DATENBLATT

THREATDOWN | ELOVADE

ENDPOINT PROTECTION

Leistungsstarker Schutz vor Schadsoftware für Endpunkte. Entwickelt für Unternehmen jeder Größe.

Heutzutage werden selbst einfache Schadsoftware-Angriffe automatisiert durchgeführt, sodass Cyberkriminelle mit wenigen Ressourcen ausgeklügelte Attacken auf Unternehmen jeder Größe durchführen können. Um sich dagegen zu wehren, setzten Unternehmen mehrere mehrschichtige, aber isolierte Endpunkt-Sicherheitslösungen ein, die von Bedrohungsakteuren bald überwunden wurden, indem sie die Lücken dazwischen ausnutzten. Diese sich gegenseitig bedingenden Trends bedeuten, dass es noch nie einen größeren Bedarf an einem einheitlichen, umfassenden Ansatz für den Endpunktschutz gab, der stark genug ist, um fortschrittliche Angriffe abzuwehren, aber auch flexibel genug, um sich an die Bedrohungslandschaft anzupassen.

Lernen Sie Endpoint Protection für Server kennen, eine umfassende Lösung zum Schutz vor und zur Beseitigung von Schadsoftware mit vorausschauender Erkennung und proaktivem Blockieren von Bedrohungen sowie integriertem End-to-End-Schutz. Endpoint Protection wird aus der Cloud über eine zentrale Konsole gesteuert und bietet flexible Verwaltung und Geschwindigkeit für Unternehmen jeder Größe.

Umfassender Schutz, der auf Geschwindigkeit ausgelegt ist

Schnelle Bereitstellung, verbesserte Produktivität der Endbenutzer

Präzise Erkennung am Ort des Angriffs

Innovativer, fortschrittlicher Endpunktschutz

Skalierung zur Bekämpfung wachsender Bedrohungen

Von eine zentralen Konsole aus einfach zu implementierende Sicherheitslösung

Entdecken Sie die Vorteile

Umfassender Schutz, der auf Geschwindigkeit ausgelegt ist

Agent mit leistungsorientierter Architektur
Viele Sicherheitsplattformen für Endgeräte stopfen Endgeräte mit einem ständig wachsenden Bestand an Malware-Signaturen voll und verlangsamen die Leistung mit Brute-Force-Scan-Algorithmen. Im Gegensatz dazu verwendet ThreatDown einen einzigen, ressourcenschonenden Agent, der bösartigen Code schnell aufspürt und blockiert, ohne die Leistung Ihrer Windows-, Mac- oder Linux-Rechner zu beeinträchtigen.

Umfassender Web-Schutz
Unsere Web-Schutztechnologie verhindert proaktiv, dass Benutzer auf bösartige Websites, Malvertising, Scammer-Netzwerke und verdächtige URLs hereinfallen oder potenziell unerwünschte Programme und Änderungen herunterladen.

Abgesicherte Geräte und Anwendungen
ThreatDown schützt Ihre Geräte, indem es Exploits blockiert, die Ausführung von Remote-Code verhindert und die Kommunikation mit feindlichen Schadsoftware-Servern unterbricht, um die Angriffsfläche für Ihr Unternehmen drastisch zu verringern.

Verhaltensbasierte Blockierung
Unsere verhaltensbasierte Analyse identifiziert unverkennbar feindliche Aktivitäten nahezu in Echtzeit und blockiert die Bedrohung automatisch, sodass der proaktivste Schutz auf dem Markt geboten wird.

Zero-Day-Prävention
ThreatDown wendet eine signaturlose Nutzdatenanalyse und Anomalieerkennung an, um proaktiv Schadsoftware, Schwachstellenausnutzungen und Infektionen von USB-Peripheriegeräten zu identifizieren und zu blockieren, damit sie Ihrer Umgebung keinen Schaden zufügen.

