DATASHEET

Adlumin Extended Detection and Response (XDR)

Adlumin XDR is an AI powered, cloud native platform that detects, prioritizes, and responds to threats across your environment. It replaces siloed, reactive security with a unified, intelligence driven approach that strengthens resilience and reduces operational workload.

N-ABLE Adlumin
Security Operations

Core capabilities

Unified security operations platform

- Unify core security functions—including AI Detection, SIEM, UEBA, SOAR, Network Health, Honeypots, and Cyberthreat Intelligence—within a single platform that correlates security telemetry across the environment to support centralized detection, investigation, response, and reporting
- Integrate with existing security and IT systems through a vendor agnostic architecture that connects to endpoints, identity providers, cloud platforms, network sensors, and log sources across your entire stack

AI-powered detection and UEBA

- Detect advanced threats, such as ransomware, account takeovers, privilege abuse, and insider activity, using proprietary AI models combined with behavioral analytics
- Adapt detection logic continuously as the AI learns from real-world attack data, SOC insights, and emerging tactics and techniques

SIEM-driven visibility and investigation

- Centralize security data with SIEM-level correlation that connects events across the kill chain to accelerate investigations
- Map lateral movement and reconstruct incident timelines with AI-driven context that highlights the most relevant evidence

SOAR automation and response orchestration

- Automate investigation and response through SOAR workflows to streamline analyst operations and rapidly contain threats by isolating endpoints, stopping malicious processes, disabling accounts, and revoking credentials

Cyberthreat intelligence and honeypots

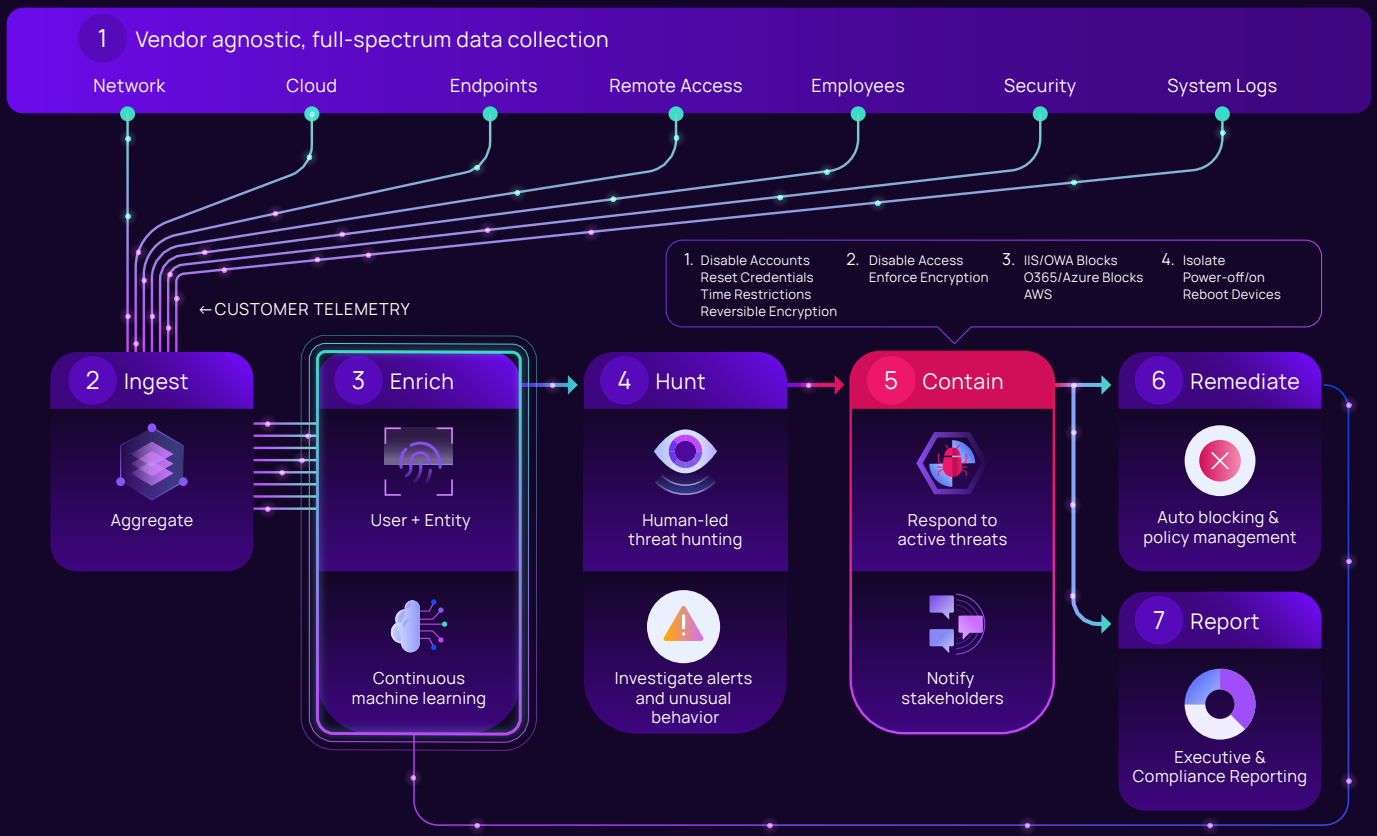
- Enrich investigations with threat intelligence, including darknet monitoring and perimeter-based early-warning signals
- Expose attacker behavior earlier using deception capabilities such as honeypots that detect unauthorized probing or lateral movement attempts

