

# THREATDOWN ELITE

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-/Sicherheitssteams sind unterbesetzt:** 62 % der Unternehmen verfügen nicht über genügend Personal für Cybersicherheit<sup>5</sup>

### THREATDOWN ELITE – VORTEILE

Speziell für Unternehmen mit begrenzten Ressourcen entwickelt, **Elite** bietet umfassenden Schutz in einer einzigen Lösung, die beispiellose Benutzerfreundlichkeit zu einem sinnvollen Preis bietet.

#### Sicherheit verbessern

- **24x7x365 endpoint monitoring and response** von unserem Team von Cybersicherheitsexperten mit 150 Jahren Erfahrung in den Bereichen Bedrohungssuche, forensische Analyse und Reaktion auf Vorfälle
- **Angriffserkennung** durch preisgekrönte Technologie mit Überwachung verdächtiger Aktivitäten, Freeform-Bedrohung Jagd und Ransomware-Rollback
- **Beschleunigte Reaktion** durch patentierte Technologie, die kontinuierlich Warnungen scannt und nur die kritischsten eskaliert, auf die unser Team in Ihrem Namen reagieren kann
- **Threat prevention** mit Multi-Vektor-Schutz, der Ihre Geräte nicht verlangsamt
- **Reduzierung der Angriffsfläche** durch Schwachstellen-Scans und automatisiertes Patching
- **Application blocking** So verhindern Sie, dass nicht autorisierte Programme auf Endpunkten ausgeführt werden
- **Sicherheit, die mit zunehmendem Alter nur noch besser wird**, da unser Expertenteam auf der Grundlage der gewonnenen Erkenntnisse die Sicherheitstechniken verfeinert, um im Laufe der Zeit schnellere und präzisere Erkennungen und Warnungen zu ermöglichen

## 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 die meisten ausführbaren Malware-Dateien und die damit verbundenen Artefakte, Änderungen und Prozessänderungen findet und automatisch entfernt
- **Security Operations Center (SOC) in einer Box** mit unseren Technologien, die von unseren Experten verwaltet werden, um die Bemühungen Ihres Teams zu verstärken

## 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, ein SOC und einen vertrauenswürdigen Partner

## THREATDOWN ELITE – FEATURES

- **Managed Detection and Response:** 24x7x365-Überwachung durch unsere Experten, die in Ihrem Namen Bedrohungen analysieren, darauf reagieren und sie beheben (auch solche, die sich der technologischen Erkennung entziehen)
- **Endpoint Detection and Response:** Preisgekrönte Lösung, die eine kontinuierliche aktive Erkennung bietet und Reaktion, Überwachung verdächtiger Aktivitäten, integrierte Cloud-Sandbox und Ransomware-Rollback
- **Managed Threat Hunting:** Automatisiertes Scannen von Warnmeldungen, das EDR-Daten mit externen und internen Bedrohungsdaten-Feeds korreliert, Bedrohungen priorisiert und die kritischsten mit klaren, schrittweisen Reaktionsanleitungen eskaliert
- **Endpoint Protection:** Defense-in-Depth-Prävention, die signaturbasierte, dateilose und Zero-Day-Angriffe stoppt bevor sie Ihr System 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 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
- **31-day lookbacks** von unserem Expertenteam, das nach Kompromittierungsindikatoren sucht, um Angriffe zu stoppen und Optimieren Sie Erkennungen und Warnungen in Zukunft

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

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

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

<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