ANOMALI

GUIDE

Four Benefits of Augmenting Splunk with Anomali

Search petabytes of data in seconds

Four Benefits of Augmenting Splunk with Anomali

Search petabytes of data in seconds

It's not your imagination: the tech world has changed dramatically over the last four years. ChatGPT catapulted to the forefront of global attention. Quantum computing actually became a thing. And cybercrime increased by more than 600%.

Given that the average cost of a data breach is $4.88M, addressing vulnerabilities in your security infrastructure has never been more mission critical. If you're using Splunk Enterprise Security, this means you've got some significant gaps to patch, including being able to quickly and affordably search all of your current and historical event log data, beefing up your threat intel, and making sure that every analyst on your team is ultra-productive and efficient.

The good news is that Anomali's transformative AI-Powered Security and IT Operations Platform gives Splunk Enterprise Security customers comprehensive visibility, speed, AI, and world-class threat intelligence in an easy-to-use integrated platform.

What's Past is Prologue

Lookback data is critical for correlating threat intel with internal telemetry. It helps you identify and understand long-term patterns, uncover dormant threats, and investigate breaches that may have originated months or even years ago.

While accessing the past is valuable, if not done right, it's not cheap or time efficient.

Splunk's pricing tiers are based on the amount of data held in "hot," "warm," and "cold" storage. Hot data resides on its fastest/most expensive storage devices for quicker retrieval; cold data on its slowest/least expensive storage devices. Retrieving and searching cold data with Splunk, while cheaper, can be agonizingly slow, making deep retrospective analysis impractical and giving an attack more time to gain traction.

Adding Anomali Copilot and Security Analytics to your Splunk deployment is a game-changer for retrospective search for cost and performance.

With Anomali, all data, regardless of age, is hot and readily accessible for rapid searching, with no additional storage cost. And it's lightning-fast. How fast? **You can search petabytes of data in seconds (compared to minutes or hours with Splunk)**, so you can detect and investigate that three-year-old malware bomb before it detonates!

How the Anomali Platform Satisfies Your Need for Speed

Anomali is purpose-built to offer the fastest search in the industry. Here's how it's done:

- **Cloud-native architecture:** Anomali's cloud-native design makes it scalable enough to handle petabytes of data without compromising performance. It leverages lossless compression algorithms to reduce data storage requirements. It efficiently ingests logs to ensure rapid data availability.
- **Serverless:** Anomali's serverless architecture enables SOCs to scale resources on demand. This efficiency significantly improves response times and overall performance.
- **Agentless:** Anomali enables you to deploy faster and more efficiently since its agentless design means that there's nothing to install, update, or patch. It also makes your deployment easier to manage and scale. Other benefits of agentless architecture include easing compliance headaches, reducing your attack surface, and decreasing endpoint load (since there is no consumption of endpoint resources, such as CPU or memory). Not to mention it reduces the risks posed by agents and witnessed in recent global outages
- **Integrated Security Data Lake:** At the heart of Anomali's groundbreaking approach is its integrated Security Data Lake. This powerful feature efficiently manages the exponential growth of security data, providing high-speed collection, processing, and analysis at scale — all while keeping costs low. With Anomali's Data Lake, all of your data is hot.

A customer reported that using **Anomali reduced their investigation and correlation search time from an average of 44 minutes to under 40 seconds!**

Skip School

Splunk University: It's expensive. It's time-consuming. And it's necessary. Or is it?

Like most traditional SIEMs, Splunk requires analysts to master a proprietary query language, which requires advanced skill sets. Given the dearth of analyst talent (and the high cost of specialized talent), this presents a major obstacle for a growing organization. Constructing queries can also be complex and cumbersome, even for senior analysts.

Anomali's AI-Powered Copilot's natural language processing (NLP) enables users of all skill levels to conduct sophisticated threat-hunting tasks simply by asking questions in their own language (it supports more than 80 languages!). This empowers junior analysts to perform at the level of far more experienced team members and reduces the need to hire highly skilled (and expensive) team members.