Network health and compliance reporting

- Monitor network health indicators alongside security telemetry to identify performance issues, misconfigurations, and risk conditions that impact resilience
- Generate audit ready compliance reports through centralized dashboards covering key regulatory frameworks

How it works

Adlumin XDR uses AI-enriched data from your entire environment to aid threat detection and remediation. Then, that learning feeds back into our AI for continuous optimization through data science, response analysis, and insights from our human-led MDR team.



Key Benefits

Improved threat detection

- Increase detection accuracy through behavior based AI that surfaces attacks traditional tools miss
- Lower attacker dwell time with continuous monitoring across data sources

Faster response

- Shorten response times through automated containment workflows and real time orchestration
- Accelerate investigations with AI driven context, incident mapping, and prioritization

Reduced analyst load

- Automate routine SOC tasks, covering up to 90% of investigation activities*
- Minimize noise with AI models that filter false positives and prioritize real threats

Consolidated visibility and control

- Unify endpoints, logs, identities, and cloud environments under a single platform
- Reduce the complexity of multiple disconnected security tools

Streamlined compliance

- Automate audit reporting and evidence collection
- Demonstrate security posture improvements through clear metrics and dashboards

Scalable protection

- Support cloud, on prem, and hybrid environments with ease
- Grow without re architecting or replacing existing technologies

*The 2026 State of the SOC Report: https://www.n-able.com/resources/state-of-the-soc-report-2026

What you gain

Enhanced detection accuracy

Achieve higher-fidelity threat identification powered by adaptive AI and correlated data from across your environment

Accelerated incident resolution

Deliver faster investigations and response with automated containment

Lower security operations overhead

Minimize manual triage and analyst fatigue through AI generated insights and automation

Unified operational intelligence

Gain centralized insights into organizational risk, security posture, and long term maturity trends

Stronger cyber resilience

Enable continuous learning, proactive anomaly detection, and a platform that improves with every data point

Ready to simplify security operations?

See how Adlumin XDR strengthens threat detection and response:

Explore Adlumin XDR

N-able fuels IT services providers with powerful software solutions to monitor, manage, and secure their customers' systems, data, and networks. Built on a scalable platform, we offer secure infrastructure and tools to simplify complex ecosystems, as well as resources to navigate evolving IT needs. We help partners excel at every stage of growth, protect their customers, and expand their offerings with an ever-increasing, flexible portfolio of integrations from leading technology providers. n-able.com