LÖSUNGSBESCHREIBUNG

Malwarebytes Endpoint Detection and Response (EDR)

Endpoint Detection and Response wurde mit Blick auf eine Response konzipiert, die so schnell ist wie ein Angriff.

Eine einfache Sicherheitsresponse für komplizierte Angriffe.

Technologie ermöglicht uns die digitale Kontaktaufnahme mit Kollegen und Partnern. Großartige Technologie ermöglicht uns genau dasselbe, nur auf sichere Weise. In einer Welt, in der Grenzen aufgehoben sind, bedeutet sichere Technologie widerstandsfähige Endpunkte, die bei einem Cyberangriff als die erste Verteidigungslinie agieren können. Doch die Forschung sagt uns, dass nahezu 60 Prozent der Endpunkte verborgene Bedrohungen enthalten. Davon sind 30 Prozent Trojaner, Rootkits und Backdoor-Programme. Diese Bedrohungen sind ausgeklügelt, persistent und umgehen häufig sogar die besten Schutzmaßnahmen.

Kompromittierte Endpunkte bedeuten einen Verlust an Produktivität. Heute reagieren Organisationen mit dem Re-Imaging infizierter Rechner, was häufig mehr kostet als das Gerät selbst, und trotzdem ist dabei mit einem Datenverlust zu rechnen. Alternativ dazu werden komplizierte Endpunkt-Response-Lösungen eingesetzt, deren Bereitstellung ein Team von Technikern erfordert – und ein noch größeres Team mit Doktorabschluss, um sie zu bedienen.

Keine dieser Optionen führt zu einem widerstandsfähigen Sicherheitsansatz. Was Organisationen brauchen, das ist die Fähigkeit, aktiv auf eine Bedrohung zu reagieren, während sie im Gange ist, und sie zu isolieren, zu untersuchen, zu beseitigen und die Daten wiederherzustellen, wodurch Endpunkte wieder in den Betriebszustand gebracht werden.

Das Argument für Widerstandsfähigkeit

Der Endpunkt und die wertvollen Daten, die darin enthalten sind, bilden den Kern der Mitarbeiterproduktivität. Sicherheitsteams fällt es schwer, Endpunkte im Fall von automatisierten Bedrohungen zu sichern, die ihre Methoden anpassen, um anfällige Benutzer, Anwendungen und Geräte anzugreifen. Organisationen, die sich auf signaturbasierte Erkennungen verlassen, die auf einer einzelnen Fehlerstelle beruhen, sind beim Schutz von Unternehmensendpunkten vor Viren der Vergangenheit erfolgreich, versagen jedoch, wenn es um die Vorhersage von und den Schutz vor Bedrohungen der Zukunft geht.

Was verhindert einen aktiven Response-Ansatz?

„Bedrohungen kommen trotzdem durch."

„Mehrere Anbieter-Schutzagents verlangsamen die Rechner der Benutzer."

„Ich habe keine Ahnung, wer meine Systeme angreift. Ich weiß nicht, wie lange die Eindringlinge schon da sind, und ich weiß auch nicht, wie sie in mein System gekommen sind."

„Ich habe weder die Tools noch erfahrene Mitarbeiter, die damit umgehen könnten."

„Ich habe ein EDR-System installiert, kann es aber nicht in vollem Umfang nutzen, weil ich keinen EDR-Experten vor Ort habe."

„Meine Endpoint-Response-Lösung erlaubt mir, den letzten Angriff zu untersuchen. Ich brauche ein Tool, mit dem ich den nächsten Angriff verhindern kann."

Für Sicherheitsexperten, die es nicht schaffen, den Endpunkt zu schützen, kann dies in eine katastrophale Unterbrechung von Vorgängen münden. Aber dieser Geschäftsbedarf entsteht zu einer Zeit, zu der Sicherheitsteams angesichts einer immensen Flut von Aufgaben in Bezug auf die Sichtung von Warnungen und die manuelle Beseitigung bei Endpunkten müde geworden sind. Organisationen benötigen einen kostengünstigen Ansatz für die Endpunktwiderstandsfähigkeit, die ihnen erlaubt, sich auf den unvermeidlichen Angriff vorzubereiten und aktiv darauf zu reagieren.

