunktion von Malwarebytes EDR bietet Transparenz und eine ständige Überwachung von Windows- und Mac-Workstations, um wertvolle Einblicke zu erhalten. Enthalten sind Suchmöglichkeiten nach MD5 (Hash-Wert), Dateinamen, Netzwerkdomains, IP-Adressen und Datei-/Prozess-Pfaden oder -Bezeichnungen. Außerdem können Sie sich automatisch verdächtige Aktivitäten anzeigen lassen, sich die vollständige Kommandozeile ausgeführter Prozesse ansehen und Ihre Daten 30 Tage lang in der Cloud speichern.

BRANCHENFÜHRENDE TECHNOLOGIE

Malwarebytes hat einige der frühesten Patente für Ransomware-Erkennung erhalten, einschließlich eines für Dateivergleiche und drei für verhaltensbasierte Erkennung. Wir setzen unser jahrelanges Sicherheits-Know-how bei der Beseitigung von Schadsoftware wirksam ein, um Ihnen die Bedrohungsdaten von Millionen durch Malwarebytes geschützten Endgeräten zur Verfügung zu stellen - sowohl für Unternehmen als auch für Privatanwender. Malwarebytes Endpoint Detection and Response für Windows und Mac, das mit unserer cloud-nativen Nebula-Managementkonsole verwaltet wird, kann leicht auf künftige Anforderungen angepasst werden. Malwarebytes gewährleistet eine hohe Rendite (Return on Investment, ROI) und niedrige Gesamtbetriebskosten (Total Cost of Ownership, TCO). Außerdem sind wir bekannt für unseren hervorragenden Service und Support.

IHRE SICHERSTE EDR-WAHL

Malwarebytes EDR erkennt effektiv und effizient verdächtige Aktivitäten, isoliert Angriffe, untersucht Bedrohungen und beseitigt Schäden. Viele Lösungen sind schwer umzusetzen und zu verwalten und sind zudem oft nicht kompatibel mit anderer Sicherheitssoftware. Viele andere EDR-Lösungen sind weniger resilient und beseitigen nur Programmdateien. Diese beinhalten nicht mehrere Isolierungsschichten, um Bedrohungen zu stoppen, bevor diese Schäden verursachen können; zudem sind diese so konzipiert, dass sie bei fast jeder Bedrohung eine Meldung auslösen und somit viele positiv falsche Ergebnisse liefern. Durch eine effektivere Erkennung und branchenweit weniger falsch positiven Meldungen hat Malwarebytes den CISO Choice Award für EDR gewonnen.

Malwarebytes EDR für Windows und Mac verwendet einen einzigen Lightweight Agent, der die Leistung nicht beeinträchtigt. Malwarebytes EDR ist zudem resilienter und über unsere cloud-native Nebula-Konsole einfacher zu verwalten. Wir erkennen verdächtige Aktivitäten auf einzigartige Weise und isolieren Prozesse und Netzwerke, um Schäden durch Schadsoftware zu minimieren. Desktopisolierung ist für Windows Workstations erhältlich und unsere proprietäre Linking Engine beseitigt Artefakte, Modifikationen und Prozessveränderungen.

Warten Sie nicht, bis es zu spät ist. Malwarebytes EDR ist Ihre sicherste Wahl für ein resilienteres Windows und Mac EDR. Mit unserem EDR für Unternehmen haben wir treue und zufriedene Kunden gewonnen, denn es ist effektiv, intuitiv und umfassend.

WEITERE INFORMATIONEN

Um weitere Informationen zu erhalten, wenden Sie sich bitte an unser Account-Team oder Ihren autorisierten Channel-Partner. Falls Sie mit einem Vertriebsmitarbeiter vor Ort sprechen möchten, besuchen Sie unsere Website unter:
www.sysob.com/hersteller/malwarebytes/endpoint-detection-response

Ist Ihre aktuelle Sicherheitsstrategie für den besten ROI optimiert? Klicken Sie hier, um sofort den Wert anzuzeigen, den dieses Produkt für Ihre Organisation erzielen kann.

https://www.sysob.com/hersteller/malwarebytes/ malwarebytes@sysob.com +49 9467 7406-200

Malwarebytes ist davon überzeugt, dass Menschen und Organisationen sich erst dann frei entfalten können, wenn sie frei von Bedrohungen sind. Wir leisten weit mehr als nur die Beseitigung von Schadsoftware. Jeden Tag bieten wir Zehntausenden von Verbrauchern und Unternehmen Cybersicherheit, Datenschutz und Prävention. Weitere Informationen finden Sie unter https://www.malwarebytes.com.