ANOMALI

Big Data Security. Actionable Intelligence. Relevant Insights.

The Anomali Platform

Cloud-native extended detection and response (XDR) rooted in intelligence.

Anomali Match™
Threat Detection Engine

ThreatStream®
Threat Intelligence Management

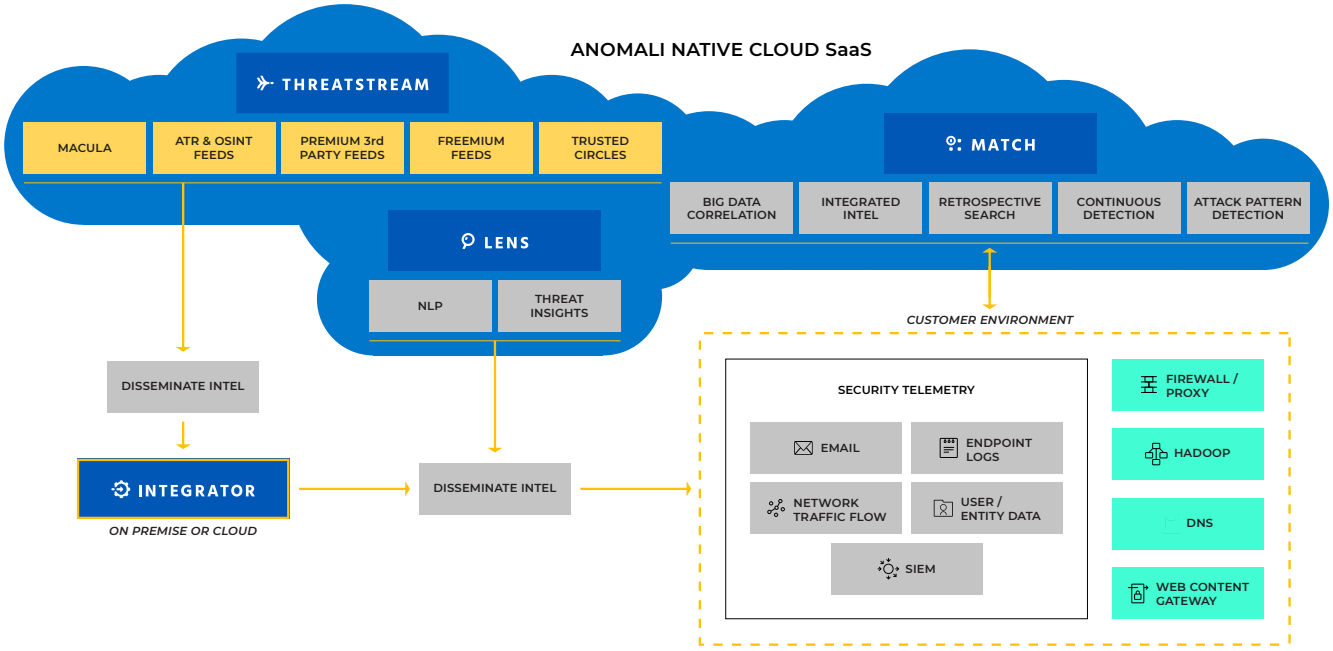
Anomali Lens™
Threat Insights

The Anomali® Platform

The Anomali Platform is a cloud-native extended detection and response (XDR) solution that automates the collection of threat data and drives detection, prioritization, and analysis, taking security from intelligence to detection in seconds.

The Anomali Platform is fueled by big data management, machine learning, and the world's largest intelligence repository to automatically correlate ALL installed security telemetry against active threat intelligence to stop breaches and attackers in real-time.

By cutting through the noise to surface relevant threats, the Anomali Platform improves organizational efficiencies, providing security teams with the tools and insights needed to detect threats, make informed decisions and defend against today's sophisticated threats.



