

TESTING & MONITORING

DoS, DDoS Testing and Protection

We measure how resilient your services are to heavy-traffic and resource-exhaustion attacks through controlled tests, and support you in building protection architecture against such attacks.

6

scope areas

5

step method

6

deliverables

// WHY IT MATTERS

Why it matters

Denial-of-service attacks can stop your business without stealing any data. Knowing weak points in advance, not during an outage, shows your real resilience. On the protection side we work vendor-neutral and choose the right solution with you.



DoS and DDoS tests are planned only with written permission, within an agreed scope and time window, and in a way that does not put your services at unnecessary risk. For third-party infrastructure (hosting, CDN, cloud) the provider's testing rules are followed.

// WHO IS IT FOR?

Who is this service for?



Organisations offering internet-facing services (e-commerce, payments, portals)



Businesses where downtime is costly



Those preparing before a campaign or peak period



Critical infrastructure and public service providers

// SCOPE

What does it cover?

**Attack surface analysis**

We map the internet-facing components of your services and their dependencies.

**Application-layer tests**

We measure the resilience of web applications and APIs to heavy requests and resource consumption.

**Network and protocol layer**

We assess the resilience of network and infrastructure components to volumetric and protocol attacks.

**Capacity and scaling**

We reveal bottlenecks and scaling limits.

**Protection architecture**

We design protection layers such as CDN, WAF, rate limiting and traffic filtering with you.

**Response procedure**

We prepare a procedure and exercise defining who does what during an attack.

Think like an attacker, build like a defender.

// METHOD

How we work

1

Scope and permissions

We clarify objectives, the test window and the required permissions (yours and third-party providers').

2

Analysis and test plan

We analyse the attack surface and prepare a controlled test plan.

3

Controlled test

We run the test in the planned window with gradual intensity.

4

Reporting and prioritisation

We present findings, bottlenecks and recommendations in priority order.

5

Protection and retest

We support implementing measures and retest their effect.

// DELIVERABLES

What do we deliver?

- ✓ Test plan and scope document
- ✓ List of weak points and bottlenecks
- ✓ DDoS response procedure

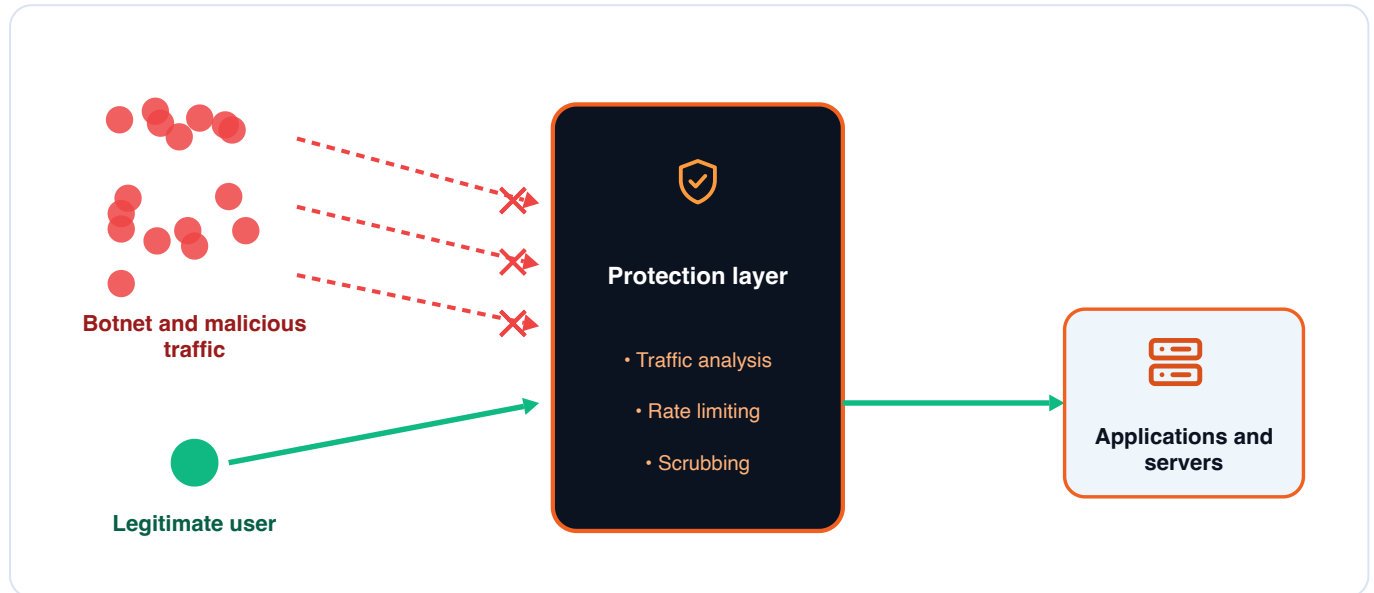
- ✓ Resilience test report
- ✓ Protection architecture recommendation
- ✓ Retest report

