

# THREATDOWN BUNDLES

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 % haben sechs oder mehr erlebt, und fast drei Viertel (~70 %) erwarten, im kommenden Jahr betroffen zu sein.<sup>1</sup>

### Herausforderungen

- ✓ **Zu viele Angriffe sind erfolgreich:** 70 % der Unternehmen waren im vergangenen Jahr Opfer von Ransomware<sup>2</sup>
- ✓ **Bedrohungsakteure verweilen zu lange:** durchschnittlich 277 Tage, um eine Sicherheitsverletzung zu erkennen und einzudämmen<sup>3</sup>
- ✓ **Mehrfachlösungen erhöhen Kosten und Komplexität:** Durchschnittlich 55 Cybersicherheitstools, die Unternehmen implementiert haben<sup>4</sup>
- ✓ **IT-/Sicherheitsteams sind unterbesetzt:** 62 % der Unternehmen verfügen nicht über genügend Personal für Cybersicherheit<sup>5</sup>

### THREATDOWN CORE

**Core** Bietet umfassenden Schutz vor Malware, Zero-Day-Bedrohungen und mehr. **Core** umfasst preisgekrönte Technologien, die das Endpoint-Protection-Management erheblich vereinfachen

### THREATDOWN ADVANCED

**Advanced** Bietet überragenden Schutz in einer einzigen, benutzerfreundlichen Lösung zu einem vernünftigen Preis. Speziell entwickelt für Unternehmen mit kleinen Sicherheitsteams mit begrenzten Ressourcen, **Advanced** enthält preisgekrönte Technologien, die das Endpoint Protection Management erheblich vereinfachen.

### THREATDOWN ELITE

**Elite** Bietet umfassenden Schutz in einer einzigen Lösung, die beispiellose Benutzerfreundlichkeit zu einem vernünftigen Preis bietet. Speziell für Unternehmen mit kleinen (bis nicht vorhandenen) Sicherheitsteams, die nicht über die Ressourcen verfügen, um auf alle Sicherheitswarnungen zu reagieren, **Elite** umfasst preisgekrönte Technologien und eine von Experten verwaltete 24x7x365-Überwachung und -Reaktion

### THREATDOWN ULTIMATE

**Ultimate** Bietet den umfassendsten Schutz über den gesamten Angriffszyklus hinweg, von der überlegenen Reduzierung der Angriffsfläche bis hin zu vollständig verwalteter 24x7x365-Prävention, -Erkennung, -Reaktion und -Abhilfe.

<sup>1</sup> 2023 Cyberthreat Defense Report, CyberEdge Group, LLC

<sup>2</sup> State of Malware Report 2023, Malwarebytes

<sup>3</sup> Cost of a Data Breach Report 2022, Ponemon Institute

<sup>4</sup> Cybersecurity Insights Report 2022, Anomali

<sup>5</sup> State of Cybersecurity 2022: Global Update on Workforce Efforts, Resources and Cyberoperations, ISACA

