THREATDOWN | ELOVADE

LÖSUNGSBESCHREIBUNG

ENDPOINT DETECTION AND RESPONSE

Erkennung, Isolierung und Behebung von Problemen für Unternehmen für Windows, Mac und Linux

ÜBERBLICK

In einem aktuellen Forschungsbericht des Ponemon Institute berichteten 68 Prozent der Befragten von einem oder mehreren schädlichen Endpunktangriffen, die wertvolle Informationen oder die Infrastruktur gefährdeten. Ähnliche Untersuchungen zeigen, dass auf fast 60 Prozent der Endgeräte versteckte Bedrohungen zu finden sind, darunter schädliche Trojaner, Rootkits und Backdoors. Diese Bedrohungen sind ausgeklügelt, hartnäckig und entgehen oft selbst dem besten Endpunktschutz, weshalb mehr als die Hälfte aller Unternehmen berichten, dass sie nicht in der Lage sind, hochentwickelte Angriffe effektiv zu erkennen und zu bekämpfen.

Ebenso besorgniserregend sind die jüngsten Änderungen der Compliance-Vorschriften, die einen strengeren Schutz personenbezogener Daten (PII) vorschreiben. Die Richtlinien des New York Department of Financial Services (NYDFS) und des California Consumer Privacy Act (AB 375) gehören zu den strengsten, aber die meisten US-Bundesstaaten haben inzwischen strengere Richtlinien. Wenn Sicherheitsteams nicht nachweisen können, dass es sich bei „Fehlalarmen“ nicht um tatsächliche Bedrohungen oder Angriffe handelt, könnten ihre Firmen zu Geldstrafen verurteilt, zu öffentlichen Bekanntmachungen gezwungen und von Generalstaatsanwälten oder privaten Parteien verklagt werden. Auf internationaler Ebene stellen die neue Datenschutzgrundverordnung (DSGVO) und die Zahlungsdiensterichtlinie 2.0 (PSD2) ebenfalls eine Herausforderung dar.

Unternehmen müssen in der Lage sein, bekannte und unbekannte Bedrohungen sofort zu erkennen, aktiv und in Echtzeit zu reagieren sowie gründlich zu isolieren und zu untersuchen. Sollten Daten verloren gehen oder für Erpressungsversuche benutzt werden, müssen Unternehmen in der Lage sein, den schädlichen Code beseitigen, einen Rollback durchführen und die Daten wiederherstellen, und das schnell und vollständig.

EDR-HERAUSFORDERUNGEN

Doppelt so viele Angriffe

Über 68 % der Unternehmen waren in letzter Zeit von Angriffen betroffen, und bei 80 % handelte es sich um neue „Zero-Day“-Bedrohungen.

Hohe Anzahl an Fehlalarmen

Fast 60 % der Unternehmen benötigen eine Zero-Day-Erkennung, aber die hohe Zahl der Fehlalarme ist ein großes Problem.

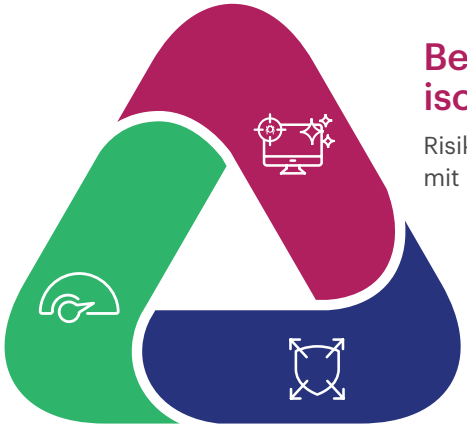
Komplexe Lösungen

Mehr als 61 % der Unternehmen geben an, dass die Komplexität und das begrenzte Personal eine große Herausforderung für die EDR darstellen.

Quelle: EDR-Studie 2020, Ponemon Institute

Schnelle Bereitstellung und einfache Verwaltung

Bereitstellung innerhalb von Minuten und Verwaltung über eine intuitive cloudbasierte Konsole



Bedrohungen erkennen, isolieren und beheben

Risiken und Fehlalarme reduzieren; Bedrohungen mit mehreren Isolationsmodi stoppen

Bedrohungsjagd und Ransomware-Rollback

Geführte Bedrohungssuche und Windows-Ransomware-Rollback

EINFACH

Endpoint Detection and Response (EDR) für Windows, Mac und Linux kann andere Sicherheitslösungen für Endgeräte, einschließlich Microsoft Defender, problemlos ersetzen oder ergänzen. Wir haben eine hohe Kundentreue und viel Lob erhalten, weil unsere Lösung unterbrechungsfrei, einfach und kostengünstig über einen einzigen Endpunkt-Agent bereitgestellt werden kann und weil wir eine robuste Integration und Kompatibilität garantieren.

