corero [NETWORK SECURITY]

Siber Dayanıklılık Burada Başlar.

Uyarlanabilir DDoS savunma platformu,
en kritik altyapılarınızın kesintisiz çalışmasını sağlar.

OTD BİLİŞİM
GLOBAL VAD

Corero Network Security

DDoS koruma uzmanları:

- DDoS'a odaklanan tekil uzmanlık yaklaşımı
  - 15+ yıllık DDoS deneyimi
  - Şirket içi tehdit araştırması
  - Gelirin yaklaşık %20'sinin Ar-Ge'ye yatırılması
- 7/24 Güvenlik Operasyon Merkezi
- Kişiselleştirilmiş destek

Şirket profili:

- Operasyonlar
  - Dünya Genel Merkezi: Londra, Birleşik Krallık
  - Mühendislik: Edinburgh, Birleşik Krallık
  - ABD Genel Merkezi: Marlborough, Massachusetts
- Londra Menkul Kıymetler Borsası (CNS)
- Kuzey Amerika ve Avrupa'da yaklaşık 85 çalışan

Müşterilerimiz:

- Orta ölçekli İnternet Servis Sağlayıcıları (ISP'ler)
- Hosting sağlayıcıları
- Kurum içi (on-prem) SaaS sağlayıcıları
- Yönetilen Hizmet Sağlayıcıları (MSP'ler) ve Yönetilen Güvenlik Hizmet Sağlayıcıları (MSSP'ler)
- Büyük ölçekli kurumsal şirketler

DDoS nedir?

Dağıtık Hizmet Engelleme Saldırısı

OTD BİLİŞİM
GLOBAL VAD

DDoS Saldırısı Açıklaması

Bilinçli olarak oluşturulmuş bir trafik sıkışıklığı gibi...

corero

[NETWORK SECURITY]

NEDEN GELENEKSEL YAKLAŞIMLAR BAŞARISIZ OLUR?

Sektörün Kör Noktaları

% 82	DDoS saldırılarının %90'ından fazlası 1 Gbps'in altındadır. Sadece bulut tabanlı çözümler bunları tamamen gözden kaçırır.
6 sn	Pulse saldırıları, trafik yönlendirme başlamadan önce bile sona ermiş olur. Manuel mitigasyon uygulanamaz.
% 0.5	2 Tbps'lik bir saldırıdan sızan trafik = 10 Gbps hasar. Terabit ölçeğinde "neredeyse mükemmel" koruma bile tam bir kesintidir.
50+	Tek bir kampanya içinde birden fazla saldırı vektörü bulunur. Ardışık tespit yöntemleri, aynı anda gerçekleşen 50 farklı saldırı türüne ayak uyduramaz.

DÜNYA 2025'TE DEĞİŞTİ

Her yeni rekor artık normal hale geldi

% 262
Saldırıların en yüksek boyutlarında yıllık bazda artış

2.7 Tbps
7/24 Güvenlik Operasyon Merkezi Kişiselleştirilmiş destek

12.3/gün
Müşteri başına ortalama DDoS saldırısı

6 sn
En kısa gözlemlenen saldırı dalgası

% 90.9
10 dakikadan kısa süren saldırılar

3'te 1
7 gün içinde tekrarlayan saldırılar

Corero’nun Yaklaşımı

Siber dayanıklılık için birleşik bir platform.

CORERO'YU TANITIYORUZ

Uyarlanabilir Savunma Platformu

Corero Network Security, 50'den fazla ülkede faaliyet gösteren işletmeler tarafından güvenilen, otomatik ağ güvenliği ve siber dayanıklılık çözümleri sunan küresel bir sağlayıcıdır.

GÜVENLİK

- Volumetrik DDoS
- HTTPS DDoS
- Uygulama Güvenliği
- Erişim Kontrolü
- Çıkış (Outbound) Koruması

GÖRÜNÜRLÜK

- Trafik Analitiği
- Peering Analizi
- Hizmet Erişilebilirliği İzleme
- Saldırı Analitiği
- OTT/Uygulama Trafiği

OPERASYONLAR

- Yapay Zekâ Asistanı
- Yönetilen Hizmetler
- API Entegrasyonları
- Birleşik Konsol
- Tehdit İstihbaratı

DAĞITIM

- Bulut (CORE)
- Sanal (vNTD)
- Donanım (NTD)
- SaaS (SSP/TA)
- Yazılım (BYOH)

