ANOMALI

Data Sheet

ANOMALI ANOMALIZER

Anomali Anomalizer mobile application provides mobile access to your Anomali ThreatStream information via Dashboards, Search, and Chat.

Explore and summarize threat intelligence faster with Anomalizer dashboards, search workflows, and on-device AI analysis.

ANOMALIZER CAPABILITIES AT A GLANCE:

- **Dashboards:** Browse pre-built views and switch dashboards to spot patterns quickly
- **Chat:** Ask natural-language questions and get structured, readable results
- **Search and Advanced Search:** Query and refine results with structured filtering
- **Scan and Summarize:** Paste a URL or text and generate a clear summary with key takeaways
- **Export:** Share results as text or PDF for reporting and collaboration
- **Demo mode:** Demo mode lets you explore core workflows without signing in. Demo exports are labeled “Data simulated for training purposes.”

DASHBOARDS

Explore and analyze your organization’s threat data through dashboards. Use the built-in dashboards to get started or create custom dashboards tailored to your workflow. Dashboards let you visualize and analyze key security and IT operations data for your organization. You have access to all built-in and user-defined dashboards available in the browser version. You can also use the Search functionality to create new dashboards directly in the app or import them using a JSON file. Any dashboards you create can be shared with others in your organization and configured to fit your needs.

SEARCH

Search lets you submit natural language search requests and automatically converts them into Anomali Query Language (AQL) to search and analyze enterprise IT and security event logs. Results can then be transformed into dashboards and used alongside ThreatStream or any user-defined dashboards available in the browser version.

CHAT

Chat lets you discuss threat intelligence in real time, providing precise answers backed by Anomali's verified sources and search data. Asset Analyzer accessible through Anomalizer Chat, streamlines threat detection by removing the need for traditional alert workflows and SOC playbooks. It enables inside-out threat analysis of your organization's assets using ingested logs stored as a lookup table in Security Analytics. The lookup table provides a high-level view of your internal assets, giving analysts a clear picture of network exposure and overall security posture. Anomali refreshes this data daily to keep it current and actionable.

SCAN AND SUMMARIZE CONTENT

Anomalizer can scan and summarize cyber threat information from web pages and PDF files. Using advanced natural language processing (NLP), it analyzes the content — whether a breach analysis article or raw intelligence data — and identifies key threat entities such as Actors, Malware, and observables. Scan results and detected entities can then be used to create Threat Bulletins and Threat Investigations.

PRIVACY

Anomalizer performs on-device AI analysis. Your prompts and content stay on your device. Everything is processed locally — nothing is ever sent to a cloud AI service.

When connected, Anomalizer retrieves threat intelligence via secure, authenticated requests. The app does not upload your local intelligence content for AI processing.

Anomalizer is built for privacy-sensitive environments:

- No third-party analytics or crash reporting SDKs
- No third-party binaries
- Clear demo-mode labeling for exports

GET STARTED WITH THE ANOMALIZER APP VIA THE APPLE APP STORE

To use the Anomalizer application download it from Apple Store the same way you download other applications to your iOS device.

TO START USING THE ANOMALIZER APP:

1. After downloading the Anomalizer app from Apple Store, tap Install to install the Anomalizer app on your iOS device.
2. Tap Accept to accept the terms of service and then tap Done
3. Sign in using your preferred method.

Apple App Store Link: https://apps.apple.com/us/app/anomalizer/id6739704964

PLEASE CONTACT ANOMALI SUPPORT WITH ANY QUESTIONS

Request Support