radware

OTD BİLİŞİM
www.onlineteknikdestek.com

DefensePro, das preisgekrönte Echtzeit-Umweltschutzgerät von Radware, schützt Unternehmen vor neuen Netzwerkangriffen mit mehreren Vektoren, mächtigen DDoS-Angriffen und IoT-Botnets, Ausnutzung von Anwendungsschwachstellen, Malware und anderen Arten von Cyberangriffen. Mit seiner bewährten verhaltens-basierten Technologie ist DefensePro darauf ausgelegt, die Oberhand gegen moderne, ausgeklügelte Angriffstools und Cyberkriminelle zu gewinnen.

AUTOMATISCHE VERTEIDIGUNG GEGEN ZERO-DAY ANGRIFFE

Verhaltensbasierte Erkennung und Minderung zur Verteidigung gegen unbekannte Zero-Day-Angriffe, ohne die legitime Benutzererfahrung zu beeinträchtigen.

SCHLÜSSELLOSE SSL/ TLS-FLUTMINDERUNG

Schlüsselloser-Schutz mit hoher Kapazität vor SSL/TLS-basierten DDoS-Angriffen, ohne die Kundenkommunikation zu beschleunigen und die Privatsphäre der Benutzer zu schützen.

ERWEITERTER ANGRIFFSSCHUTZ

Erkennung und Minderung der modernsten Angriffe von heute, einschließlich Burst-Angriffe, Domain Name System/DNS) Verstärkungsangriffe, IoT-Botnet-Floods, Layer 3-7 und andere beeinflussende DDoS-Angriffe.

PATENTGESCHÜTZTE ECHTZEIT-ANGRIFFSSIGNATUR

Automatische Signaturerstellung und erweiterte Effekt-Upgrades um die höchste Abschwächungsgenauigkeit zu erreichen, die unbekannte Angriffe automatisch mindern und die Auswirkungen auf legitimen Datenverkehr minimieren kann.

WIE HÄLT RADWARE IHRE NETZWERKELEMENTE SICHER?

SPEZIELLE DDOS-MINDERUNGSHARDWARE

Ein spezielles DefensePro-Hardwaremodul, mit dem Angriffe gemindert werden können, ohne den legitimen Datenverkehr und die Benutzererfahrung zu beeinträchtigen, selbst bei großen Angriffen.

ANALYTIK UND BERICHTE

Die Verwaltungsplattform von Radware bietet Warnungen, Berichte, Forensik und Einblicke für Verweigerung des Dienstes und für Angriffen auf Webanwendungen, sowohl für historische Daten als auch in Echtzeit.

VERTEIDIGUNGSNACHRICHTEN

Zur Verbesserung der Reaktion und Genauigkeit der Erkennung und Minderung, synchronisiert Angriffsinformationen und Grundlinien über verschiedene Elemente dieser Lösung hinweg.

UNSERES OTD KATALOG

SPEZIELLE DDOS-MINDERUNGSHARDWARE

Ein spezielles DefensePro-Hardwaremodul, mit dem Angriffe gemindert werden können, ohne den legitimen Datenverkehr und die Benutzererfahrung zu beeinträchtigen, selbst bei großen Angriffen.

Breitestes Angriffsspektrum

- Vollständiger Layer 3-7-Schutz gegen bekannte und Zero-Day-DoS/DDoS-Angriffe, die Netzwerkbandbreite, Server- und Anwendungsressourcen missbrauchen.
- Zwei-Wege-Sichtbarkeit zur Verteidigung gegen die ausgeklügeltsten Angriffe, bei denen sowohl der eingehende als auch der ausgehende Datenverkehr untersucht werden müssen.
- Mit Signaturerstellung und sofortiger Durchsetzung für die schnellste Behebung bietet der Schutz vor Burst-Angriffen eine sofortige verhaltensbasierte Erkennung und Minderung einer der wichtigsten Bedrohungen von heute.
- Um den kostengünstigsten Schutz vor bekannten und unbekannten DNS-Flood-Angriffen zu bieten, einschließlich DNS-Water Torture Angriffen, erweiterte DNS-Angriffsumfang, die erstklassige verhaltensbasierte Algorithmen nutzt.
- Eine zustandslose und schlüssellose Lösung zur Minderung von SSL/TLS-Angriffen mit Patentschutz, die vor jedem verschlüsselten Angriff ohne Paketentschlüsselung und reduzierter Latenz für eine hohe Schutzkapazität schützt.