Anomali®

By correlating the world's largest repository of global actor, technique, and indicator intelligence with our infinite detection capabilities, The Anomali Platform delivers a one-of-a-kind extended detection and response solution that continuously detects threats and prevents attacks before they happen.

Platform Benefits:

- Quickly identify targeted threats to your organization
- Automate detection and analysis of threats to empower analysts
- Improve response with insights into threat actors and behaviors
- Save time and resources by the reducing impact of attacks
- Break down silos and enable collaboration between internal and external teams
- Increase ROI of existing security investments

ThreatStream®

Threat Intelligence Management that automates the collection and processing of raw data and transforms it into actionable threat intelligence for security teams.

- Map threat intelligence to threat models (Actor Profiles, Campaigns, and TTPs)
- Automatically collect and aggregate OSINT, 3rd party, Labs, and ISAC data
- Automate workflows for quicker analyst insights
- Securely share and collaborate threat intelligence with trusted partners
- Integrate with SIEM, FW, Endpoint, IDS, API, and more

Anomali Match™

Intelligence-driven extended detection and response that helps organizations quickly identify and respond to threats in real-time by automatically correlating ALL security telemetry against active threat intelligence to stop breaches and attackers.

- Detect exposure to current and historical threats within your environment
- Automatically tie indicator matches to threat models (e.g. CVEs and MITRE ATT&CK)
- Search 5+ years of telemetry across 100s of millions of IOCs;
- Automatically correlate new intelligence against historical telemetry
- Automate attack pattern analysis to identify and protect against the attackers “next move.”

Anomali Lens

A powerful Natural Language Processing engine that helps operationalize threat intelligence by automatically scanning web-based content to identify relevant threats and streamline the lifecycle of researching and reporting on them. Lens provides instant access to strategic and tactical intelligence from any mobile or browser page. Analysts at all levels are empowered with real-time context that helps inform their organization to accelerate decision-making.

Threat Intelligence Sharing

Anomali provides a complete threat-sharing platform for ISAC and ISAO partners to power secure sharing and collaboration. Partners leverage ThreatStream to offer their members a branded threat-sharing portal with community training, education, and an Anomali Analyst license.

- Dedicated Trusted Circle in Anomali
- Admin access to vet and control membership
- STIX/TAXII server for programmatic access
- Industry-specific tactical and operational research from Anomali Threat Analysis Center

APP Store

The Anomali APP Store is a unique cyber security marketplace providing instant access to a growing catalog of threat intelligence providers, integration partners, and threat analysis tools.

SDKs

The Anomali SDK Suite is an open and integrated ecosystem that brings a new level of customization and capability to your security program.

Technology Partners

Leverage the Feeds, Enrichments, Integrations, and ULink to unite security solutions and increase collaboration.

- ***Feeds***— Integrate proprietary threat intelligence feeds
- ***Enrichments***— Develop custom data enrichments
- ***Integrator***— Create downstream integrations with SIEM firewalls, endpoint systems, and other security and IT solutions
- ***Universal Link***— Create upstream links that ingest data from vulnerability scanners, big data, SIEM, and other security and IT solutions

Learn More

Visit us at www.anomali.com to learn more or schedule a demo.

About Anomali
Anomali is the leader in intelligence-driven extended detection and response (XDR) cybersecurity solutions. Anchored by big data management and refined by artificial intelligence, the Anomali XDR platform delivers proprietary capabilities that correlate the largest repository of global intelligence with telemetry from customer-deployed security solutions, empowering security operations teams to detect threats with precision, optimize response, achieve resiliency, and stop attackers and breaches. Our SaaS-based solutions easily integrate into existing security tech stacks through native-cloud, multi-cloud, on-premises, and hybrid deployments. Founded in 2013, Anomali serves public and private sector organizations, ISACs, MSSPs, and Global 1000 customers around the world in every major industry. Leading venture firms including General Catalyst, Google Ventures, and IVP back Anomali.

ANOMALI