// VISUAL GUIDE

Service-specific visuals

How DDoS protection works

The protection layer filters malicious traffic and forwards legitimate requests to the service.

**Filtering**

Traffic analysis and rate limiting drop malicious requests before they reach the server.

Continuity

Legitimate users keep reaching the service unaffected.

Test first

Controlled tests show how protection behaves under real load.

Main attack types

Tests cover three families of attack; each needs a different defence.

Volumetric attacks (L3/L4)

Aim to saturate bandwidth: UDP/ICMP floods, reflection and amplification attacks.

Protocol attacks

Exhaust server and firewall resources: SYN floods, connection table exhaustion.

Application layer (L7)

Tire the application with legitimate-looking requests: HTTP floods, slow requests, costly queries.

Different attack, different defence

Volumetric attacks need capacity and scrubbing; L7 needs application-level filtering.

Capacity planning

Test results inform bandwidth and resource planning.

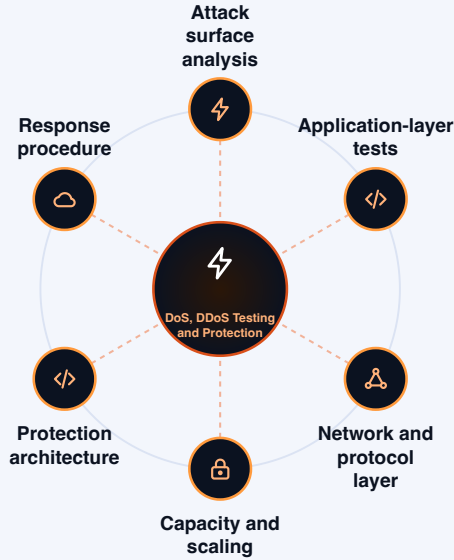
Response procedure

Who does what during an attack is defined in advance.

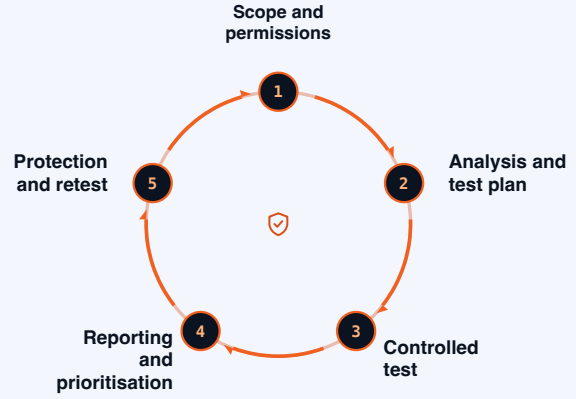
// AT A GLANCE

Service overview

SCOPE MAP



OUR DELIVERY LOOP



// UNDER ONE ROOF

Our other services

- | | | |
|--|---|--|
|  ISO 27001 Consulting |  ISO 22301 Consulting |  ISO 14298 Consulting |
|  KVKK Compliance Consulting |  Cyber Security Consulting |  Risk Management Consulting |
|  Penetration Testing |  Regular Vulnerability Scanning and Management |  SOC / SIEM Implementation |
|  Endpoint Security Monitoring |  Secure Software Development |  Information Security Awareness Program |
|  Incident Response Readiness | | |

// CONTACT

Get in touch

Share your needs and current situation and we will define the right scope and roadmap together. Fill in our information form or contact us directly.

Troy Bilgi Teknolojileri Ticaret Limited Şirketi

Atatürk Mah. Vedat Günyol Cad. 44M/2

Ataşehir / İstanbul, Türkiye

T 0-216-575 5222 **E** info@troybilgiteknojileri.com



Scan the QR code for the service page and information form