ANOMALI

Anomali Integrator

Share integrated data, intelligence, and insights across your security ecosystem

Maximize your security investments with integrated intelligence

Effective cybersecurity depends on comprehensive visibility and actionable insight, but blind spots, siloed security solutions, and high storage costs for Security Information and Event Management (SIEM) data make this hard to achieve. As a result, security teams often lack the context they need to address vulnerabilities, protect critical assets, and respond quickly to security events.

Anomali Integrator works at the heart of the Anomali Security Operations platform to automatically distribute threat intelligence across your on-premises and cloud security infrastructure. Data from Anomali ThreatStream, the world's largest threat repository, is filtered according to your own criteria, pushed into Anomali Security Analytics for correlation with vulnerabilities in your own environment, and fed into your existing security controls for real-time, intelligence-driven defense.

By automating and orchestrating the distribution of relevant intelligence throughout the Anomali platform and across your security controls, Integrator makes your entire security infrastructure smarter and more effective.

Automate and orchestrate security

Direct integration

Seamless connections with firewalls, SIEM systems, proxy, DNS, messaging systems, and endpoint protection platforms reduce incident response times by up to 30%

Customized intelligence

Analysts can automatically filter threat intelligence from Anomali ThreatStream by relevance and criticality to work more quickly and efficiently

Versatile compatibility

Support for a broad range of data formats (CSV, Syslog, JSON, SNORT, CEF) ensures compatibility with existing security controls

Rapid threat management

Customized, automatically distributed threat intelligence helps teams work faster to identify, prevent, and respond to breaches

Integrate customized threat intelligence into your existing security ecosystem

Operationalize threat intelligence

Empower security teams with actionable intelligence on IOCs, IOAs, and TTPs to identify and address points of vulnerability while there's still time to prevent a breach.

Reduce response times

Integrate comprehensive threat insights directly into your operational tools for real-time defense mechanisms that can reduce incident response times by up to 30%.

Improve operational efficiency

Lower the cost of managing and storing telemetry data across security controls while maximizing the value of existing security investments.

Future-proof security

Adapt to the rapidly changing threat landscape and stay ahead of potential breaches with a flexible, easily adaptable solution compatible with a broad array of controls.

Key capabilities

- Out-of-the-box integrations with endpoints, SIEM, firewalls, proxies, DNS, and more
- Built-in SDKs for custom integrations
- Broad system compatibility through support for data output formats, including CSV, Syslog, JSON, SNORT, and CEF
- Web-based interface to configure, manage, and view threat intelligence sites and integration destinations
- Workflow automation to disseminate intelligence to security controls
- Easily configurable rules for filter sources, destinations, and threat information
- In-product notifications of source or destination sync failures, as well as available third-party updates
- Flexible deployment on-premises, air-gapped, or in the cloud
- Integrates ThreatStream AirGap system with existing security solutions
- Integrates with ThreatStream OnPrem for direct download of private intelligence from OnPrem and public intelligence from ThreatStream Cloud

The Anomali Security Operations Platform

Anomali ThreatStream

The world's largest threat repository, Anomali ThreatStream captures raw threat data in real time to power the LLM at the heart of the Anomali Security Operations Platform. IOCs and IOAs are immediately correlated with relevant telemetry to drive actionable insights.

Anomali Security Analytics

Built in the cloud for massive scale and speed, Anomali Security Analytics consolidates SIEM, SOAR, UEBA, and TIP capabilities into a best-in-class, AI-driven solution at a fraction of the cost of competing offers.

Anomali CoPilot

The integrated generative AI capabilities of CoPilot makes our Security Operations Platform the fastest and most comprehensive solution in the market. Based on an LLM using the industry's largest threat repository, CoPilot mitigates hallucinations for accurate, actionable insights in plain language. The perfect partner for every analyst at every level.

Anomali ASM

Anomali Attack Surface Management provides comprehensive visibility into all your IT assets, including shadow IT, to fuel actionable security analytics. Real-time monitoring flags outdated policies, misconfigured assets, and other at-risk entities.

ANOMALI