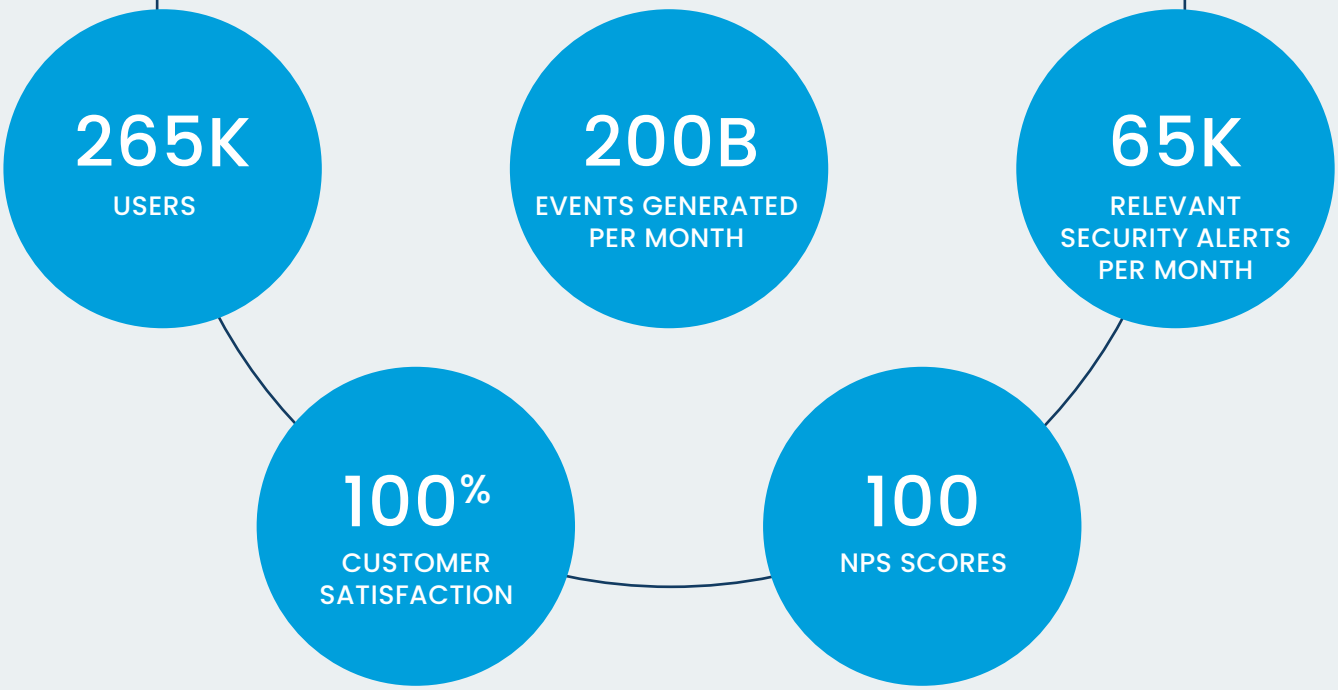
AHEAD elastic

AHEAD Stops Threats in Minutes, Not Hours

What the AHEAD Next-Gen SOC Can Do for You

Our Clients



> *AHEAD Managed Security is an integral part of our security infrastructure, and we consider them to be a true extension of our team.*
> *Food City / KVAT Foods*

> *I've had SOC services at no fewer than six companies, and AHEAD continues to be one of the best and with the new SIEM technology I'm excited about the future.*
> *Aegis Sciences Corporation*

> *Literally the best SOC I have ever worked with - all their members are extremely knowledgeable and helpful.*
> *Duluth Trading Company*

Our Platform

6.9 MIN
Market-Leading MTTR

AHEAD maintained a MTTR under 7 minutes even as security events increased 50%

Industry average 20-30 minutes

73%
Reduction in Triage Time

Thousands of hours of analyst time saved

92%
Automatic Resolution Rate

Machine learning massively reduced manual interventions

23M+
Automation Activities

Performing unique actions across hundreds of standard and custom data sources

15K+
Detection Rules (2K+ Unique Rules)

Standard Queries, Algorithm-based Structured Queries, Event Correlation, Threshold, Machine Learning, Novel Activity, Threat Intelligence

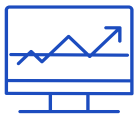
30+
Case Workflows

EDR, Phishing, DNS, Firewall, Phishing, External Ticketing/Case Management Tools

Smarter Detection Before Human Intervention

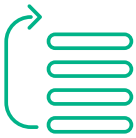
IDENTIFY

No more sorting through thousands of logs to get a high-level view of a security incident. Analysts see the sequence of events leading up to and following a security incident, painting a clear picture of an attacker's movements, and facilitating faster threat identification.



ANALYZE

By analyzing historical data, the algorithms of the AHEAD SOC build a database of "normal" activity patterns and only alert you to relevant events. For example, the SOC automatically adjusts to user behavior and travel patterns, so legitimate logins from employees on vacation will not trigger endless alerts.



PRIORITIZE

AI-driven alarms highlight relevant information within security events, including user, country, IP address, or any captured data point. Analysts can skip manually sifting through data and prioritize critical issues in seconds.

AHEAD elastic