Mehrere Verteilungsoptionen nach Ihren Bedürfnissen

- Es unterstützt Sowohl Inline- als auch Offroad-Anwendungen (SmartTap) oder eine Datenbereinigung-Zentrum-Bereitstellung.
- Integriert in den Radware Hybrid-Cloud-DDoS-Schutzdienst bietet eine Hybridlösung von einem einzigen Anbieter, die keine Zeit bis zur Beseitigung bietet.
- Mit Multi-Mieter- und Multi-Politik-Unterstützung ermöglicht es Dienstanbietern, marktführende DDoS-Minderungsdienste für entsprechende Anwendungen und Netzwerkmandanten bereitzustellen.
- Virtuelles Gerät bietet DDoS-Minderung für softwaredefinierte Rechenzentren (SDDC).
- Sortiment an Schutzvorrichtungen bietet eine Minderungskapazität von 6 Gbit/s bis 400 Gbit/s.

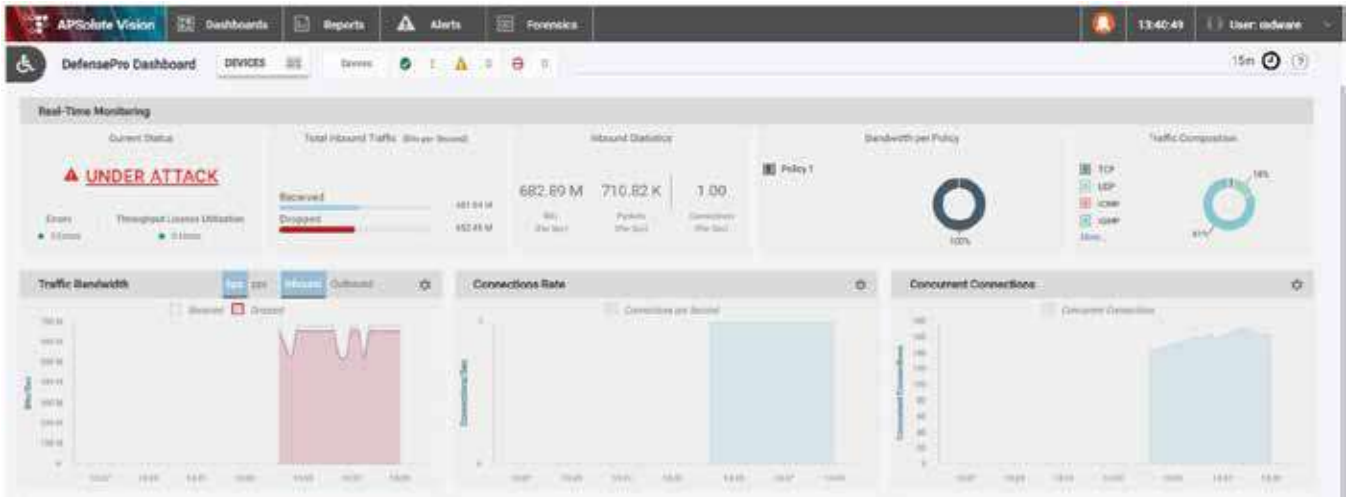

Abbildung 1: Ein zentrales Dashboard, das Bedrohungen in Echtzeit anzeigt und Drilldown-Kapazität, die einen besseren Einblick in spezifische Angriffsdaten und -merkmale bietet