aa teknoloji

Vectra NDR

AI-Powered Hybrid Network and Identity Security Platform

Vectra NDR analyzes attacker behavior across network, identity, and cloud environments to help surface the threats that truly require a response from the flood of security signals. AA Teknoloji positions Vectra NDR alongside your existing SOC, endpoint, and network security solutions, managing POC, on-site deployment, integration, license management, product training, and Turkish-language technical support under SLA end-to-end.

Modern Security Challenges

In hybrid environments, network traffic, identity activity, cloud services, and unmanaged assets are monitored across separate security layers. Attackers who use valid credentials or move laterally within the network can slip through when individual alerts lack sufficient context. High alert volumes also make it harder for SOC teams to determine which incidents truly deserve priority.

⚠ Who can benefit?

- SOC teams that can't see threats hidden in encrypted traffic and lateral movement
- Organizations that want to monitor credential abuse and privilege escalation attempts
- Teams unable to prioritize real threats due to high alert volume
- Organizations that want to assess network and identity behavior together across hybrid and multi-cloud environments

Core Principles

Observability
Seeing network and identity behavior together

Speed
Faster focus on priority threats

Control
Reducing exposure and attack spread

Signal
Surfacing genuine attacker behavior

Technical Specifications

Observability & Coverage

- On-premises, AWS, Azure, GCP, and Oracle Cloud support
- Microsoft 365, Active Directory, and Entra ID integration
- IoT/OT, edge, and SaaS environment support
- Agentless deployment with visibility within minutes

Detection Capabilities

- 200+ behavioral detection models
- 12 MITRE ATT&CK reference categories
- Attack Signal Intelligence
- No decryption required for encrypted traffic

Integrations

- CrowdStrike Falcon, Microsoft Defender, SentinelOne
- Microsoft Sentinel, Splunk, Google SecOps
- Cortex XSOAR, Splunk SOAR
- Firewall, ITSM, and packet broker integrations

Compliance & Reporting

- NIST CSF 2.0, NIS2, and Zero Trust alignment
- Reporting and evidence generation that supports compliance audits
- Executive-level security posture reports
- MITRE ATT&CK framework alignment

How Does Vectra NDR Work?

Vectra NDR evaluates behavior from network and identity environments together, helping determine whether seemingly unrelated signals are part of the same attack. Its Attack Signal Intelligence approach lets analysts focus on priority attack behaviors instead of sifting through countless alerts.

Workflow

1. Continuous Observability

- Every asset across on-premises, multi-cloud, SaaS, and IoT/OT environments is monitored.
- Human and machine identities are inventoried in real time.
- Risky access paths and over-privileged identities are identified.
- Unmanaged and transient devices are discovered dynamically.

→

2. Threat Detection and Prioritization

- 200+ behavioral detection models identify attacker actions.
- Credential abuse, lateral movement, and command-and-control traffic are detected.
- Threat analysis is performed on encrypted traffic without decryption.
- False positives are automatically filtered out, surfacing real threats.

→

3. Investigation and Response

- Dynamic attack maps visualize every stage of the attack.
- AI-assisted investigation is accelerated through natural-language queries.
- Response actions are taken against compromised identities and affected endpoints through integrations.
- Response actions are triggered through the firewall and integrated security solutions.

Sample Use Case

When a valid user account is compromised and unusual access and lateral movement begin, Vectra NDR evaluates network and identity behavior together to surface related signals. Instead of reacting to individual alerts, the SOC team can plan its response around the full context of the attack.

Advantages

Attack Signal Intelligence
Correlates scattered signals within the context of an attack, helping analysts know which threat to investigate first.

Fast Investigation and Response
With dynamic attack graphs and AI-assisted investigation, analysts grasp the full attack story; this meaningfully shortens response time and helps contain the spread of attacks.

Network and Identity Visibility
Continuously monitors every asset and identity across on-premises, multi-cloud, SaaS, edge, and IoT/OT environments, providing a dynamic view of the attack surface based on real-time activity rather than static inventory lists.

Integrates With Your Existing Security Ecosystem
Complements detection and response processes alongside solutions like CrowdStrike and Palo Alto Networks.

aa teknoloji

AA Teknoloji is a technology company and an Anadolu Ajansı affiliate, providing media technologies, cybersecurity, and open-source solutions. It delivers SOC services, penetration testing, SIEM/EDR, threat intelligence, and media infrastructure solutions together with deployment, integration, and 24/7 local technical support.

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