- Unterbrechungsfrei, Einsatz innerhalb von Minuten
- Ein Endpunkt-Agent, einfache Integration
- Intuitive cloudbasierte Verwaltungskonsole

EFFEKTIV

EDR verwendet einzigartige Lernalgorithmen zur Anomalieerkennung, um proaktiv webbasierte Angriffe, Zero-Day-Malware, Ransomware, potenziell unerwünschte Programme oder Modifikationen (PUPs und PUMs) sowie Infektionen von USB-Peripheriegeräten zu erkennen.
EDR zeichnet sich durch eine höhere Genauigkeit aus, weshalb wir eine der niedrigsten Fehlalarmraten der Branche haben. Unsere granularen Isolationsfunktionen verhindern die laterale Verbreitung von Angriffen, indem sie einzelne Computer, Subnetze oder Gruppen eindämmen und aktive Reaktionsmaßnahmen fortsetzen.

- Erkennt „Zero-Day"-Bedrohungen und löst dabei weniger Fehlalarme aus
- Granulare Isolierung für Prozesse, Netzwerke und Windows-Desktops
- Entfernt ausführbare Dateien, Artefakte und Änderungen

EEFFIZIENT

EDR hat eine Ransomware-Rollback-Funktion für Windows und verwendet zur Vermeidung von Leistungseinbußen einen ressourcenschonenden Agent, der nur drei Hintergrundprozesse benötigt (viel weniger als andere Lösungen).

- Ein einziger ressourcenschonender Agent, keine Auswirkungen auf die Leistung
- 72-Stunden-Rollback von Ransomware für Windows
- Niedrige Gesamtbetriebskosten (TCO)

INTEGRIERTER PROAKTIVER ENDPUNKTSCHUTZ

EDR bietet einen integrierten Endpunktschutz und automatisierte adaptive Erkennungstechniken, die in jeder Phase der Bedrohungserkennung dazulernen. Im Gegensatz zu reaktiveren, signaturbasierten Lösungen, die erst eingreifen, wenn eine Schadsoftware ausgeführt wird, blockiert unser Endpunktschutz Bedrohungen, bevor Geräte infiziert werden. EDR erkennt und verhindert proaktiv und präzise sowohl schädlichen Code als auch verdächtiges Verhalten.

BETRIEBSSYSTEMSPEZIFISCHE ISOLATIONSMODI

EDR ist die erste Lösung, die mehrere Modi zur Endpunktisolierung kombiniert. Wenn ein Endpunkt angegriffen wird, können Sie die Ausbreitung von Malware und die Entstehung von Schäden leicht verhindern. Die Ausfallzeiten für IT und Benutzer können so minimiert werden.

- Die **Netzwerkisolierung** schränkt die Gerätekommunikation ein, damit Angreifer ausgesperrt werden und die Schadsoftware nicht „nach Hause telefonieren" kann.
- Die **Prozessisolierung** schränkt ein, welche Vorgänge ausgeführt werden können, um Schadsoftware zu stoppen, während die Benutzer weiterhin produktiv arbeiten können.
- Die **Desktop-Isolierung** für Windows-Workstations warnt Benutzer vor Bedrohungen und blockiert vorübergehend den Zugriff, während das Gerät zur Analyse online bleibt.

AUTOMATISIERTE UND GRÜNDLICHE BESEITIGUNG VON SCHADSOFTWARE

Unser automatisierter Ansatz ermöglicht es IT- und Sicherheitsanalysten, den manuellen Aufwand zur Behebung von Angriffen zu eliminieren und so wertvolle Zeit zu sparen. Typische Schadsoftware-Infektionen können mehr als 100 Artefakte hinterlassen, darunter Dateien, Ordner und Registrierungsschlüssel, die sich auf andere Systeme im Netzwerk eines Unternehmens ausbreiten können. Die meisten Lösungen beseitigen nur aktive Schadsoftwarekomponenten, wie z. B. ausführbare Dateien, wodurch die Systeme einer erneuten Infektion ausgesetzt sind.

Die geschützte Linking Engine erkennt und entfernt dynamische und verwandte Artefakte, Änderungen und Prozessveränderungen. Unsere Engine wendet die sogenannte verbundene Sequenzierung an, um eine gründliche Beseitigung von Schadsoftware-Persistenzmechanismen sicherzustellen.

