MALWAREBYTES
UNTERNEHMENS-PORTFOLIO

Endpunkt-Sicherheitslösungen

	Malwarebytes Incident Response	Malwarebytes Endpoint Protection	Malwarebytes Endpoint Detection and Response
BESEITIGUNG VON BEDROHUNGEN			
Bedarfsgesteuerte und geplante Bedrohungs-Scans, auflösbare Malwarebytes Breach Remediation (MBBR)	✔	✔	✔
BEDROHUNGSPRÄVENTION			
Manipulationsschutz Verlangt von Benutzern, ein Kennwort einzugeben, wenn sie versuchen, Malwarebytes Endpoint Agent Software zu deinstallieren	✔	✔	✔
Systemüberwachung Erlaubt dem Malwarebytes Endpoint Agent Monitor Service, den Endpoint Agent Service zu überwachen und neu zu starten, wenn dieser offline geht oder angehalten wird	✔	✔	✔
USB-Geräteüberwachung Legen Sie Berechtigungen für USB-Massenspeichergeräte fest, sodass der Zugriff gesperrt, erlaubt oder nur im schreibgeschützten Modus möglich ist		✔	✔
MULTI-VEKTOR-SCHUTZ – die Technologie von Malwarebytes umfasst mehrere Ebenen, damit Angreifer an jedem Punkt der Angriffskette gestoppt werden können			
Internetschutz Verhindert den Zugriff auf bösartige Websites, Werbe- und Scammer-Netzwerke		✔	✔
Anwendungshärtung Reduziert die Angriffsfläche von Schwachstellen und erkennt proaktiv Fingerprinting-Versuche bei fortgeschrittenen Angriffen		✔	✔
Exploit-Abwehr Erkennt und blockiert proaktiv Versuche, Schwachstellen auszunutzen und aus der Ferne Code auf dem Endpunkt auszuführen		✔	✔
Schutz des Anwendungsverhaltens Verhindert, dass Anwendungen zur Infektion von Endpunkten missbraucht werden		✔	✔
Anomalie-Erkennung mithilfe maschineller Lernalgorithmen Erkennt proaktiv unbekannte Viren und Schadsoftware mithilfe maschineller Lernverfahren		✔	✔
Payload-Analyse Anti-Schadsoftware-Technologie, die dazu ausgelegt ist, ganze Familien bekannter und relevanter Schadsoftware anhand heuristischer und verhaltensbasierter Regeln zu identifizieren		✔	✔
Ransomware-Abwehr Erkennt und blockiert Ransomware, die durch verhaltensbasierte Überwachungstechnologie identifiziert wurde		✔	✔
Brute-Force-Schutz Schutz für Windows-Endpunkte vor verdächtigen Verbindungen über Remote-Geräte		Windows-Desktop und -Server	Windows-Desktop und -Server

Endpunkt-Sicherheitslösungen

	Malwarebytes Incident Response	Malwarebytes Endpoint Protection	Malwarebytes Endpoint Detection and Response
BEDROHUNGSSUCHE, ISOLIERUNG UND WIEDERHERSTELLUNG			
Überwachung verdächtiger Aktivitäten Kontinuierliche Überwachung und Transparenz von Dateisystem-Ereignissen an Endpunkten, Netzwerkverbindungen, Prozess-Ereignissen und Registry-Aktivitäten			✔
Flight Recorder-Suche Unstrukturierte Bedrohungssuche auf allen mit EDR verwalteten Geräten			✔
Integrierte Cloud-Sandbox Niemals zuvor gesehene (einzigartige und neue) Binärdateien werden in einer sicheren, isolierten virtuellen Umgebung automatisch zur Detonation gebracht. Die Ergebnisse werden verwendet, um die Daten, die unter „Verdächtige Aktivitäten" aufgeführt werden, anzureichern			✔
Endpoint Isolation Netzwerk-, Prozess- und Desktop-Isolierung, die verhindert, dass Schadsoftware „zu Hause anruft" und gleichzeitig Remote-Angreifer aussperrt			✔
Ransomware-Rollback Bis zu 72 Stunden Schutz für Dateien, die durch einen Ransomware-Angriff verschlüsselt, gelöscht oder verändert wurden			✔
MITRE ATT&CK-Zuordnung Zeigt auf, wie die Erkennungsregeln von Malwarebytes mit dem MITRE ATT&CK-Framework verknüpft sind			✔
Active Response Shell Fernabruf von verdächtigem Code und Nutzung von Forensic Timeliner zur Untersuchung und Protokollierung			✔
MANAGEMENT			
Zentralisierte Managementkonsole	✔	✔	✔
MOBILE SICHERHEIT			
Erweitert unseren leistungsstarken Endpunktschutz auf Ihre mobilen Geräte und schützt vor den neuesten mobilen Bedrohungen wie Ransomware, bösartigen Apps und PUPs. Mit dem Echtzeitschutz für Ihre mobilen Geräte können Sie den versehentlichen Zugriff auf gefährliche Websites verhindern, sich vor schädlichen Apps schützen und unerwünschte Werbung blockieren.	**Unterstützte Betriebssysteme:** Android, Chromebooks, iOS		

