Sektörün En Gelişmiş DDoS Koruması

Dağıtılmış Hizmet Reddi (DDoS) saldırıları giderek daha sık, güçlü ve karmaşık hale gelmektedir. Saldırı araçlarının çevrimiçi ortamda daha yaygın hale gelmesiyle, potansiyel saldırı havuzu her zamankinden daha büyük hale gelmiştir. Radware Cloud DDoS Protection Service, ağ katmanı (L3/4) ve uygulama katmanı (L7) saldırılarına karşı gelişmiş davranış tabanlı algılama, gerçek zamanlı otomatik imza oluşturma (sıfır gün saldırılarına karşı koruma), benzersiz SSL DDoS koruması ve her müşterinin ihtiyaçlarına uygun esnek bulut tabanlı veya hibrit dağıtım seçenekleri ile kurumları korur.

En Üst Düzey DDoS Koruması

Davranış tabanlı algılama, otomatik imza oluşturma ve benzersiz SSL saldırı azaltma ile tüm olası tehditlere karşı kapsamlı DDoS koruması.

Endüstri Lideri SLA

Gelişmiş otomasyon ve önceden tanımlı iş akışları sayesinde algılama, uyarı, yönlendirme ve azaltma taahhüdü. Görünürlük ve kontrol için ek hizmetler ve metriklerin geniş bir seti.

Kesintisiz Dağıtım Modları

İsteğe bağlı (On-Demand), Her zaman açık (Always-On) ve Hibrit (Hybrid) dağıtım modelleri; müşteri ihtiyaçlarına, ağ topolojisine veya tehdit profiline benzersiz şekilde uyarlanır.

Yanınızdaki Uzmanlar

Acil Müdahale Ekibi (ERT): En iyi uygulamalar, stratejiler ve uyarılar için odak noktası olarak hizmet veren DDoS koruma uzmanı, her türlü saldırı süresince kurumunuza destek sağlar.

Quadrant Knowledge Solutions SPARK MATRIX: DDoS Mitigation, Q2, 2024 LEADER

Quadrant Knowledge Solutions SPARK MATRIX: DDoS Mitigation, 2023 LEADER

FORRESTER® WAVE LEADER 2021 DDoS Mitigation Solutions

IDC Analyze the Future

İhtiyaçlarınıza En Uygun Çözümü Belirleyin

İsteğe Bağlı	Her Zaman Açık	Hibrit
Normal trafik döneminde ek gecikme yoktur; trafik yalnızca saldırı tespit edildiğinde yönlendirilir.	Her zaman aktif, gerçek zamanlı bulut tabanlı DDoS koruması sağlar.	Şirket içi cihazları, bulut tabanlı temizleme kapasitesiyle birleştirir.
En düşük maliyetli ve yalnızca bulut tabanlı basit bir dağıtım sunar.	Anında koruma sağlar; ek gecikme minimum düzeydedir.	Gerçek zamanlı koruma ve operasyon zamanında minimum gecikme sunar.
Gecikmeye duyarlı ve nadiren saldırıya uğrayan kuruluşlar için en uygun seçenektir.	Sürekli DDoS saldırısı altında bulunan bulut tabanlı uygulamalar ve kuruluşlar için idealdir.	Güvenlik açısından önerilen en iyi uygulamadır; veri merkezi koruması için en uygun çözümdür.

Küresel Kapsam, Devasa Kapasite

Radware'in Cloud DDoS Protection Service'i, 22 temizleme merkezinden oluşan küresel bir ağla desteklenir ve 15 Tbps azaltma kapasitesine sahiptir (ve artmaya devam etmektedir). Bu temizleme merkezleri Anycast tabanlı yönlendirme kullanan tam mesh modunda küresel olarak birbirine bağlıdır. Bu, DDoS saldırılarının kaynak noktasına en yakın yerde azaltılmasını sağlar ve en büyük hacimli saldırıları bile emebilen gerçek anlamda küresel bir DDoS azaltma sunar.

DDoS Mitigation Scrubbing Center

Kolay Yönetim & Kontrol

Tam Görünürlük

Tüm ilgili bilgi ve verilerin tek bir yerde toplandığı merkezi görünürlük.
Ağ yönetimine katkı sağlayan gelişmiş analitikler, ayrıntılı trafik bilgileri ve normal trafik dönemi verileri içerir.

Gelişmiş Kullanıcı Deneyimi

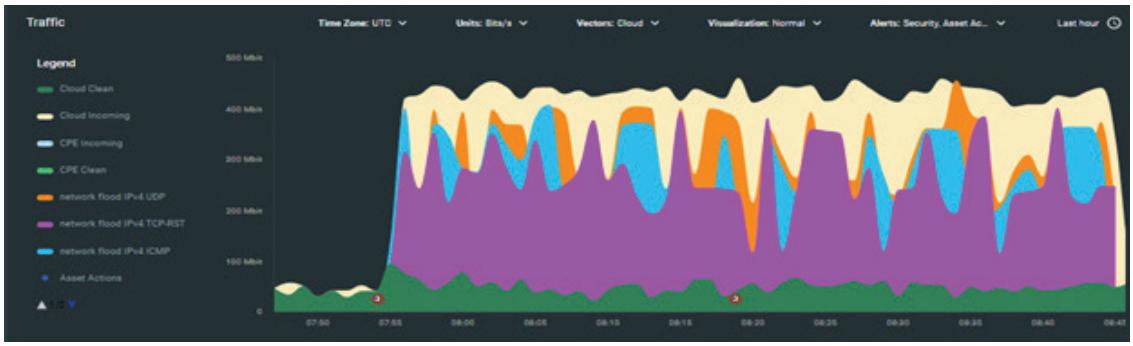
Son derece sezgisel bir grafik kullanıcı arayüzü (GUI) sayesinde, ekranlar ve arayüzler arasında gezinmek yalnızca birkaç tıklamadan ibarettir.
Karanlık mod ve normal mod, kullanıcının tercihlerine göre mevcuttur.

Saldırı Odaklı Yapı

Ağ sağlığı durumu saldırı sırasında gerçek zamanlı olarak güncellenir ve net bir göstergeyle belirtilir. Bir saldırı varlık ekranı, saldırı bilgilerini ayrıntılı biçimde gösterir ve kullanıcıların hızlı yanıt vermesini sağlar.

Detaylı Raporlama

Normal trafik dönemi veya saldırı anında fark etmeksizin değerli raporlar ve analizler sunulur. Bilgiler tek bir widget üzerinden kolayca görüntülenebilir ve ek analizler için dışa aktarılabilir.



White Glove Destek

- Uzman yönetilen hizmet, Radware'in Acil Müdahale Ekibi (ERT) aracılığıyla sağlanır.
- Saldırı öncesi uyarılar, Radware'in siber tehdit danışma kütüphanesinden alınır; bu bilgiler sürekli olarak web, darknet ve saldırı sonrası adli analizlerden toplanır.
- Adanmış Teknik Hesap Yöneticisi (TAM), yapılandırma, entegrasyon, yükseltmeler ve saldırı azaltma dahil tüm konularda odak noktası olarak görev yapar.
- Sektörün en ayrıntılı Hizmet Düzeyi Anlaşması (SLA) ile desteklenir; algılama, yönlendirme ve azaltma süreleri için detaylı taahhütler sunarak azaltmanın tutarlılığını ve genel hizmet sürekliliğini sağlar.