

TESTING & MONITORING

Endpoint Security Monitoring

We support you in monitoring endpoints such as computers, servers and mobile devices with advanced endpoint security (EDR/XDR) solutions and detecting threats early.

**6**

scope areas

5

step method

6

deliverables

// WHY IT MATTERS

Why it matters

Most attacks start at an endpoint: a phishing email, a malicious file, a compromised account. Without endpoint visibility it is hard to understand where and how an attack progressed. We work vendor-neutral and choose the solution that fits your infrastructure with you.



Whether endpoint monitoring is run in-house or externally depends on your scope. We clarify your needs together in the meeting.

// WHO IS IT FOR?

Who is this service for?



Organisations with remote or hybrid teams



Those who want to move from classic antivirus to advanced protection



Those who want to reduce ransomware risk



IT teams seeking central endpoint visibility

// SCOPE

What does it cover?

**Endpoint inventory and risk**

We identify your device types, operating systems and risks.

**EDR/XDR selection and deployment**

We help you choose and roll out the right solution.

**Policy and hardening**

We define device security policies and basic hardening settings.

**Monitoring and alert tuning**

We set up dashboards and alerts and reduce false positives.

**Incident triage**

We define how alerts are reviewed, prioritised and acted on.

**SIEM and SOC integration**

We correlate endpoint data with your central monitoring infrastructure.

**Think like an attacker,
build like a defender.**

// METHOD

How we work

1

Current-state and needs analysis

We assess the device inventory, existing protection and expectations.

2

Solution selection and architecture

We determine the right solution and architecture vendor-neutrally.

3

Deployment and policy

We start with pilot groups and roll out gradually.

4

Monitoring and alert tuning

We tune alerts and dashboards to your environment.

5

Operations and improvement

We develop the monitoring process with regular reporting and reviews.

// DELIVERABLES

What do we deliver?



Endpoint inventory



Policy and hardening document



Incident triage and response workflow



Solution and architecture recommendation



Monitoring dashboards



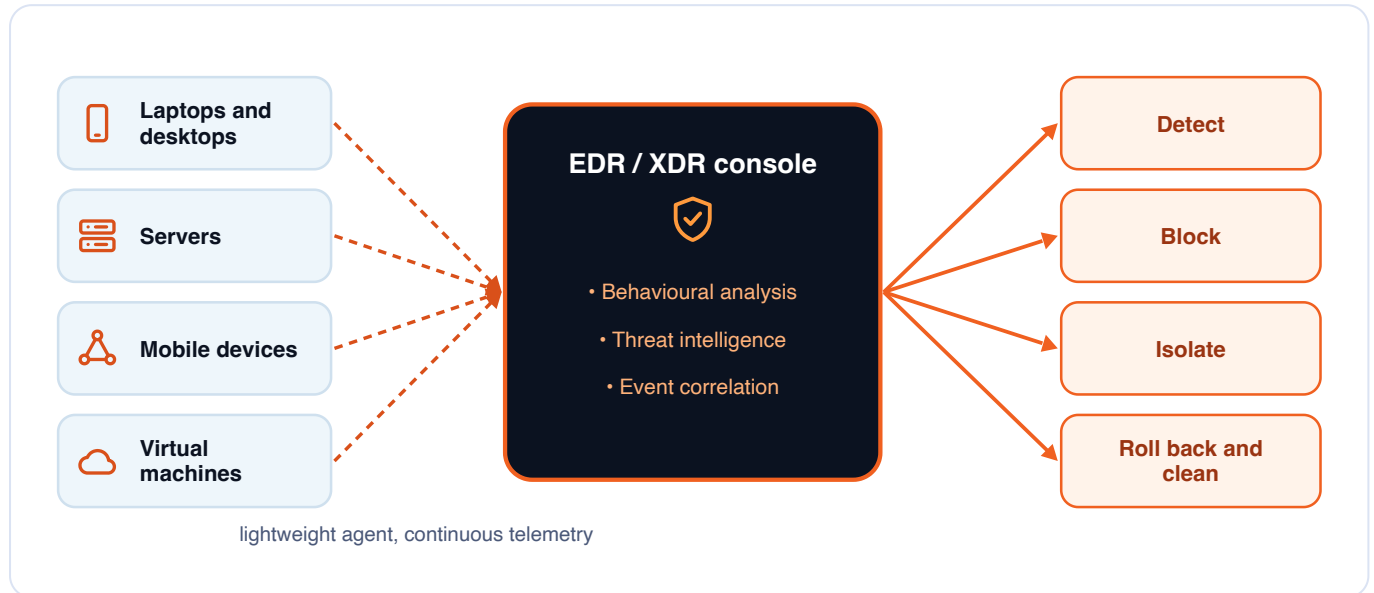
Regular monitoring reports

// VISUAL GUIDE

Service-specific visuals

Endpoint monitoring architecture

An agent on each device sends telemetry to the console, which detects threats and triggers response actions.