Wenn verdächtige Aktivität stattfindet, müssen Sicherheitsexperten innerhalb weniger Minuten aktiv reagieren, potenzielle Bedrohungen sofort unterbinden, damit sie sich nicht verbreiten, und dabei feststellen, ob das Verhalten tatsächlich bösartig ist. Endpoint-Response-Lösungen müssen eine schnelle und einfache Bereitstellung bieten, für den umgehenden Schutz der Assets der Organisation sorgen und die Reaktionszeit verkürzen. Integrierte Bedrohungserkennung erlaubt die progressive Bereicherung der Erkenntnisse der Bedrohungserkennung in der gesamten Angriffskette. Und eine cloudbasierte Plattfrom, die Administratoren durch die Untersuchung, die Response und die Wiederherstellung führt, gibt ihnen die Tools und die Daten, die sie für eine Response benötigen.

Aktive Response innerhalb von Minuten

Im Fall einer Sicherheitsverletzung haben Sicherheitsteams keine Zeit, um Modelle zu trainieren. Wenn Bedrohungen akut sind, muss der Fokus auf das Ergreifen von Maßnahmen gerichtet sein, anstatt eine Paralyse durch Analyse zu gestatten, während sich die Bedrohung verbreitet.

Malwarebytes ermöglicht Sicherheitsexperten eine unverzügliche, alle Endpunkte betreffende Response mit einer intuitiven Lösung, die keine steile Lernkurve erfordert.

Wenn eine Beseitigung von Schadsoftware erforderlich ist, eliminiert ein einziger, einheitlicher Agent die Komplexität und Kosten, die mit der Bereitstellung mehrerer Lösungen verbunden sind, sowie alle Systemkonflikte, die sich negativ auf die Leistung auswirken. Malwarebytes schützt, ohne die Endpunktleistung zu beeinträchtigen, und ermöglicht Organisationen, von der Infizierung zur Wiederherstellung zu gehen.

Einfache Bereitstellung minimiert die Reaktionszeit

Malwarebytes ist einfach bereitzustellen und liefert Ihnen über einen einzelnen Endpunkt-Agent wertvolle Erkenntnisse über Ihre Endpunkte und verborgene Bedrohungen. Über die Malwarebytes Nebula-Konsole wird alles zentral gesteuert und eine intuitive Benutzeroberfläche ermöglicht Sicherheitsteams, die Situation in weniger als fünf Sekunden zu beurteilen.

Was ist eine aktive Bedrohungsresponse?

- **Aktive Response**, die innerhalb von wenigen Minuten bereitgestellt werden kann
- **Progressive Bedrohungserkennung**, die Bedrohungen erfasst und sofortige Responsefunktionen gegen Angriffe sicherstellt
- **Plattform für geführte Bedrohungsresponse**, die die Daten bereitstellt, die zur Minimierung der durchschnittlichen Reaktionszeit (Mean Time To Respond, MTTR) nötig sind

Wichtigste Vorteile

- **Effektives und doch einfaches Konzept**, das von Sicherheitsexperten auf jedem Niveau bereitgestellt und gemanagt werden kann
- **Vollständige und gründliche Beseitigung von Schadsoftware**, sodass Endpunkte in einen fehlerfreien Zustand zurückversetzt werden
- **Kontinuierliche cloudbasierte Überwachung** von verdächtiger Aktivität
- **Integrierte Bedrohungserkennung**, die einen Angriff unabhängig vom Angriffsvektor stoppt
- **Die progressive Bedrohungserkennung bereichernde Intelligence**, die eine rapide Untersuchung eines erfolgreichen Angriffs ermöglicht
- **Geführte Bedrohungsresponse**, um kompromittierte Endpunkte zu isolieren, zu beseitigen und wiederherzustellen
- **Eine erweiterbare, cloudbasierte Malwarebytes Nebula-Plattform**, die eine unternehmensweite Angriffsresponse orchestriert

Linking Engine für eine vollständige Beseitigung der Schadsoftware

Typische Schadsoftware-Infektionen können mehr als 100 Artefakte zurücklassen, einschließlich Dateien, Ordner und Registrierungsschlüssel, die sich auf andere Systeme im Netzwerk einer Organisation ausbreiten können. Damit andere Sicherheitsanbieter diese Artefakte gründlich entfernen können, müssen sie Datenbankregeln erstellen oder Signaturen, um auf jede einzelne Komponente der Bedrohung abzuzielen und sie zu beseitigen. Dieser mühsame Ansatz verlangsamt die Endpunktleistung beträchtlich.