Managed Detection and Response

	Malwarebytes Managed Threat Hunting (MTH)	Malwarebytes Managed Detection & Response (MDR)
24/7/365 Überwachung, Analyse, Hilfestellung, Untersuchung		✔
24/7/365 individuelle Bedrohungssuche		✔
24/7/365 aktive Kampagnen zur Bedrohungssuche	✔	✔
24/7/365 fachkundige Schadsoftware-Beseitigung auf Endpunkten		✔
24/7/365 Hilfestellung zur Schadsoftware-Beseitigung	✔	✔
Verwendung von Bedrohungsdaten aus mehreren Quellen	✔	✔
31-tägiger Rückblick über kritische IOCs		✔
Benachrichtigungen über die Portale Nebula und OneView sowie abgestufte Benachrichtigungen basierend auf dem Schweregrad des Vorfalls	✔	✔
Monatliche Berichterstattung über die Servicebereitstellung		✔
Integration mit Account-Managern für eine schnelle Sicherung und Wiederherstellung		✔
Erstklassiges Kunden-Onboarding		✔
Lizenzmodell	Abonnement	Abonnement

Dienste

SCHADSOFTWARE-ENTFERNUNGSSERVICE	
Unsere Branchenexperten helfen Ihnen, die Arbeitsfähigkeit Ihres Unternehmens nach einem Vorfall rasch wiederherzustellen. Von der ersten kritischen Reaktion bis hin zur vollständigen Beseitigung – wir bieten aus der Ferne einen lückenlosen Service, der eine sofortige Schadsoftware-Entfernung ermöglicht.	**Service-Phasen** • Festlegung des Projektumfangs • Überprüfung der Umgebung • Unterstützung bei der Installation • Bestätigung der Bereinigung und Wissenstransfer

Support

	Standard-Support	Standard Plus-Support
Support per Telefon, E-Mail, Chat	✔	✔
24/7 Schweregrad 1-Support		✔
Priorisierte Fallweiterleitung		✔
Zugang zu Wissensdatenbank, Community, Produktanleitungen, Online-Schulungen der Malwarebytes Academy	✔	✔

TECHNISCHE KUNDENBETREUUNG	
Sie erhalten eine tatkräftige, beratende Partnerschaft mit dem für Sie zuständigen technischen Kundenberater (TAM), der Ihnen hilft, die Möglichkeiten Ihrer Malwarebytes-Lösungen voll auszunutzen und Ihre IT-Servicelevel zu optimieren. Die TAM-Dienste von Malwarebytes bieten proaktive Sicherheitsressourcen für die Kundenvertretung und einen technischen Partner, der Sie dabei unterstützt, Ihr Sicherheitsprofil zu stärken.	Zusatzservice einschließlich Standard Plus-Support

Cybersicherheits-Module

VULNERABILITY ASSESSMENT	
Identifiziert, klassifiziert und priorisiert Schwachstellen in Treibern, Anwendungen, macOS und Windows Server- und Desktop-Betriebssystemen (OS), indem die Ergebnisse der automatischen Scans mit einem aktuellen Inventar der Software in Ihrer IT-Umgebung abgeglichen werden. Mit Vulnerability Assessment können Sie Scans planen, die fehlende Updates oder veraltete Versionen Ihrer Software aufspüren.	**Unterstützte Betriebssysteme:** Windows, MacOS
PATCH MANAGEMENT	
Automatisiert und beschleunigt die Installation und Überprüfung von Softwareaktualisierungen über verschiedene Betriebssysteme und eine breite Palette von älteren und modernen Drittanbieter-Anwendungen, darunter Adobe, Chrome und Cloud-Speicheranwendungen (wie Box). Mit Patch Management können Sie die Installation von Patches planen und zusammenfassende Berichte erstellen, die Sie bei der Einhaltung von Governance-, Datenregulierungs- und Cyberversicherungsanforderungen unterstützen.	**Unterstützte Betriebssysteme:** Windows
DNS FILTERING	
Ermöglicht es Ihnen, Websites zu sperren, die Risiken bergen und die Produktivität beeinträchtigen, sodass Sie Endbenutzer und Ihre webbasierten Anwendungen besser schützen können. DNS Filtering hilft Ihnen sicherzustellen, dass Ihre Endbenutzer im Internet sicherer und produktiver sind, indem es ganze Kategorien unangemessener Websites, bekannte verdächtige Domänen sowie weitere gefährliche Inhalte filtert und so verhindert, dass sie in Ihrem Unternehmen verheerenden Schaden anrichten.	**Unterstützte Betriebssysteme:** Windows
CLOUD STORAGE SCANNING-SERVICE	
Vereinfacht die Überwachung, den Schutz und die Berichterstattung über die Sicherheit von Daten, die in verschiedenen Cloud-Speichern wie Box und OneDrive gespeichert sind. Cloud Storage Scanning verwendet einen einzigartigen, speziell entwickelten, herstellerunabhängigen Multi-Engine-Ansatz, der bekannte und unbekannte Bedrohungen in Dateien erkennt, die in der Cloud gespeichert sind.	**Unterstützte Speicheranbieter:** Box, OneDrive, Google Drive *Demnächst verfügbar:* Dropbox, AWS S3
APPLICATION BLOCK	
Versetzt Sie in die Lage, mühelos Anwendungen zu identifizieren und zu sperren, bei denen es sich um bekannte Bedrohungen handelt oder die am Arbeitsplatz einfach unnötig sind, ohne dass es die Komplexität Ihres Sicherheitsmanagements erhöht. Unser Application Block-Modul erweitert unsere cloudbasierte Sicherheitsplattform und sperrt Anwendungen, die ein Risiko darstellen oder die Produktivität mindern könnten, sodass Sie Endbenutzer besser schützen können.	**Unterstützte Betriebssysteme:** Windows

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.