**Visibility**

Continuous telemetry is collected from every device.

Behaviour-based detection

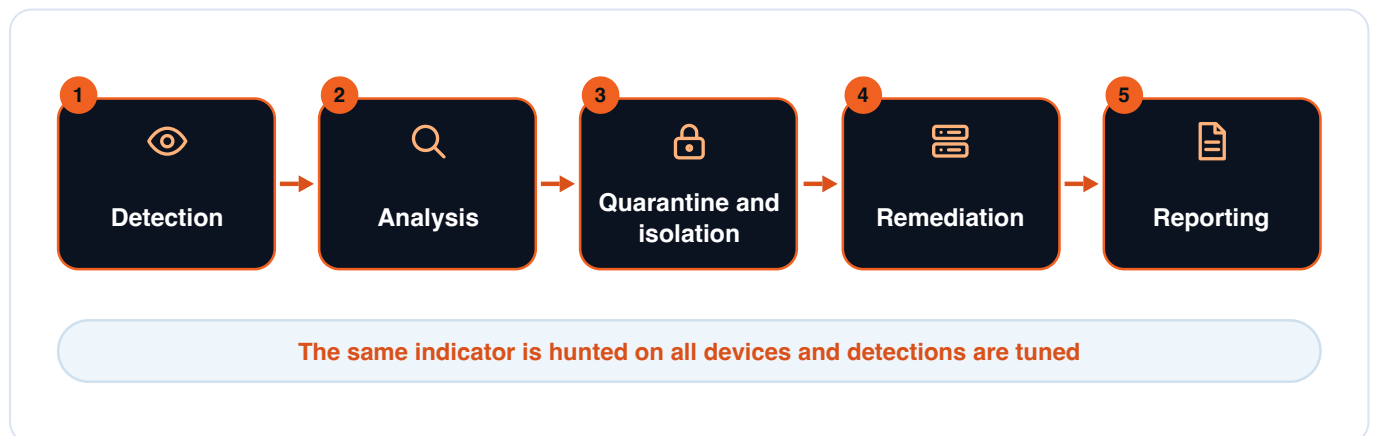
Threats without signatures are caught through unusual behaviour.

Fast response

A suspicious device is isolated and malicious activity is rolled back.

Response flow for an endpoint incident

Steps from suspicious behaviour to remediation.

**Minutes matter**

Time from detection to isolation decides how far an incident spreads.

Fleet-wide hunt

A found indicator is searched for on all other devices.

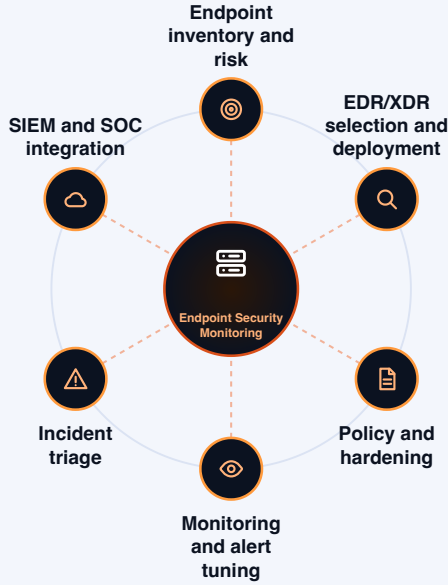
A learning system

Detection rules are improved after each incident.

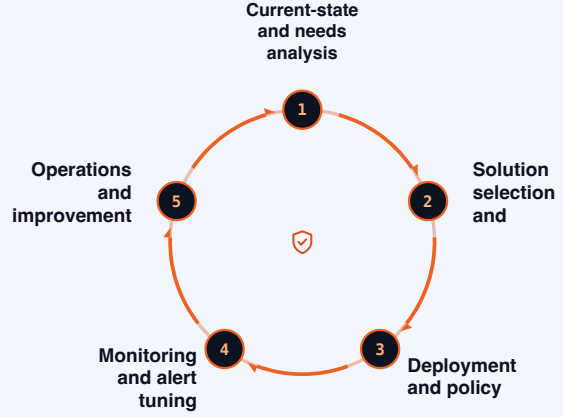
// AT A GLANCE

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 |  DoS, DDoS Testing and Protection |
|  SOC / SIEM Implementation |  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@troybilgiteknolojileri.com



Scan the QR code for the service page and information form