SANDBOX IN DER CLOUD

Um die Präzision unserer Bedrohungserkennung zu erhöhen, verwendet ThreatDown eine „Sandbox" in der Cloud, eine Art virtueller Zellenblock, in dem potenziell schädliche Malware zur Bewertung und Analyse isoliert und zerstört wird.

Mit der Sandbox können Sie verdächtigen Code sogar aus der Ferne untersuchen, ohne die Produktivität der Endbenutzer zu beeinträchtigen. Nach der Analyse liefert ThreatDown einen umfassenden Bericht, damit Sie angemessen auf Kompromittierungsvorfälle (IoCs) reagieren können.

GEFÜHRTE BEDROHUNGSJAGD

Die intuitive grafische Benutzeroberfläche ähnelt einer Kanban-Tafel, auf der die Aktionen in übersichtlicher Form automatisch in das MITRE ATT&CK-Framework eingeordnet werden. Außerdem werden Erklärungen angezeigt, warum unser Lernalgorithmus die verdächtige Aktivität identifiziert hat, die Ihre Aufmerksamkeit erfordert. Darüber hinaus bieten wir eine detaillierte Ansicht für den forensischen Analysten, der die genaue Abfolge der Aktionen und ausgegebenen Befehle benötigt, um Ihnen die erforderlichen IoCs zu liefern.

Außerdem können Sie von der Benutzeroberfläche aus in das Unterfenster für die Überwachung auf verdächtige Aktivitäten, den Flight Recorder Search (FRS), wechseln, ohne den Überblick zu verlieren. Die Flight Recorder-Suche ist eine Funktion, die Sie in einer grafischen Benutzeroberfläche systematisch durch die Suche nach Breadcrumbs/Hinweisen auf allen verwalteten Endpunkten in Ihrem Unternehmen führt, um frühe Anzeichen eines Bedrohungsakteurs zu erkennen, der sich seitwärts bewegt.

WINDOWS RANSOMWARE-ROLLBACK

Auf Windows-Plattformen gehört zur EDR eine einzigartige 72-Stunden Ransomware-Rollback-Technologie, mit der Sie die Uhr sprichwörtlich zurückdrehen und Ihr Unternehmen schnell wieder in einen funktionsfähigen Zustand versetzen können. ThreatDown kann mit dem Rollback alle Dateien in ihrem ursprünglichen Zustand wiederherstellen, bevor sie durch einen Ransomware-Angriff verschlüsselt, gelöscht oder verändert wurden. Und keine Sorge: Unsere firmeneigene Datenspeichertechnologie minimiert den Platzbedarf für die Sicherung Ihrer Daten.

KONTINUIERLICHE ÜBERWACHUNG

Die Flight-Recorder-Suchfunktion in EDR ermöglicht eine kontinuierliche Überwachung und Transparenz für Windows und Mac, um aussagekräftige Erkenntnisse zu gewinnen. Dazu gehören Suchfunktionen für Dateinamen, Netzwerkdomänen, IP-Adressen, MD5-Hashes und Datei-/Prozesspfade oder -namen. Außerdem können Sie verdächtige Aktivitäten automatisch anzeigen lassen, die vollständigen Befehlszeilendetails der ausgeführten Prozesse einsehen und dreißig Tage lang rollierende Daten in der Cloud speichern.

SCHWACHSTELLEN- UND PATCH-MANAGEMENT

Unser Modul zur Schwachstellenbewertung fügt sich nahtlos in die Reihe der Präventionstools unserer EDR-Lösung ein und bietet die gleiche Transparenz. So können Sie Ihre Abwehrkräfte innerhalb derselben cloudbasierten Sicherheitsplattform stärken. Anhand einer aktuellen Bestandsaufnahme Ihrer Software, Treiber und Betriebssysteme identifiziert das Modul bekannte Softwareschwachstellen, d. h. Bereiche, die Bedrohungsakteure nutzen könnten, um sich Zugang zum Netzwerk zu verschaffen. Anschließend werden die empfohlenen Maßnahmen auf der Grundlage des Risikograds der ermittelten Schwachstellen nach Prioritäten geordnet. Patch-Management kontrolliert den Software-Patching-Prozess. In Kombination mit unserem Modul zur Schwachstellenbewertung beschleunigt das Patch-Management-Modul die Identifizierung, Bereitstellung, Installation und Überprüfung von notwendigen Aktualisierungen von Windows-Endpunkt- und -Server-Betriebssystemen sowie einer Vielzahl von Drittanbieteranwendungen.