Incident-Response-Teams weltweit vertrauen auf Malwarebytes, was teils auf die Effektivität unserer Linking-Engine-Technologie zurückzuführen ist, die alle mit der primären Schadfunktion (Threat Payload) verbundenen Artefakte identifiziert und entfernt.

Malwarebytes Endpoint Detection and Response nutzt diesen proprietären Ansatz zusammen mit Erkenntnissen über verdächtige Aktivitäten, um Zero-Day- oder brandneue Schadsoftware zu entfernen und Endpunkte in ihren fehlerfreien Zustand zurückzuversetzen und dabei die Auswirkung auf Endbenutzer zu minimieren. Linking-Engine-Technologie:

- Findet und entfernt alle Spuren und Artefakte einer Infektion – nicht nur die primäre Schadfunktion (Threat Payload)
- Spart Zeit, die sonst für das Bereinigen und Re-Imaging von Endpunkten aufgewendet werden muss

Ransomware Rollback für bis zu 72 Stunden

Die „Ransomware Rollback"-Technologie ermöglicht Organisationen, die Uhr zurückzudrehen und schnell einen fehlerfreien Zustand wiederherzustellen. Falls sich ein Angriff auf die Endbenutzerdateien auswirkt, werden diese Modifikationen von Malwarebytes Endpoint Detection and Response einfach rückgängig gemacht, um Dateien wiederherzustellen, die in einem Ransomware-Angriff verschlüsselt, gelöscht oder modifiziert wurden. Außerdem haben Organisationen bis zu 72 Stunden Zeit, um den Schaden rückgängig zu machen.

- Drehen Sie die Uhr zurück und verhindern Sie den Schaden durch Ransomware dank rechtzeitiger Sicherungen.
- Machen Sie diese Änderungen schnell rückgängig und stellen Sie Dateien wieder her, die durch einen Angriff verschlüsselt, gelöscht oder verändert wurden.
- Die Datenspeicherung wird durch die Nutzung unserer unternehmenseigenen dynamischen Ausschlusstechnologie minimiert.

Flight Recorder für die Überwachung auf verdächtige Aktivitäten

Die **Flight-Recorder-Funktion** von Malwarebytes Endpoint Detection and Response bietet Transparenz und eine ständige Überwachung von Windows-Desktops, um wertvolle Einblicke zu erhalten. Damit können Sie:

- Ereignisse, die das Dateisystem, Netzwerkverbindungen, Prozessereignisse und Registry-Aktivitäten betreffen, ganz einfach nachverfolgen
- Vollständige Befehlszeilendetails ausgeführter Prozesse anzeigen
- Ereignisse während eines rollierenden Zeitraums von 72 Stunden in der Cloud speichern
- Verdächtige Aktivitäten automatisch anzeigen

Endpoint Isolation

Wenn ein Endpunkt gefährdet ist, stoppt Malwarebytes die Bedrohung, indem der Endpunkt isoliert wird. Kombiniert man diese Isolierung mit einer schnellen Beseitigung der Schadsoftware, wird verhindert, dass sich die Infektion lateral ausbreiten kann. Die Schadsoftware kann Ihre Daten nicht weiterleiten und Angreifer werden ferngehalten. Endpoint Protection and Response ist das erste Produkt, das drei Methoden der Endpunktisolierung miteinander kombiniert:

- **Netzwerk-Isolation**, die alle vom Endpunkt ausgehenden Prozesse daran hindert zu kommunizieren.
- **Prozess-Isolation**, die neue Prozesse daran hindert, am Endpunkt zu starten.
- **Desktop-Isolation**, die weitere Interaktion sofort unterbindet; das System bleibt im sicheren Zustand online und kann nur über die Nebula-Konsole aufgerufen werden.

Progressive Bedrohungserkennung

Der mehrschichtige Schutz durch Malwarebytes Endpoint Detection and Response erfasst Bedrohungen und bietet die Intelligence, die für die Untersuchung, Isolierung und Beseitigung von Cyberangriffen erforderlich ist.

Malwarebytes findet und beseitigt drei Millionen Infektionen pro Tag. Unsere einzigartige Telemetrie vermittelt umfangreiche Erkenntnisse über Bedrohungen und Techniken, die in Benutzerumgebungen erforderlich sind. Wir erhalten dadurch ein besseres Verständnis davon, warum diese Angriffe effektiv sind und wie sie am besten in den Griff zu bekommen sind.

