Datenblatt

ThreatDown Powered by Malwarebytes

ThreatDown Elite

Robuster Schutz und effizienter, kostengünstiger Service

Überblick

Elite wurde speziell für Unternehmen mit begrenzten Ressourcen entwickelt und bietet umfassenden Schutz in einer einzigen Lösung, die unvergleichliche Benutzerfreundlichkeit und Sicherheitsanalysen zu einem vernünftigen Preis bietet.

Verbesserte Sicherheit

- **24x7x365 Endpunkt-Überwachung und Abhilfe** durch unser Team von Cybersecurity-Experten mit insgesamt 150 Jahren Erfahrung in den Bereichen Bedrohungssuche, forensische Analyse und Reaktion auf Sicherheitsvorfälle.
- **Angriffserkennung** durch preisgekrönte Technologie mit Überwachung verdächtiger Aktivitäten, unstrukturierter Bedrohungssuche und Ransomware-Rollback.
- **Beschleunigte Reaktion** durch zum Patent angemeldete Technologie, die Alarme kontinuierlich scannt und nur die besonders kritischen eskaliert, auf die unser Team in Ihrem Namen reagieren kann.
- **Bedrohungsprävention** mit Multi-Vektor-Schutz, der Ihre Geräte nicht verlangsamt.
- **Verringerung der Angriffsfläche** durch Schwachstellen-Scans, automatisches Patching und Firewall-Management.
- **Anwendungsblockierung** verhindert die Ausführung nicht autorisierter Programme auf Endpunkten.
- **Browser-Phishing-Schutz** hält die Produktivität hoch und schützt sensible Daten.
- **Sicherheit, die mit der Zeit immer besser wird**, da unser Expertenteam die gewonnenen Erkenntnisse zur Verfeinerung der Sicherheitstechniken einsetzt, um schnellere und präzisere Erkennungen und Warnungen zu ermöglichen.
- **Moderne integrierte Cloud-E-Mail-Sicherheit (ICES)** schützt vor komplexen Phishing-Angriffen mit adaptivem KI-Schutz und Abhilfemaßnahmen in Echtzeit (Add-on)

Geringere Komplexität

- **Zentralisierte Verwaltung** über eine cloudbasierte Konsole mit benutzerfreundlicher Oberfläche, die das Erlernen mehrerer Konsolen überflüssig macht – auch beim Hinzufügen von Sicherheitsfunktionen.
- **Einzelner, ressourcenschonender Agent**, der in wenigen Minuten installiert ist und mit allen ThreatDown-Produkten funktioniert.
- **Gerätesichtbarkeit** mit farbiger Anzeige des Sicherheitsstatus auf einen Blick.

Herausforderungen

- Zu viele Angriffe haben Erfolg – 88 % der Unternehmen wurden im vergangenen Jahr Opfer von Ransomware[1]
- Bedrohungsakteure verweilen zu lange – Es dauert im Durchschnitt 292 Tage, bis eine Sicherheitsverletzung erkannt und eingedämmt wird[2]
- Viele Einzellösungen erhöhen die Kosten und die Komplexität – 70 % der KMUs sind dabei oder planen, Software und Anbieter zu konsolidieren[3]
- Die IT-/Sicherheitsteams sind unterbesetzt – 86 % der Sicherheitsteams leiden unter einem Mangel an qualifizierten Arbeitskräften[4]

Vorteile

- Verbesserte Sicherheit – Patchen Sie identifizierte Software-Schwachstellen, um das Risiko eines erfolgreichen Cyberangriffs zu verringern
- Reduzierte Komplexität – Nutzen Sie Automatisierung, um den Zeit- und Arbeitsaufwand für die Suche und Bereitstellung von Patches für Schwachstellen zu reduzieren
- Optimierte Leistung – Beheben Sie Fehler und verbessern Sie die Stabilität und Leistung Ihrer Anwendungen insgesamt

- **Automatische Beseitigung** über die eigene Linking Engine, die die meisten ausführbaren Schadsoftwaredateien und die damit verbundenen Artefakte, Änderungen und Prozessveränderungen findet und automatisch entfernt.
- **Security Operations Center (SOC)** inbegriffen, mit unseren Technologien, die von unseren Experten verwaltet werden, um die Arbeit Ihres Teams zu unterstützen.