DNS-FILTERUNG

Das DNS-Filtermodul von ThreatDown verhindert, dass Benutzer vor Ort und an anderen Standorten auf ungeeignete Webinhalte oder schädliche Websites zugreifen können, und es unterstützt Sie bei der Durchsetzung der Verhaltensrichtlinien Ihres Unternehmens. Darüber hinaus verschlüsselt unser DNS-Filtermodul alle Domain-Namensanfragen, um die Mittel zu verringern, mit denen Bedrohungsakteure Websites und webbasierte Anwendungen ausnutzen. Um das Risiko weiter zu reduzieren, wird unsere DNS-Filterung durch den Echtzeitschutz von ThreatDown vor bösartigen Downloads unterstützt.

MANAGED DETECTION AND RESPONSE (MDR)

ThreatDown bietet auch für Unternehmen mit begrenzten Ressourcen für die Cybersicherheit eine MDR-Lösung (Managed Detection and Response) an. Mit MDR wird Ihre Umgebung durch EDR geschützt, und unser Team von Cybersicherheitsexperten mit jahrzehntelanger Erfahrung überwacht Ihre Umgebung rund um die Uhr, um die von EDR generierten Warnmeldungen in Echtzeit zu untersuchen. Darüber hinaus beseitigt unser MDR-Team Bedrohungen oder gibt Ihrem Team Anleitungen zur Beseitigung von Schadsoftware, sodass Ihre IT- und Sicherheitsteams mehr Zeit für andere, dringendere Projekte zur Verfügung haben.

HOHE INVESTITIONSRENDITE, NIEDRIGE GESAMTBETRIEBSKOSTEN

Mit unserer cloudgestützten Lösung lässt sich EDR problemlos skalieren, um zukünftigen Anforderungen gerecht zu werden. Dank unseres Fachwissen im Bereich der Cyberintelligenz und der Beseitigung von Schadsoftware können wir Ihnen eine Lösung anbieten, die auf den Bedrohungsdaten von Millionen Endgeräten basiert, die von ThreatDown geschützt werden – sowohl von Unternehmen als auch von Privatanwendern. Die ThreatDown-API ermöglicht eine einfache Integration mit SIEM, SOAR, ITSM usw., um die Automatisierung und Kompatibilität weiter voranzutreiben. EDR garantiert eine hohe Investitionsrentabilität (ROI) und niedrige Gesamtbetriebskosten (TCO). Darüber hinaus sind wir für unseren hervorragenden Service und Support bekannt.

IHRE SICHERSTE WAHL FÜR EDR

Endpoint Detection and Response der Enterprise-Klasse für Windows-, Mac- und Linux-Plattformen erkennt verdächtige Aktivitäten effektiv und effizient, isoliert Angriffe, untersucht Bedrohungen und behebt Schäden.

Andere Lösungen können schwierig zu implementieren und zu verwalten sein und sind in der Regel nicht mit anderer Sicherheitssoftware wie Microsoft Defender kompatibel. Viele andere EDR-Lösungen entfernen lediglich ausführbare Dateien und bieten keine mehrschichtige Isolierung, um Bedrohungen zu stoppen, bevor diese Schaden anrichten können. Außerdem sind sie so konzipiert, dass sie bei fast jeder Bedrohung Alarm schlagen, was zu einer hohen Anzahl an Fehlalarmen führt.

EDR lässt sich nahtlos in die meisten anderen Sicherheitslösungen für Endgeräte integrieren und ist mit diesen kompatibel, einschließlich Microsoft Defender. Unsere Lösung ist über unsere cloudbasierte Nebula-Konsole einfach zu implementieren und zu verwalten. Wir erkennen verdächtige Aktivitäten und isolieren Prozesse und Netzwerke, um den Schaden zu begrenzen. Die Desktop-Isolierung ist auch für Windows-Workstations verfügbar. ThreatDown geschützte Linking Engine entfernt Artefakte, Änderungen und Prozessveränderungen und bietet ein einzigartiges 72-Stunden Ransomware-Rollback für Windows-Workstations. EDR für Windows, Mac und Linux verwendet einen einzigen ressourcenschonenden Agent, der die Leistung nicht beeinträchtigt.

Warten Sie nicht, bis es zu spät ist. ThreatDown ist Ihre sicherste Wahl für Windows-, Mac- und Linux-EDR. Wir haben eine hohe Kundenbindung und bekommen viel Lob für unsere EDR-Lösung für Unternehmen, da sie effektiv, intuitiv und umfassend ist.

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