Corero SmartWall One'u Tanıtıyoruz

Yerinde (on-prem) modüler platform

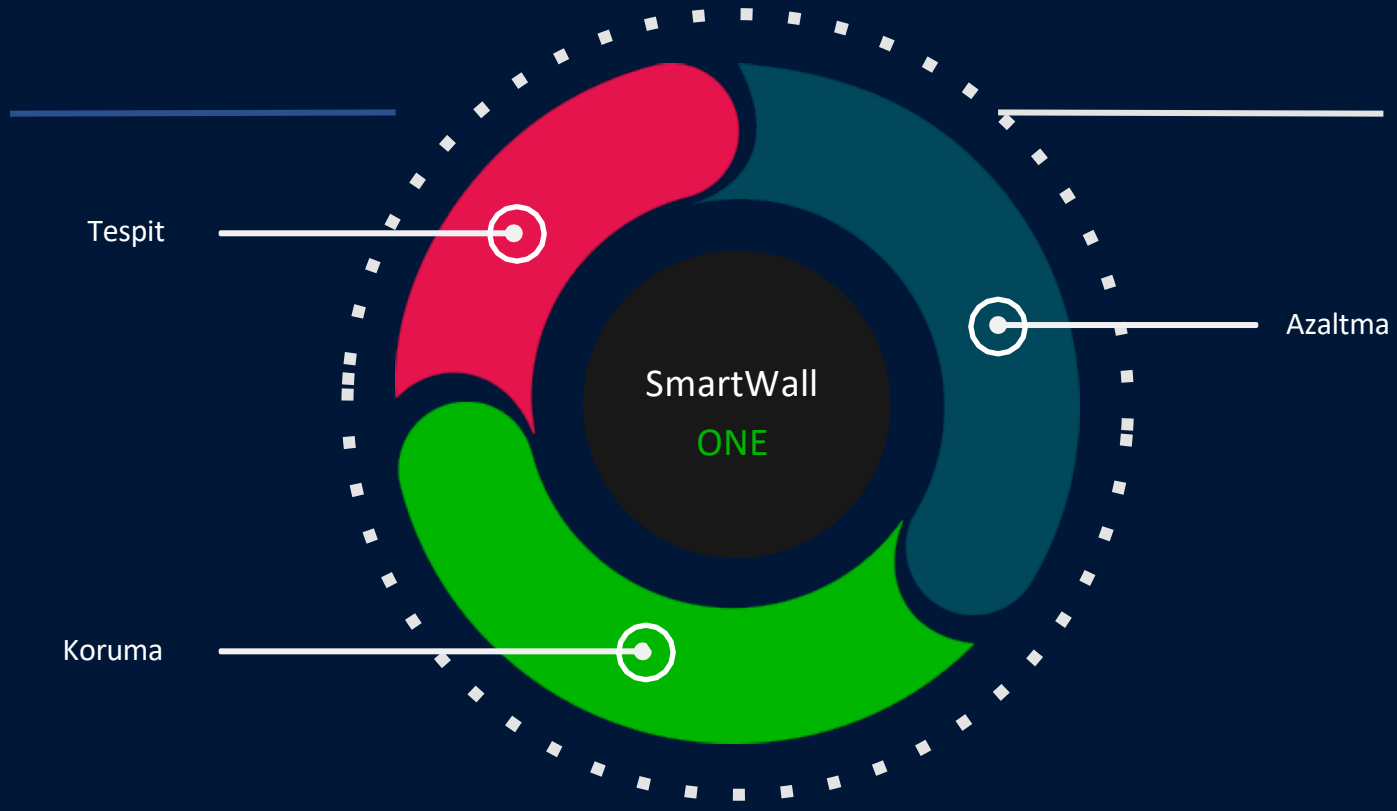
- Esnek dağıtım seçenekleri
- Donanım ve sanal cihazlar
- Mevcut altyapıyla entegrasyon sağlar

Yönetilen hizmetler ve destek

- Günlük izleme ve yönetim
- Saldırı anında destek
- Kişiselleştirilmiş destek

Katma değerli hizmetlerden gelir elde etme

- Sağlayıcı müşterileri için self-servis portal
- Hizmet olarak DDoS koruması
- Kendini finanse eden koruma
  (kendi maliyetini çıkaran koruma)



YERİNDE (ON-PREMISES) KORUMA

Inline. Her Zaman Aktif. Saniyenin Altında.