Wertmaximierung

- **Schnellste Implementierung**, validiert durch den „G2 Implementation Index“, der zeigt, dass unsere Suite die kürzeste Go-Live-Zeit unter allen Wettbewerbern hat.
- **Einfachste Verwaltung**, validiert durch den „G2 Usability Index“, der unsere Suite mit dem Prädikat „Easiest to use“ für ihre einfache Verwaltung und Nutzung auszeichnet.
- **Beste Kapitalrendite**, validiert durch den „G2 Results Index“, der unsere Suite mit dem „Best estimated ROI“ unter allen Wettbewerbern auszeichnet.
- **Bestes Preis-Leistungs-Verhältnis** für ein Paket, einen Agenten, eine Konsole, ein SOC und einen zuverlässigen Partner.

Merkmale

- **Managed Detection and Response**: 24x7x365-Überwachung durch unsere Experten, die in Ihrem Namen Bedrohungen analysieren, auf sie reagieren und sie beseitigen (auch solche, die sich der technischen Erkennung entziehen).
- **Endpoint Detection and Response**: Preisgekrönte Lösung, die kontinuierliche aktive Erkennung und Abhilfe, Überwachung verdächtiger Aktivitäten, einen integrierten Cloud-Sandkasten und Ransomware-Rollback bietet.
- **Threat Hunting**: Automatisiertes Alarmscanning, das EDR-Daten mit externen und internen Bedrohungsdaten abgleicht, Bedrohungen priorisiert und die besonders kritischen mit klaren Schritt-für-Schritt-Anleitungen eskaliert.
- **Endpoint Protection**: Defense-in-Depth-Prävention, die signaturbasierte, dateilose und Zero-Day-Angriffe stoppt, bevor sie Ihr System infiltrieren, einschließlich Firewall-Management.
- **Vulnerability Assessment**: Durchführung von Scans bei Bedarf oder nach Plan, um nach Schwachstellen in Betriebssystemen und Anwendungen zu suchen.
- **Patch Management**: Automatisierung des Patching-Prozesses, um potenzielle Eintrittspforten zu verschließen.
- **Application Block**: Einfaches Blockieren nicht autorisierter Programme zur Durchsetzung von Nutzungsrichtlinien.
- **Browser-Phishing-Schutz**: Verwendung von Heuristik und Signaturen, um bösartige Phishing-Websites, unerwünschte Werbung, Tracking-Skripte und Betrugsversuche zu blockieren.
- **Incident Response**: Basierend auf unserer eigenen Linking Engine, die nicht nur ausführbare Schadsoftwaredateien entfernt, sondern auch alle zugehörigen Dateien und Änderungen findet und automatisch löscht, um eine erneute Infektion zu verhindern.
- **31-Tages-Rückblicke** durch unser Expertenteam, das nach Anhaltspunkten für eine Gefährdung sucht, um Angriffe zu stoppen und Erkennungen und Warnungen in Zukunft zu verfeinern.
- **Premium-Support**: SLAs mit verbesserter Reaktionszeit und verlängerte Supportzeiten für Probleme der Stufe 1 (Add-on).
- **Adaptive KI-gestützte Erkennung und Beseitigung von E-Mail-Bedrohungen**: Stoppt moderne Phishing-Angriffe und deren Varianten – verwaltet über die einzelne, cloudbasierte ThreatDown-Konsole (Add-on).

[1] The Global Cost of Ransomware Study, Ponemon Institute 2025
[2] Cost of a Data Breach Report 2024, Ponemon Institute
[3] Elevate SMB IT Strategy with These Top 4 Priorities, Goto 2024
[4] 2024 Cyberthreat Defense Report, CyberEdge Group, LLC

Copyright © 2025, Malwarebytes. Alle Rechte vorbehalten. Malwarebytes, das Malwarebytes-Logo, ThreatDown und das ThreatDown-Logo sind Marken von Malwarebytes. Sonstige Marken und Warenzeichen können Eigentum Dritter sein. Alle hier aufgeführten Beschreibungen und technischen Daten können ohne vorherige Ankündigung geändert werden und werden ohne jedwede Gewährleistung zur Verfügung gestellt. 09/25