

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

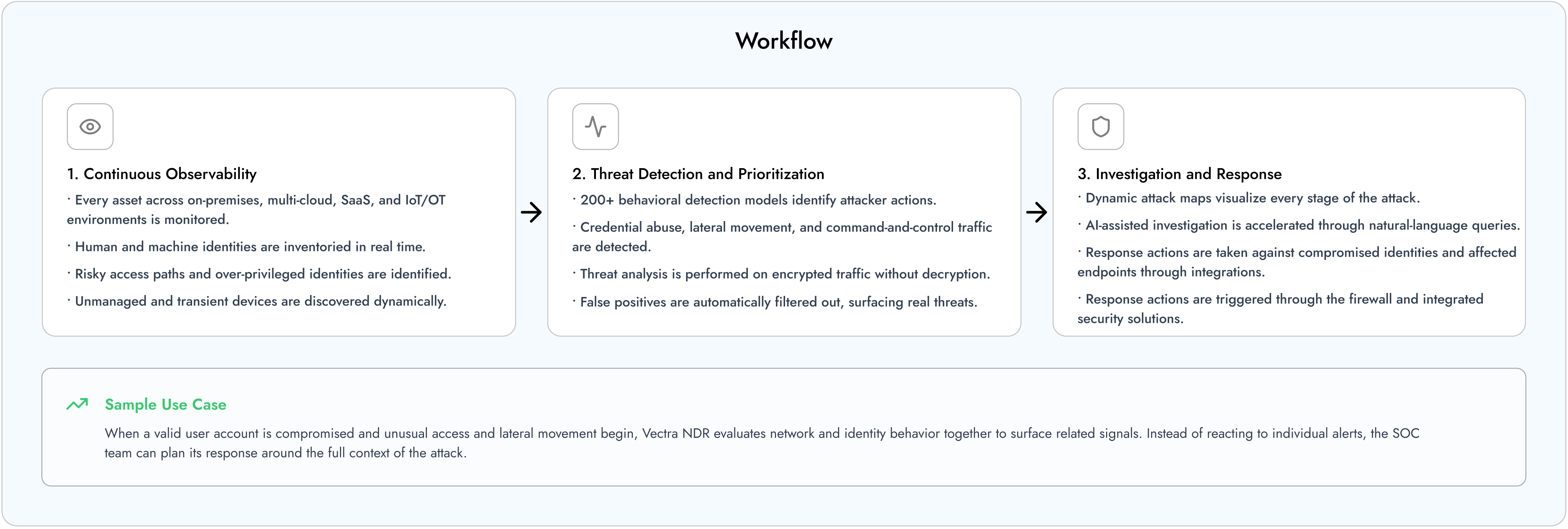
Reducing exposure and attack spread

Signal

Surfacing genuine attacker behavior

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.



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](https://www.linkedin.com/company/aateknoloji) on LinkedIn.