corero [NETWORK SECURITY]

Cyber Resilience Starts Here.

The adaptive DDoS defense platform that keeps your most critical infrastructure running.

OTD BİLİŞİM GLOBAL VAD

Corero Network Security

DDoS protection specialists:

- Singular focus on DDoS
  - 15+ years of DDoS experience
  - In-house threat research
  - ~20% of revenue invested into R&D
- 24/7 security operations center
- Personalized support

Company profile:

- Operations
  - Worldwide HQ: London, UK
  - Engineering: Edinburgh, UK
  - US HQ: Marlborough, MA
- London Stock Exchange (CNS)
- ~85 people in North America and Europe

Our customers:

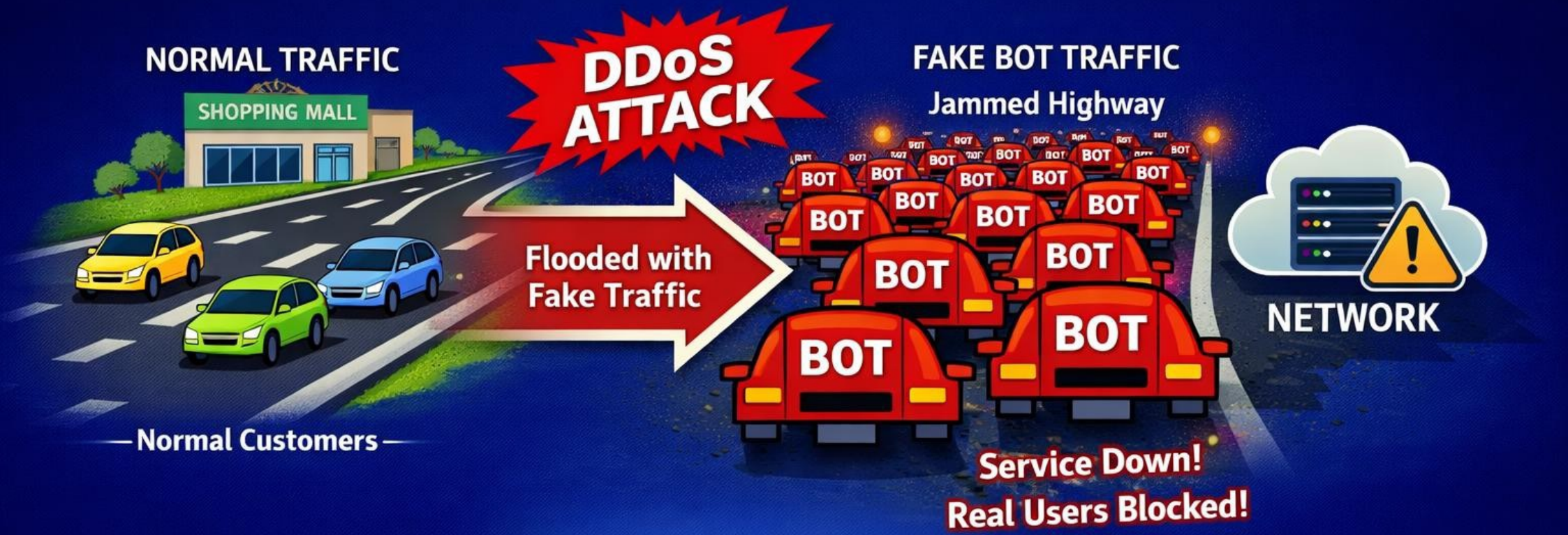
- Mid-sized ISPs
- Hosting providers
- On-prem SaaS providers
- MSP's , MSSP's
- Large Enterprise

What is DDoS?

Distributed Denial of Service

A DDoS Attack Explained

Like a Traffic Jam on Purpose...



corero

[NETWORK SECURITY]

WHY LEGACY APPROACHES FAIL

The Industry's Blind Spots

82% of DDoS attacks are under 1 Gbps. Cloud-only solutions miss them entirely.

6 sec Pulse attacks are over before traffic rerouting even begins. Manual mitigation is a non-starter.

0.5% leakage of a 2 Tbps attack = 10 Gbps of damage. At terabit scale, 'almost perfect' is a complete outage.

50+ vectors in a single campaign. Sequential detection can't keep up with 50 simultaneous attack types.

THE WORLD CHANGED IN 2025

Every Record Became the New Normal

262%
YoY increase in peak attack sizes

2.7 Tbps
Largest observed peak attack volume

12.3/day
Average DDoS attacks per customer

6 sec
Shortest observed attack wave

90.9%
Attacks lasting less than 10 minutes

1 in 3
Attacks followed by a repeat within 7 days

Source: Corero 2026 Threat Intelligence Report

Corero's Approach

A unified platform for cyber resilience.