Geführte Bedrohungsresponse

Malwarebytes stellt mit einer benutzerfreundlichen Plattform und vereinfachten Tools eine geführte Bedrohungsresponse für Sicherheitsexperten auf jedem Niveau bereit, um proaktive und kostengünstige Untersuchungen durchzuführen. Damit große als auch kleine Organisationen eine Endpunktwiderstandsfähigkeit erzielen können, müssen sie Zugriff auf intelligente Tools haben, mit der Fähigkeit, für eine Angriffsresponse die richtige Anleitung bereitzustellen. Diese Tools und ihre Plattform müssen erweiterbar sein, damit eine umfassende und konsistente Response über alle vorhandenen SIEM-, ITSM- und Netzwerkmanagementtools erfolgen kann. Abschließend muss eine geführte Bedrohungsresponse eine agile Datenuntersuchung mit visuellen Daten-Maps unterstützen, mit denen Ihre IR-Teams betroffene Endpunkte, Daten, Benutzer sowie andere Details zum Bedrohungsakteur identifizieren können.

Funktionen einer geführten Bedrohungsresponse umfassen:

- Geplantes Scannen von Endpunkten und Scannen bei Bedarf zum Auffinden individueller IOC-Bedrohungen
- Vom Benutzer initiierte Bereinigungs-Scans, die durch Integration mit Ihren vorhandenen Werkzeugen für das Management von IT-Systemen aktiviert werden
- Kontinuierliche Überwachung auf verdächtige Dateien und Prozessereignisse, Netzwerkverbindungen und Registry-Aktivitäten
- Asset-Management, bei dem Endpunktdaten (z. B. installierte Software, Updates und Startprogramme) erfasst und angezeigt werden
- Visuelle Grafiken zur Untersuchung von Prozessen, die von einer Bedrohung hervorgebracht wurden, und wohin diese sich lateral bewegt hat

Der Wert der Widerstandsfähigkeit von Unternehmen

Malwarebytes Endpoint Detection and Response bietet Unternehmen die Widerstandsfähigkeit, die nötig ist, um Mitarbeiter, Endpunkte und die darin gespeicherten vertraulichen, proprietären Daten zu schützen. Bei Sicherheitsverletzungen unterbindet eine Lösung mit aktiver Bedrohungsresponse unverzüglich die Verbreitung einer Infektion im Netzwerk einer Organisation, minimiert die Auswirkung und sorgt dafür, dass Geräte, Daten und Mitarbeiter wieder arbeiten. Progressive Bedrohungserkennung verhindert so viele Sicherheitsverletzungen wie möglich, während sie die erforderlichen Daten und Tools bereitstellt, um jegliche erfolgreiche Angriffe zu untersuchen, zu isolieren und zu beseitigen. Und abschließend ist unsere Plattform für die geführte Bedrohungsresponse nicht nur benutzerfreundlich, sondern auch flexibel und erweiterbar; sie überbrückt Technologie- und Sicherheitslücken, um Sicherheitsteams einen zusammenhängenden und konsistenten Responseplan bereitzustellen.

Malwarebytes Endpoint Detection and Response umfasst alle drei Ansätze – die aktive Bedrohungsresponse, die progressive Bedrohungsresponse und die geführte Bedrohungsresponse – und bietet gleichzeitig eine innovative Beseitigungstechnologie in einer eleganten, benutzerfreundlichen Oberfläche. All dies zusammen ergibt nicht nur widerstandsfähige Endpunkte, sondern eine widerstandsfähige Organisation, die bereit ist, sich von jedem Cyberangriff zu erholen und die Arbeit wieder aufzunehmen.

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

Malwarebytes ist ein Unternehmen für Cybersicherheit, dem weltweit Millionen von Anwendern vertrauen. Malwarebytes schützt Endanwender und Unternehmen proaktiv vor bösartigen Bedrohungen, einschließlich Ransomware, die herkömmlichen Antivirusprogrammen entgehen. Das führende Produkt des Unternehmens verwendet signaturlose Technologien, um einen Cyberangriff zu erkennen und zu stoppen, bevor er Schaden anrichtet. Mehr dazu erfahren Sie unter www.malwarebytes.com.