# Vorteile

		Core	Advanced	Elite	Ultimate
Improve security	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 Warnmeldungen kontinuierlich scannt und nur die kritischsten mit klaren Anweisungen zu empfohlenen Reaktionsmaßnahmen eskaliert		•	•	•
	Threat prevention mit Multi-Vektor-Schutz, der Ihre Geräte nicht verlangsamt	•	•	•	•
	Reduzierung der Angriffsfläche durch Schwachstellen-Scans und Patching-Prozesse, die geplant oder ad hoc ausgeführt werden	•*	•	•	•
	24x7x365 Endpunktüberwachung und -reaktion durch unser Team von Cybersicherheitsexperten mit 150 Jahren Erfahrung in der Bedrohungssuche, forensischen Analyse und Incident Response			•	•
	Sicherheit, die mit zunehmendem Alter nur noch besser wird, da unser Expertenteam seine Erkenntnisse anwendet, um Sicherheitstechniken für schnellere und präzisere Erkennungen und Warnungen im Laufe der Zeit zu verfeinern			•	•
	Blockieren von Applications, um zu verhindern, dass nicht autorisierte Programme auf Windows-Endpunkten ausgeführt werden	•	•	•	•
Reduce complexity	Verbesserte Sicherheit und Produktivität durch Einschränkung ganzer Website-Kategorien von bösartigen Websites und unerwünschten Websites, die nicht dem Verhaltenskodex der Mitarbeiter entsprechen				•
	Zentralisierte Verwaltung über eine Cloud-basierte Konsole mit benutzerfreundlicher Oberfläche, die das Erlernen mehrerer Konsolen überflüssig macht – selbst wenn Sicherheitsfunktionen hinzugefügt werden	•	•	•	•
	Ein einziger, schlanker Agent, der in wenigen Minuten bereitgestellt wird und mit allen Malwarebytes-Produkten funktioniert	•	•	•	•
	Gerätesichtbarkeit mit farbcodierten Hinweisen für den Sicherheitsstatus auf einen Blick	•	•	•	•
	Automatische Fehlerbehebung über die proprietäre Linking Engine, die die meisten ausführbaren Malware-Dateien und die damit verbundenen Artefakte, Änderungen und Prozessänderungen findet und automatisch entfernt		•	•	•
Maximize value	Security Operations Center (SOC) in einer Box mit unseren Technologien, die von unseren Experten verwaltet werden, um die Bemühungen Ihres Teams zu unterstützen			•	•
	Schnellste Implementierung, die durch den G2 Winter 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 Winter 2023 Usability Index, der unsere Suite für ihre einfache Verwaltung und Verwendung als "am einfachsten zu bedienen" ausgezeichnet hat	•	•	•	•
	Bester ROI, validiert durch den G2 Winter 2023 Results Index, der unsere Suite mit dem "Best estimated ROI" aller Wettbewerbslösungen auszeichnete	•	•	•	•
	Bestes Preis-Leistungs-Verhältnis ein Bundle, ein Agent, eine Konsole, ein SOC (Ultimate und Elite) und ein vertrauenswürdiger Partner	•	•	•	•

# FEATURES

	Core	Advanced	Elite	Ultimate
<b>Endpoint Detection and Response:</b> Preisgekrönte Lösung, die kontinuierliche aktive Erkennung und Reaktion, Überwachung verdächtiger Aktivitäten, integrierte Cloud-Sandbox, Endpunktisolation, Ransomware-Rollback, MITRE ATT&CK-Mapping und Active Response Shell bietet		•	•	•
<b>Managed Threat Hunting:</b> Automatisiertes Scannen von Warnmeldungen, das EDR-Daten mit externen und internen Bedrohungsdaten-Feeds korreliert, Bedrohungen priorisiert und die kritischsten mit klaren, schrittweisen Reaktionsanleitungen eskaliert		•	•	•
<b>Endpoint Protection:</b> Multi-Vektor-Prävention, die auf mehreren Technologieebenen basiert, die signaturbasierte, dateilose und Zero-Day-Angriffe stoppen, bevor sie Ihre Systeme infiltrieren	•	•	•	•
<b>Vulnerability Assessment:</b> Ausführen von Scans bei Bedarf oder nach Zeitplan, um nach Schwachstellen in Betriebssystemen und Anwendungen zu suchen	•	•	•	•
<b>Patch Management:</b> Automatisieren Sie den Patching-Prozess, um potenzielle Access Points zu sperren		•	•	•
<b>Incident Response:</b> 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	•	•	•	•
<b>Managed Detection and Response:</b> 24x7x365-Überwachung durch unsere Experten, die in Ihrem Namen Bedrohungen analysieren, darauf reagieren und sie beheben (auch solche, die sich der technologischen Erkennung entziehen)			•	•
<b>Application Block:</b> Blockieren Sie auf einfache Weise nicht autorisierte Programme, um Richtlinien zur akzeptablen Nutzung durchzusetzen	•	•	•	•
<b>31-day lookbacks:</b> Unser Expertenteam sucht nach Kompromittierungsindikatoren, um Angriffe zu stoppen und Erkennungen und Warnungen in Zukunft zu verfeinern			•	•
<b>Website content filtering:</b> Blockieren Sie ganze Kategorien unangemessener, verdächtiger und bösartiger Websites				•

**Kompletter Schutz in einem einzigen Paket zu einem sinnvollen Preis.  
Rufen Sie noch heute an, um loszulegen.**



[www.malwarebytes.com/business](http://www.malwarebytes.com/business)



[corporate-sales@malwarebytes.com](mailto:corporate-sales@malwarebytes.com)



1.800.520.2796