INTRODUCING CORERO

The Adaptive Defense Platform

Corero Network Security is a global provider of automated network security and cyber resilience solutions, trusted by enterprises in 50+ countries.

SECURITY

- Volumetric DDoS
- HTTPS DDoS
- Application Security
- Access Control
- Outbound Protection

VISIBILITY

- Traffic Analytics
- Peering Analysis
- Availability Monitoring
- Attack Analytics
- OTT/App Traffic

OPERATIONS

- AI Assistant
- Managed Services
- API Integrations
- Unified Console
- Threat Intelligence

DEPLOYMENT

- Cloud (CORE)
- Virtual (vNTD)
- Hardware (NTD)
- SaaS (SSP/TA)
- Software (BYOH)

Introducing Corero SmartWall One

On-prem, modular platform

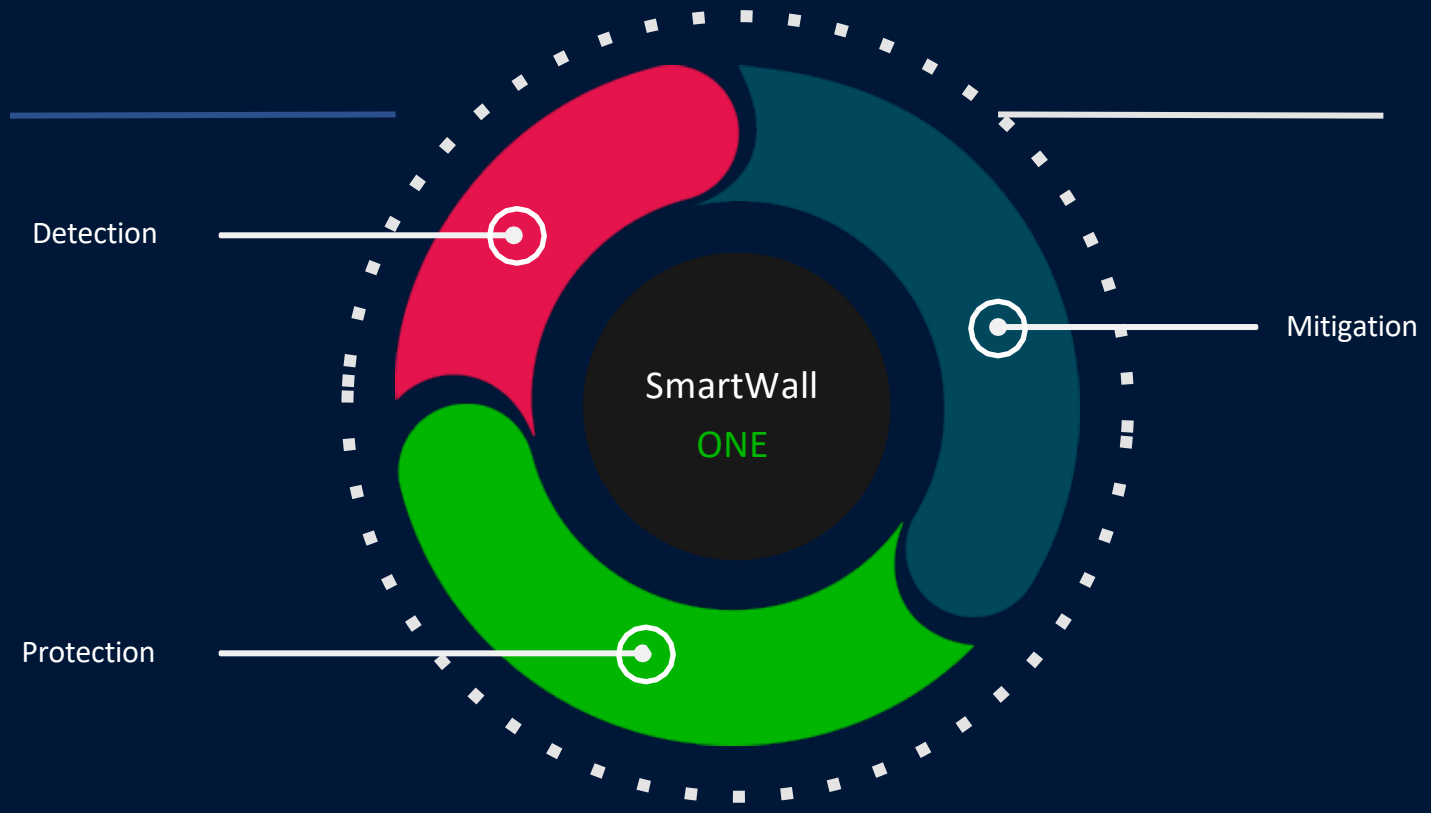
- Flexible deployment options
- Hardware and virtual appliances
- Integrates with existing infrastructure

Managed services and support

- Day-to-day monitoring administration
- Attack-time assistance
- Personalized support

Value-add service monetization

- Self-service portal for providers' customers
- DDoS protection as a service
- Protection that pays for itself



ON-PREMISES PROTECTION

Inline. Always-On. Sub-Second.