Präzise Erkennung am Ort des Angriffs

Die richtige Art des maschinellen Lernens
Anstatt auf Schadsoftware zu trainieren, wird das ThreatDown-Modell darauf geschult, „Goodware“ zu erkennen – ordnungsgemäß signierten Code von bekannten Anbietern. Das Ergebnis sind vorausschauende Schadsoftware-Vorhersagen, die immer schneller und präziser werden. Außerdem testen wir in allen Phasen auf bösartigen Code und Fehlverhalten. Verdächtiger Code wird aus der Entfernung untersucht, ohne die Produktivität der Endbenutzer zu beeinträchtigen.

Schnellste Bedrohungsanalyse auf dem Markt
Profitieren Sie von den Erkennungs- und Abhilfemaßnahmen, die ThreatDown auf Millionen von geschützten Endgeräten in Unternehmen und bei Privatanwendern durchführt. Selbst brandneue, nicht identifizierte Schadsoftware wird in der Regel beseitigt, bevor sie sich auf Ihre Endgeräte auswirken kann.

Einheitlicher Erkennungstrichter fängt mehr Bedrohungen ab
ThreatDown verwendet Funktionen zur Verhaltensüberwachung und Lernalgorithmen, um ein Profil der Bedrohungen in den Bereichen Web, Speicher, Anwendungen und Dateien zu erstellen. Aufeinanderfolgende Lernvorgänge entlang des Erkennungstrichters sorgen für immer höhere Erkennungsraten und weniger Fehlalarme.

Verfolgt die Infektion, kartiert die Entfernung
Die Linking Engine verfolgt jede Installation, Änderung und Prozessinstanziierung – einschließlich speicherinterner ausführbarer Dateien,

die von anderen Anti-Schadsoftware-Paketen übersehen werden – und zeichnet so ein vollständiges Bild der Bedrohung auf, was eine umfassende Abhilfe ermöglicht.

Gründlichste „One-and-done"-Bereinigung
ThreatDown nutzt die detaillierten Erkenntnisse der Linking Engine, um sowohl die Infektion als auch alle Artefakte „in einem Aufwasch" gründlich und dauerhaft zu entfernen.

Skalierung zur Bekämpfung wachsender Bedrohungen

Vollständige Endpunktsicherheit, von einer einzigen Konsole aus zentral gesteuert
Mit unserem Komplettpaket von Endpunktsicherheitsfunktionen und Automatisierungsmöglichkeiten, die von der Nebula Cloud-Plattform aus mit einer intuitiven Benutzeroberfläche gesteuert werden, können Sie Schadsoftware mit ein paar Klicks bekämpfen, anstatt Skripts programmieren zu müssen.

Priorisiert die Produktivität des Sicherheitsteams
Ihr Sicherheitsteam kann mit nur wenigen Klicks vom globalen Dashboard aus zu identifizierten Bedrohungen und unter Quarantäne gestellten Geräten navigieren. Das Scannen und die Beseitigung von Sicherheitslücken erfolgt automatisiert in einer Abteilung oder auf Tausenden von Geräten gleichzeitig.

Analysiert die Auswirkungen, damit Sie es nicht tun müssen
ThreatDown bietet eine ausführliche Bedrohungsanalyse mit einer Bewertung der potenziellen Auswirkungen. Ihr CISO kann so Zeit sparen und mögliche Auswirkungen wirksam an die Geschäftsleitung kommunizieren.

Skalierbar bis zum größten Unternehmen
Unsere Lösung nutzt die Leistungsfähigkeit der Cloud, um selbst den Anforderungen der größten Unternehmen gerecht zu werden, fortschrittliche Bedrohungen effizient zu erkennen und eine weltweit einheitliche und schnelle Reaktion zu ermöglichen.

ELOVADE

Kontaktdaten für Deutschland & Österreich:

ELOVADE Deutschland GmbH
malwarebytes@elovade.com
DE: +49 6441 67118 842
AT: +43 820 0010 36
elovade.com/malwarebytes

Kontaktdaten für die Schweiz:

ELOVADE Swiss AG
sales@elovade.ch
CH: +41 55 552 27 92
elovade.ch/malwarebytes