ThreatDown
Powered by Malwarebytes

DATENBLATT

THREATDOWN ADVANCED

Wenn “gut genug” nicht gut genug ist

UNTERNEHMEN BENÖTIGEN EINEN BESSEREN SCHUTZ IN EINEM EINZIGEN, BENUTZERFREUNDLICHEN PAKET, DAS NICHT DIE BANK SPRENGT

Cyberangriffe werden nicht langsamer. Im Jahr 2022 erlebten ~85 % der Unternehmen mindestens einen erfolgreichen Cyberangriff, ~40 % sechs oder mehr und fast drei Viertel (~70 %) erwarten, im kommenden Jahr getroffen zu werden.[1]

HERAUSFORDERUNGEN

- **Zu viele Angriffe sind erfolgreich:** 70 % der Unternehmen waren im vergangenen Jahr Opfer von Ransomware[2]
- **Bedrohungsakteure verweilen zu lange:** durchschnittlich 277 Tage, um eine Sicherheitsverletzung zu erkennen und einzudämmen[3]
- **80 % der Unternehmen** haben einen Exploit-Versuch auf eine bekannte Schwachstelle erlitten[4]
- **Mehrfachlösungen erhöhen Kosten und Komplexität:** Durchschnittlich 55 Cybersicherheitstools, die von Unternehmen eingesetzt werden[5]

THREATDOWN ADVANCED – VORTEILE

Speziell für Unternehmen mit begrenzten Ressourcen entwickelt, **ThreatDown Advanced** bietet überragenden Schutz in einer einzigen Lösung, die einfach zu verwalten ist, und das zu einem vernünftigen Preis.

Sicherheit verbessern

- **Erkennung von Angriffen** durch preisgekrönte Technologie, die die Überwachung verdächtiger Aktivitäten, die Freiform-Bedrohungssuche und das Rollback von Ransomware umfasst
- **Beschleunigte Reaktion** durch patentierte Technologie, die kontinuierlich Warnungen scannt und nur eskaliert die kritischsten mit klaren Leitlinien für empfohlene Reaktionsmaßnahmen
- **Threat prevention** mit Multi-Vektor-Schutz, der Ihre Geräte nicht verlangsamt
- **Reduzierung der Angriffsfläche** durch Schwachstellen-Scans und Patching-Prozesse, die planmäßig oder ad hoc ausgeführt werden, sowie Anwendungsblockierung, um die Ausführung bösartiger und unerwünschter Anwendungen zu verhindern

Komplexität reduzieren

- **Zentralisierte Verwaltung** über eine Cloud-basierte Konsole mit benutzerfreundlicher Oberfläche, die das Erlernen mehrerer Konsolen überflüssig macht – selbst wenn Sicherheitsfunktionen hinzugefügt werden
- **Ein einziger, leichtgewichtiger Agent**, der innerhalb von Minuten bereitgestellt wird und mit allen ThreatDown-Produkten funktioniert

- **Gerätesichtbarkeit** mit farbcodierten Hinweisen für den Sicherheitsstatus auf einen Blick
- **Automatische Fehlerbehebung (Remediation)** über die proprietäre Linking Engine, die Artefakte, Änderungen und Prozessänderungen, die Malware hinterlässt (und die die anderen übersehen), findet und automatisch entfernt

Wert maximieren

- **Schnellste Implementierung**, die durch den G2 Fall 2023 Implementation Index validiert wurde, der zeigt, dass unsere Suite die kürzeste Go-Live-Zeit aller Konkurrenzlösungen hat
- **Am einfachsten zu verwalten**, validiert durch den G2 Herbst 2023 Usability Index, der unsere Suite als "am einfachsten zu bedienen" ausgezeichnet hat für die einfache Verwaltung und Verwendung
- **Bester ROI**, validiert durch den G2 Fall 2023 Results Index, der unsere Suite mit dem "Best estimated ROI" aller Wettbewerbslösungen auszeichnete
- **Bestes Preis-Leistungs-Verhältnis** für ein Paket, einen Agenten, eine Konsole und einen vertrauenswürdigen Partner

THREATDOWN ADVANCED – FEATURES

- **Endpoint Detection and Response:** Preisgekrönte Lösung, die kontinuierliche aktive Erkennung und Reaktion, Überwachung verdächtiger Aktivitäten, integrierte Cloud-Sandbox, Endpunktisolierung, Ransomware-Rollback, MITRE ATT&CK-Mapping und Active Response Shell bietet
- **Managed Threat Hunting:** Proaktive, automatisierte Bedrohungssuche korreliert EDR-Warnungen und -Benachrichtigungen mit externen und internen Threat Intelligence-Feeds, die alle priorisieren und nur die kritischsten Warnungen mit klaren, schrittweisen Reaktionsanleitungen eskalieren
- **Endpoint Protection:** Multi-Vektor-Prävention, die auf mehreren Technologieebenen aufbaut, die signaturbasierte, dateilose, und Zero-Day-Angriffe, bevor sie Ihre Systeme infiltrieren
- **Vulnerability Assessment:** Ausführen von Scans bei Bedarf oder nach Zeitplan, um nach Schwachstellen in Betriebssystemen und Anwendungen zu suchen
- **Patch Management:** Automatisieren Sie den Patching-Prozess, um potenzielle Access Points zu sperren
- **Application Block:** Blockieren Sie auf einfache Weise nicht autorisierte oder unerwünschte Programme, um Richtlinien zur akzeptablen Nutzung durchzusetzen
- **Incident Response:** Basierend auf unserer proprietären Linking Engine, die nicht nur ausführbare Malware-Dateien entfernt, sondern auch alle zugehörigen Dateien und Änderungen findet und automatisch löscht, um eine erneute Infektion zu verhindern

ERWEITERTER SCHUTZ, EINFACHSTE BEDIENUNG,
BESTES PREIS-LEISTUNGS-VERHÄLTNIS.
Rufen Sie noch heute an, um loszulegen.

[1] 2023 Cyberthreat Defense Report, CyberEdge Group, LLC
[2] State of Malware Report 2023, Malwarebytes
[3] Cost of a Data Breach Report 2022, Ponemon Institute
[4] Cyber Security Report 2021, Check Point
[5] Cybersecurity Insights Report 2022, Anomali

ThreatDown™ Powered by Malwarebytes | de.malwarebytes.com/business/ | corporate-sales@malwarebytes.com | 1.800.520.2796