Her Zaman Aktif

Gerçek zamanlı, hat hızında inline mitigasyon. Buluta yönlendirme yok. Manuel müdahale yok. Koruma, saldırı gerçekleşmeden önce zaten hazırdır.

Tam yığın (Full-Stack)

L3'ten L7'ye kadar koruma. Volumetrik saldırılar, protokol kötüye kullanımı ve uygulama katmanı tehditleri. Hepsi tek bir geçişte ele alınır.

Gizlilik Öncelikli

Seçici TLS denetimi, özel anahtarları veri merkezinizde tutar. Uyumluluk riski olmadan tam şifreli trafik görünürlüğü sağlar.

Zero-Tuning

Kendini çalıştıran yapay zekâ destekli tehdit tespiti. Özel kural yok. Manuel konfigürasyon yok. Ekibiniz stratejiye odaklanır.

KİMLERE HİZMET VERİYORUZ

Tek Platform. İki Dünya.

HİZMET SAĞLAYICILAR

ISP'ler (İnternet Servis Sağlayıcıları), MSP'ler (Yönetilen Hizmet Sağlayıcıları), Hosting, CDN'ler, Eğitim Ağları

- Kârlı DDoS koruma hizmetleri sunun
- Ölçeklenebilir, çok kiracılı mimari
- SLA cezalarını ve müşteri kaybını azaltın
- Koruma hizmetini gelir kaynağına dönüştürün
- Her müşteri için sıfır operasyonel yük

KURUMSAL ŞİRKETLER

Finans, Sağlık, Oyun, Kamu, Perakende

- Gelir üreten hizmetleri 7/24 koruyun
- Uyumluluk gerekliliklerini karşılayın (PCI, HIPAA, GDPR)
- Operasyonel yükü ve personel maliyetlerini azaltın
- Yerinde (on-prem) tam şifreli trafik görünürlüğü
- Mevcut altyapının yatırım getirisini (ROI) artırın

SEKTÖRE ÖZGÜ RİSK

Sizin dünyanızda riskler neler?

Finansal Hizmetler

Yüksek frekanslı işlem (HFT) sistemleri mikrosaniye seviyesinde performans gerektirir. Bulut gecikmesi kabul edilemez. PCI-DSS ve SOC 2, tam denetim izleri zorunlu kılar. Tek bir kesinti, işlemleri sekteye uğratır ve müşteri güvenini zedeler.

Sağlık Sektörü

HIPAA, PHI'nin korunmasını zorunlu kılar. Hasta verisinin üçüncü taraf bulutta şifre çözülmesi yasal sorumluluk doğurur. Telehealth ve EHR sistemlerindeki kesintiler doğrudan hasta bakımını etkiler.

Oyun ve Eğlence

Gerçek zamanlı gecikme hassasiyeti. Oyuncu kaybı anlık ve kalıcıdır. Yoğun saat saldırıları hedefli ve koordinelidir. Gelir kaybı saniye bazında ölçülür.

Kamu ve Kritik Altyapı

Ulusal veri egemenliği gereksinimleri. Kritik altyapılar veriyi ülke sınırları dışında çözemez. Gelişmiş yeteneklere sahip ulus-devlet tehdit aktörleri.

DAĞITIM SEÇENEKLERİ

Sizi bulunduğunuz yerde karşılıyoruz

Donanım (NTD)

Maksimum trafik işleme kapasitesi için özel olarak tasarlanmış cihazlar.

Sanal (vNTD)

Esnek bulut ve VM ortamları için yazılım tanımlı yapı.

Bulut (CORE)

Bulut-yerel (cloud-native) yönetim ve zeka platformu

SaaS (SSP/TA)

Hizmet sağlayıcı ve trafik analizi platformu

Yazılım (BYOH)

Standart ticari donanım (COTS) üzerinde dağıtım — sizin altyapınız, bizim korumamız

COTS ÜZERİNDE ÇALIŞIR | YAZILIM DAĞITIMININ ÖZEL DONANIM SPESİFİKASYONLARIYLA EŞDEĞER OLDUĞU TEK SAĞLAYICI

Tedarikçi bağımlılığı yok. Amaç odaklı donanımlarımızla aynı performans garantilerine sahip olarak ticari standart (COTS) donanım üzerinde dağıtım yapın.

corero [NETWORK SECURITY]

