aa teknoloji

Falcon Insight EDR

Designed for cybersecurity teams, Falcon Insight is an advanced EDR platform that makes cyber threats visible through real-time endpoint monitoring, automated threat detection, and intelligent response mechanisms.

End Point Security Challenges

Growing digital infrastructures and the increasing number of devices are pushing corporate network complexity to its peak. The inadequacy of traditional security tools creates blind spots, leading to the infiltration of advanced threats and the slowing down of operational processes.
The inability to monitor activities across dispersed endpoints from a single central point restricts network visibility. The lack of real-time threat detection and manual analysis processes lower event response speeds, creating vulnerabilities. Intense alert fatigue and data lacking context form a bottleneck that causes cybersecurity teams to overlook critical threats.

⚠ Who can benefit?

- For teams experiencing blind spots on endpoints with traditional tools
- For analysts suffering from cyber fatigue due to excessive alert density
- For teams losing time in threat analysis and incident response processes
- For infrastructures struggling with complex deployment and manual security processes

Core Principles

Visibility
Full endpoint monitoring with zero blind spots.

Speed
Real-time threat detection.

Protection
Stopping advanced cyber threats.

Automation
Intelligent incident analysis powered by AI.

How Does Falcon EDR Work?

Falcon Insight processes the data it collects from endpoints via its lightweight agent within a cloud architecture. It protects your infrastructure seamlessly through a 3-step workflow that instantly detects cyberattacks using advanced AI and threat intelligence.

Technical Specifications

Threat Detection & Analysis
- IOA indicators via behavioral analysis
- Full mapping with the MITRE ATT&CK framework
- Deep data collection through the kernel driver
- Capturing over 400 raw logs with the Forensic module

Incident Response & Reaction
- Immediate action with Real Time Response (RTR)
- Automated SOAR workflows with Falcon Fusion
- Preventing threats from spreading across the network
- Remote analysis on isolated devices

Intelligence & Threat Hunting
- Device health assessment with Zero Trust Assessment
- Security policies compliance control
- Conditional access support based on risk score
- Enterprise threat scoring via CrowdScore

Identity & Status Verification
- Device health assessment with Zero Trust Assessment
- Security policies compliance control
- Conditional access support based on risk score
- Enterprise threat scoring via CrowdScore

Cloud & Infrastructure Management
- Rapid live deployment with a single, lightweight agent
- Zero overhead with a serverless cloud architecture
- Retrospective log archive up to 90 days
- Continuous monitoring with zero performance loss

Workflow

1. Continuous Monitoring
- Monitors endpoints instantly using a lightweight agent.
- Collects raw events via the kernel driver.
- Transmits activity data to the cloud pipeline.
- Operates continuously with zero performance loss.

→

2. Threat Detection
- Analyzes data using AI and the Threat Graph.
- Detects behavioral IOA indicators.
- Maps attacks against the MITRE matrix.
- Prioritizes threats using CrowdScore.

→

3. Instant Response
- Stops cyberattacks in real time.
- Isolates the compromised device from the network.
- Provides remote intervention via the RTR feature.
- Triggers SOAR workflows with Falcon Fusion.

Integration and High Security Standards
It offers a flexible integration model that adapts fully to SIEM and log infrastructures. It puts your critical corporate networks under protection with hardened data isolation and the highest security standards.

Advantages

Advanced Threat Detection
Goes beyond traditional signatures to capture complex adversary activities in real time using behavioral analysis methods.

Real-Time Incident Response
Provides direct remote access to compromised endpoints, instantly isolating malicious activities and rapidly purging them from systems.

Root Cause and Visual Analysis
Visualizes the attack chain on a single screen, mapping it to the MITRE ATT&CK framework and drastically accelerating root cause analysis.

CrowdScore Intelligent Analysis
Consolidates scattered alerts under a single enterprise threat score, reducing alert fatigue for teams and keeping them focused on critical incidents.

aa teknoloji

AA Teknoloji is an AI-powered media technologies platform developed for modern newsrooms. Our integrated solutions, ranging from news workflow systems to digital archive solutions, real-time broadcasting infrastructure to multi-channel content management, accelerate the digital transformation processes of media organizations and offer scalable broadcasting operations.

For more information, visit aateknoloji.tr or follow the @aateknoloji LinkedIn account.