

ANOMALI

# Security Operations Done Differently



# Anomali:

Security Operations Done Differently



CIOs and CISOs are navigating a complex and evolving threat landscape fueled by AI-driven cyber attacks, geopolitical instability, and an ever-increasing big data challenge. They're fighting the battle with a weakened arsenal of fatigued workforces and dated technology, leaving their organizations dangerously vulnerable to attack.

**To win the war against cybercrime, they must think differently.**

## Introducing Anomali: The Leading AI-Powered Security Operations Platform

Anomali modernizes the delivery of legacy security systems. We combine ETL, SIEM, XDR, SOAR, and TIP to deliver powerful security analytics that empower our customers to detect, investigate, respond, and remediate threats with unprecedented speed and precision. We do it all in one easy-to-use integrated platform at a fraction of the cost of other solutions.

## Our Mission

Anomali delivers innovative and effective technologies and solutions to address cybersecurity challenges for organizations of all sizes. Through trust, collaboration, and communication, Anomali strives to implement AI-Powered intelligence-driven solutions to achieve its vision: a more secure world.

**"Before Anomali, we had tons of information without context. We had to look through thousands of alerts quickly just to see what stood out and then react to those. Anomali enabled us to spend less time dealing with noise, and more time focusing on critical issues"**



Devin Ertel | CISO,  
Blackhawk Network Holdings



## Meet the Anomali Copilot

Imagine your talent starting with an intelligent Copilot that automates and frees up significant time to do more advanced threat hunting while reporting to management in seconds. Imagine your talent, along with our Copilot, navigating a modern cloud-native Security Data Lake that gives relevant visibility and drives necessary decisions, making security an integral part of executive management decisions.

## Unparalleled Visibility and Performance

The Anomali Security Operations Platform combines numerous legacy security analytics solutions and improves scale and performance by over 1,000x. We also provide curated access to the largest repository of threat intelligence available.

The combination allows you to compare every bit of information regarding known bad actors with every piece of data ingested by the platform to provide insight and predictive analytics that competitors cannot. One-hundred percent of the data within the platform is hot, and we have no limits to the duration or quantity of the data that you analyze. If you'd like 20 years' worth of dashboards or anomaly detection, be our guest.

Also different from legacy solutions is that we don't sit on top of a big data provider. We are a big data player, enabling us to pass those margins to you — improving your P&L, earnings per share, and cash.

## Threat Intelligence at Your Fingertips

Forget reading lengthy technical documents or conducting days and days of research and analysis. If you want to know more about a threat actor, simply scan anything you'd like with our Copilot inside or outside of our platform, and have all of the relevant answers within seconds. On top of that, report operational risk to management in simple terms, also in seconds. On the go, you can leverage Anomali's full capability with a mobile app.

## Better Decision Making, Lower Costs

Legacy approaches to security make it complicated and expensive to get the security insights required to drive good decision-making. Security teams struggle to assemble a complete picture from multiple systems (ETL, SIEM, XDR, TIP, and SOAR) and analysis is time-consuming and requires advanced skill sets. Instead of requiring complex queries, Anomali's embedded generative AI-powered Copilot lets analysts ask questions in natural language and retrieve answers almost instantaneously — slashing your analysts' workloads in half and dramatically boosting ROI.



**>50%**

Time saved by eliminating parsing, indexing & archival

**300x**

Faster than legacy SIEMs

**30TB+**

Data ingested in hours, not days

**30 sec**

Search petabytes of data in seconds

## Client Testimonials

**“We leverage market-leading tools to give our company a competitive advantage and our 24.7 SOC a leg up on bad actors. With Anomali, we improve on both of these goals. By adding intelligence, we achieve a high level of certainty that enhances prioritization of the most serious threats our customers face, while improving our mitigation decisions.”**



Grant Leonard | Co-Founder, Castra

**“The time it takes to analyze a threat has gone down from 30 minutes to just a few minutes, time that adds up over the course of investigating many malicious Ips every week. There has been a substantial decrease in terms of meantime-to-know.”**



Arindam Bose | Senior Vice President & Security Officer, Bank of Hope

## Get Started Today

Discover how Anomali can help you think differently and deliver transformational results.

Schedule a live product demo or visit us at [www.anomali.com](http://www.anomali.com).