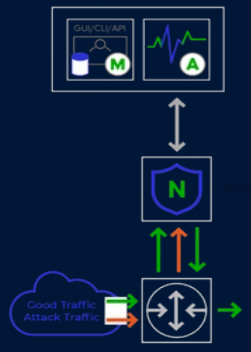
Dağıtım Mimarisi Türleri

INLINE

- Appliance transit trafiğini korur
- Tam edge bant genişliğini korur
- Saniyenin altında koruma sağlar
- Backhaul ihtiyacı yoktur
- Routing yeniden yapılandırması gerektirmez
- Edge ile birlikte ölçeklenir

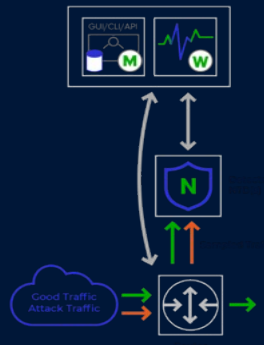
VERİ YOLU

- Appliance transit trafiğini korur
- Full veya % edge bant genişliğini korur
- Saniyenin altında koruma sağlar
- Backhaul ihtiyacı yoktur
- Routing konfigürasyonu gerektirir
- Edge / servis ile ölçeklenir



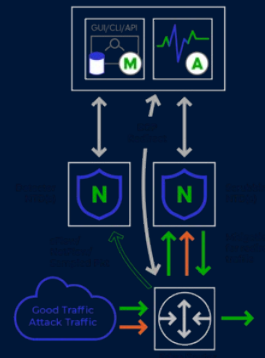
EDGE

- Edge'e yönelik appliance yoktur
- Full edge bant genişliğini korur
- Saniyeler içinde koruma sağlar
- Backhaul ihtiyacı yoktur
- Router vendor bağımsızdır
- Edge ile birlikte ölçeklenir



SCRUBBING

- Edge'e yönelik appliance yoktur
- Edge bant genişliğinin %20+'sini korur
- Saniyeler içinde koruma sağlar
- On-ramp routing gerektirir
- Maliyet optimizasyonu sağlar



DESTEKLENEN

ANALİTİK

- Trafik ve saldırı analizi
- Trend, uyarı ve raporlama

SERVİSLER

- Dünya Standartlarında SOC Hizmeti
- 7/24/365 MSSP / Destek

PORTAL

- Multi-Tenant Koruma SaaS
- Detaylı raporlar ve görünürlük

BULUT

- Doygunluk koruması
- Kurumsal ihtiyaçları karşılar

KÜRESEL OLARAK GÜVENİLİR

50’den fazla ülkede kritik altyapıları koruyor

Gartner®

DDoS Azaltma Çözümleri için en güncel Market Guide'da tanınan üretici

Market Guide for DDoS Mitigation Solutions

Published 15 May 2023 - ID G00742109 - 25 min read

By Analyst(s): Rajpreet Kaur, Thomas Lintemuth

Initiatives: Infrastructure Security

> Distributed denial of service attacks are setting records for volume and becoming more frequent and sophisticated. Here, we help security and risk management leaders choose DDoS mitigation services that protect externally facing services, and describe the options best aligned with their needs.

FORRESTER®

DDoS Azaltma Çözümleri için en güncel Now Tech Landscape Raporunda tanınan üretici

MARKETSANDMARKETS™

Mordor Intelligence

DDoS azaltma pazar analizinde önemli bir oyuncu olarak tanınan ve DDoS inovasyonunda lider üretici

Quadrant Knowledge Solutions

2024 DDoS Azaltma SPARK Matrix™'inde Tanınan Lider

OMDIA

DDoS Önleme Teknoloji Pazar Takibi'nde üst üste 10 yıl boyunca tanınma

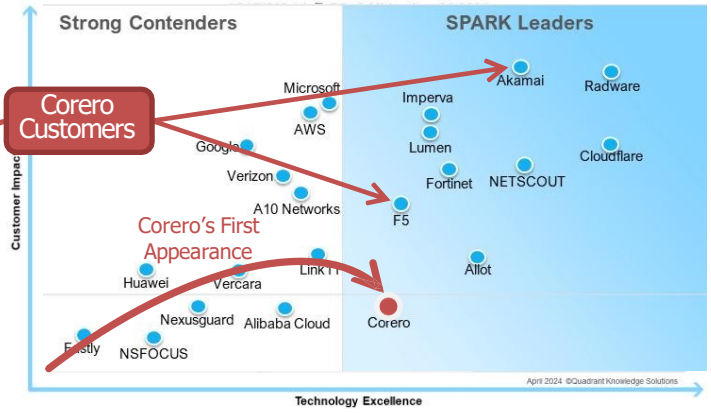
ARBOR NETWORKS

Akamai

f5

radware

corero



FROST & SULLIVAN

Artan Saldırı Karmaşıklığını Karşılamak için Gelişmiş DDoS Yetenekleri Çalışmasında katkı sağlayan üretici