As an added bonus, Copilot significantly reduces the time required to investigate newly reported threats. A recent Anomali customer reported that using Copilot reduced their investigation and correlation search time from an average of 44 minutes to under 40 seconds!

Increase Your Threat IQ

Splunk offers customers only a dozen or so threat intelligence feeds and delivers periodic security content updates via a manual upgrade process. In contrast, Anomali ThreatStream provides curated access to more than 200+ threat intelligence feeds from a wide range of sources, including open-source intelligence (OSINT), commercial feeds, dark web monitoring, and proprietary research.

As the pioneer in Threat Intelligence Platforms (TIPs), Anomali integrates the world's most comprehensive threat intelligence repository into security operations, detecting and responding to threats faster and more accurately than ever before. Whereas Splunk's limited intel means it can only detect roughly two million IoCs, Anomali detects millions more.

You can also add threat intel feeds (often with free trials) via the Anomali App Marketplace. This diverse, customizable library covers a wide spectrum of potential threats and attack vectors mapped to the MITRE ATT&CK® framework.

Intel in action

Threat intelligence shouldn't live in a silo. That's why Anomali Integrator infuses threat intel into the security workflow — including alerts and incidents — ensuring seamless data analysis, better contextualization of threats, and faster detection and response.

Anomali ThreatStream provides analysts with the AI-enriched threat intelligence they need to understand their threat landscape, security posture, and in-progress attacks. The solution filters and prioritizes data by relevance to help security teams focus on what's essential and optimize decision-making at scale.

With ThreatStream you can:

- **Transform data into insight** – Capture, curate, and enrich raw threat data to help security teams quickly understand the context of SIEM and SOAR alerts.
- **Operationalize threat intelligence** – Respond quickly to emerging threats and potential attacks with real-time, automated blocking and monitoring.
- **Speed research and investigations** – Accelerate triage and incident response with a complete research, analysis, and publication workbench.
- **Distribute and collaborate on intelligence** – Share high-quality threat bulletins and finished intelligence products with stakeholders within and beyond your organization.

Imagine investigating a suspicious IP address and seeing relevant high-fidelity threat intel alongside your internal log data in real time, immediately drawing your attention to the connection. This holistic view allows analysts to make faster, more informed decisions, reducing the time from detection to resolution.

Anomali also integrates data from vulnerability assessment tools like Qualys, allowing for risk prioritization based on real-world activity. By leveraging the MITRE ATT&CK framework, Anomali provides deep context across strategic intelligence, enabling analysts to assess and respond with great efficiency.

Upgrade Splunk Enterprise Security with Anomali

Anomali's transformative AI-Powered Security and IT Operations Platform gives Splunk Enterprise Security customers comprehensive visibility, speed, AI, and world-class threat intelligence in an easy-to-use integrated platform. It provides first-in-market speed, scale, and performance, consolidates your tech stack, and empowers your team to do more with less.

Innovative, effective technology. Cybersecurity solutions for organizations of all sizes. AI-powered intelligence-driven solutions for a more secure world. That's Anomali.

Discover how Anomali can help you create a robust, highly adaptive security solution. Schedule a demo of Anomali's Security and IT Operations Platform to see why it's different and how it can transform your organization's cybersecurity.

Security and IT Operations Done Differently.

Anomali is the leading AI-Powered Security and IT Operations Platform that delivers mind-blowing speed, scale, and performance at a fraction of the cost. Our cloud-native approach modernizes the delivery of legacy systems, combining ETL, SIEM, Next-Gen SIEM, XDR, UEBA, SOAR and TIP to deliver security analytics that enable our customers to detect, investigate, respond, and remediate threats in one integrated platform.

Request a demo to learn more about the Anomali AI-Powered Security and IT Operations Platform.

ANOMALI