Always-On

Real-time inline mitigation at line rate. No rerouting to cloud. No manual intervention. Protection is there before the attack hits.

Full-Stack

L3 through L7 protection. Volumetric floods, protocol abuse, and application-layer threats. All handled in a single pass.

Privacy-First

Selective TLS inspection keeps private keys in your data center. Full encrypted traffic visibility without compliance risk.

Zero-Tuning

AI-powered threat detection that runs itself. No custom rules. No manual configuration. Your team focuses on strategy.

WHO WE SERVE

One Platform. Two Worlds.

SERVICE PROVIDERS

ISPs, MSPs, Hosting, CDNs, Education Networks

- Launch profitable DDoS protection services
- Scalable, multi-tenant architecture
- Reduce SLA penalties and customer churn
- Turn protection into a revenue stream
- Zero operational lift per customer

ENTERPRISES

Finance, Healthcare, Gaming, Government, Retail

- Protect revenue-generating services 24/7
- Meet compliance mandates (PCI, HIPAA, GDPR)
- Lower operational burden and staffing costs
- Full encrypted traffic visibility on-prem
- Improve ROI on existing infrastructure

INDUSTRY-SPECIFIC RISK

What's at Stake in Your World

Financial Services

HFT systems need microsecond performance. Cloud latency is a non-starter. PCI-DSS and SOC 2 demand full audit trails. A single outage disrupts trading and erodes client trust.

Healthcare

HIPAA requires PHI protection. Decrypting patient data in third-party cloud creates legal liability. Telehealth and EHR downtime directly impacts patient care.

Gaming & Entertainment

Real-time latency sensitivity. Player churn is immediate and permanent. Peak-hour attacks are targeted and coordinated. Revenue loss is measured per second.

Government & Infrastructure

National data sovereignty requirements. Critical infrastructure can't decrypt outside borders. Nation-state threat actors with advanced capabilities.

DEPLOYMENT OPTIONS

We Meet You Where You Are

Hardware (NTD)

Purpose-built appliances for maximum throughput

Virtual (vNTD)

Software-defined for flexible cloud and VM environments

Cloud (CORE)

Cloud-native management and intelligence platform

SaaS (SSP/TA)

Service provider and traffic analysis platform

Software (BYOH)

Deploy on COTS hardware — your infrastructure, our protection

RUNS ON COTS | THE ONLY PROVIDER WHERE SOFTWARE DEPLOYMENT MATCHES PROPRIETARY HARDWARE SPECS

No vendor lock-in. Deploy on commercial off-the-shelf hardware with the same performance guarantees as our purpose-built appliances.

corero [NETWORK SECURITY]

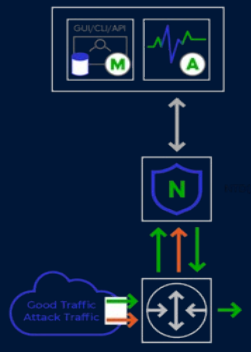
Types of Deployment Architecture

INLINE

- Appliance protects transit
- Protects Full Edge b/w
- Protects sub-second
- No need to backhaul
- No Routing Re-config
- Scales with Edge

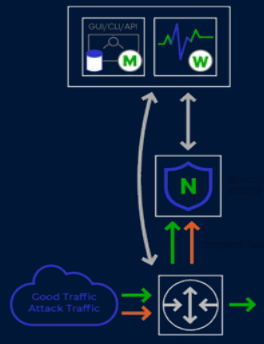
DATAPATH

- Appliance protects transit
- Protect Full or % Edge b/w
- Protects sub-second
- No need to backhaul
- Needs Routing config
- Scales with Edge/Service



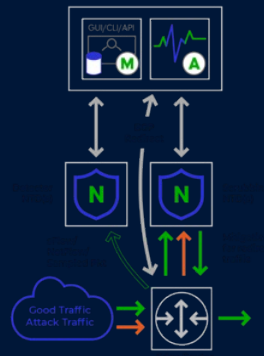
EDGE

- No Edge Facing Appliances
- Protects Full Edge b/w
- Protects in seconds
- No need to backhaul
- Router Vendor Neutral
- Scales with Edge



SCRUBBING

- No Edge Facing Appliances
- Protects 20+% Edge b/w
- Protects in seconds
- Needs Onramp Routing
- Cost Optimization