OTD BİLİŞİM GLOBAL VAD

SEKTÖRDE TANINMA

Analistler ve sektör liderleri tarafından tanınan

PAZARLAR VE PAZARLAR

DDoS Azaltmada Yıldız

Pazardaki ürün yayılımı ve pazar payı/sıralamasına göre DDoS azaltma çözümleri alanında küresel ölçekte en üst tedarikçiler arasında konumlandırılmıştır.

İtiraz: “ISP / Bulut tarafında DDoS korumamız var.”

Corero Inline DDoS Koruması

- Her zaman açık / inline
- Saldırıları anında durdurur
- Gerçek zamanlı görünürlük
- Tam kontrol

VS

ISP / Bulut DDoS Servisleri

- Trafik yeniden yönlendirilir ve gecikir
- Manuel aktivasyon gerekir
- Sınırlı görünürlük ve kontrol
- Gecikme ve paket kaybı

Boşluk: ISP / Bulut koruması her zaman ağın (edge) noktasında aktif değildir!

Corero, saldırıları doğrudan ağınızın içinde otomatik olarak durdurur!

corero
[NETWORK SECURITY]

Bölgesel Odak – Türkiye

CORERO NASIL YARDIMCI OLABİLİR?

Bölgesel Bağlam	META bölgesindeki artan jeopolitik gerilim, özellikle telekom ve kritik altyapıları hedef alan DDoS saldırıları başta olmak üzere siber risklerin yükselmesine yol açmaktadır.
GERÇEKLİK	Birçok operatör ve kamu ağı, egemenlik, gecikme (latency) ve uluslararası bulut scrubbing altyapılarına sınırlı bağımlılık nedeniyle ülke içi koruma gerektirmektedir.
OPERASYONEL ZORLUK	Artan saldırı hacimleri ile sınırlı yerel mitigasyon altyapısının birleşmesi, hizmet kesintisi riskini artırmaktadır.
ON-PREMISE AVANTAJI	Gerçek zamanlı, inline DDoS mitigasyonu operatör ağının içinde konuşlandırılır, dış scrubbing merkezlerine bağımlılığı ortadan kaldırır.

SONUÇ

NEDEN CORERO?

Saniyenin Altında, Her Zaman Aktif	Gerçek zamanlı inline mitigasyon. Yönlendirme yok, manuel müdahale yok, bekleme yok. Koruma ya saldırı gelmeden önce vardır ya da çok geçtir.
Gerçek Hibrit Mimari	On-prem hız, cloud'un kaçırdığı %82 saldırı için. Cloud ölçeklenebilirlik, yerel kapasiteyi aşan volumetrik olaylar için. İkisi. Birlikte.
Gizliliği Koruyan Şifreleme	Seçici TLS denetimi, özel anahtarları veri merkezinizde tutar. Tam uyumluluk. Tam görünürlük. Taviz yok.
Operasyonel Basitlik	Otomatik tehdit istihbaratı, sıfır ayarlı (zero-tuning) L7 koruma, birleşik konsol. Ekibiniz uyarı peşinde koşmak yerine stratejiye odaklanır.

SONRAKİ ADIMLAR

Siber Dayanıklılığa Giden Yolunuz

1

Teknik Derin İnceleme

Gerçek zamanlı inline mitigasyon. Yönlendirme yok, manuel müdahale yok, bekleme yok. Koruma ya saldırı gelmeden önce vardır ya da çok geçtir.

2

Özel Değerlendirme

Mevcut koruma duruşunuzu analiz edeceğiz, boşlukları tespit edeceğiz ve bu boşlukların iş etkisini gerçek saldırı verilerine karşı modelleyeceğiz.

3

Kavram Kanıtı (PoC)

Sizin ortamınızda, sizin trafiğinizle nasıl çalıştığımızı görün. Taahhütte bulunmadan önce ölçülebilir sonuçlar. Risk yok.

corero [NETWORK SECURITY]

Siber Dayanıklılık Hakkında Konuşalım

OTD BİLİŞİM
GLOBAL VAD