SUPPORTED BY

ANALYTICS

- Traffic & Attack Analysis
- Trend, Alerting, Reporting

SERVICES

- World-Class SOC Service
- 24x7x365 MSSP/Support

PORTAL

- Multi-Tenant Protection SaaS
- Detailed Reports & Visibility

CLOUD

- Saturation Protection
- Meet Enterprise Need

TRUSTED GLOBALLY

Protecting Critical Infrastructure Across 50+ Countries

OTD BİLİŞİM GLOBAL VAD

Gartner®

Recognized vendor in latest
Market Guide for
DDoS Mitigation Solutions

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®

Recognized vendor in latest
Now Tech Landscape Report
for DDoS Mitigation Solutions

MARKETSANDMARKETS™

Mordor Intelligence

Recognized as a major player
in DDoS Mitigation Market analysis
and leader in DDoS Innovation

Quadrant Knowledge Solutions

Recognized Leader in 2024
DDoS Mitigation SPARK Matrix™

OMDIA

Ten straight years of recognition
in DDoS Prevention Technology
Market Tracker

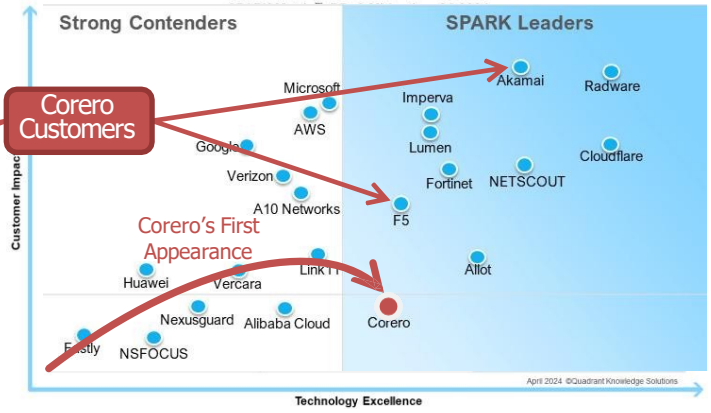
ARBOR NETWORKS

Akamai

f5

radware

corero



FROST & SULLIVAN

Contributing vendor in study of
Enhanced DDoS Capabilities to
Meet Growing Attack Complexity

OTD BİLİŞİM
GLOBAL VAD

INDUSTRY RECOGNITION

Recognized by Analysts and Industry Leaders

MARKETSANDMARKETS

Star in DDoS Mitigation

Positioned among the top vendors globally for DDoS mitigation solutions based on product footprint and market share/rank.

Objection: "We have DDoS protection from our ISP / Cloud."

Corero Inline DDoS Protection

- Always-On / In-Line
- Stops Attacks Instantly
- Real-Time Visibility!
- Full Control

VS

ISP / Cloud DDoS Services

- Traffic Rerouted & Delayed
- Manual Activation
- Limited Visibility & Control
- Latency & Packet Loss

Gap: ISP / Cloud Protection Is Not Always Active At The Edge!

Corero Automatically Stops Attacks Inside Your Network!

corero
[NETWORK SECURITY]

Regional Focus- Turkiye

HOW CORERO CAN HELP

Regional context	Increasing geopolitical tension in the META is driving higher cyber risk, particularly DDoS attacks targeting telecom and critical infrastructure.
REALITY	Many operators and government networks require in-country protection due to sovereignty, latency, and limited reliance on international cloud scrubbing.
OPERATIONAL CHALLENGE	Growing attack volumes combined with limited local mitigation infrastructure increases service disruption risk.
ON-PREMISE ADVANTAGE	Real-time, inline DDoS mitigation deployed inside the operator network – eliminating dependency on external scrubbing centers.

Source: Corero 2026 Threat Intelligence Report

OTD BİLİŞİM GLOBAL VAD

THE BOTTOM LINE

Why Corero

Sub-Second, Always-On

Real-time inline mitigation. No rerouting, no manual intervention, no waiting. Protection is either there before the attack hits, or it's too late.

True Hybrid Architecture

On-prem speed for the 82% of attacks cloud misses. Cloud scale for the volumetric events that exceed local capacity. Both. Together.

Privacy-Preserving Encryption

Selective TLS inspection that keeps private keys in your data center. Full compliance. Full visibility. No compromises.

Operational Simplicity

Automated threat intelligence, zero-tuning L7 protection, unified console. Your team focuses on strategy instead of chasing alerts.

NEXT STEPS

Your Path to Cyber Resilience

1

Technical Deep Dive

We'll walk your team through the platform architecture, demonstrate real-time mitigation, and show how it maps to your specific environment.

2

Custom Assessment

We'll analyze your current protection posture, identify gaps, and model the business impact of those gaps against real attack data.

3

Proof of Concept

See how we work in your environment with your traffic. Measurable results before you commit. No risk.

corero [NETWORK SECURITY]

Let's Talk Cyber Resilience.

OTD BİLİŞİM GLOBAL VAD