ANOMALI

GUIDE

Anomali vs QRadar

5 Ways to Compare and Evaluate

Anomali vs QRadar

5 Ways to Compare and Evaluate

When IBM sold off its relatively new QRadar Suite SaaS division, IP, and customer list to Palo Alto Networks (PAN), QRadar customers were left with an unexpected dilemma. Should they stay with IBM and deploy QRadar on premises, which has limited support? Migrate to PAN's Cortex XSIAM product? Or explore other options?

In short, should QRadar even be on your radar anymore?

The concern is understandable. This merger opens a host of unknowns, such as:

- How long will PAN support QRadar customers?
- What happens to innovation? Is the product roadmap dead?
- When (not if) will you be forced to migrate to a new platform?
- If you migrate, will pricing change?

This is no longer the same organization from which QRadar customers originally purchased. The team's leadership, product innovation, and mission have changed. That's why so many QRadar customers are exploring alternative solutions like Anomali.

Security and IT Operations Done Differently

Anomali brings a modern approach to the SIEM market, consolidating security and IT operations into one easy-to-use, AI-Powered, integrated platform. It enables you to detect, investigate, respond, and remediate threats at quantum-quick speed at a fraction of the cost of other solutions.

Five Ways Anomali Outperforms QRadar

Here are the top five reasons why Anomali is superior to QRadar in terms of cost, ease of use, search speed, threat intelligence, and tools for beginning threat hunters.

1. Straightforward Cost and Operating Model

QRadar's pricing models are confusing, with limits on storage duration. User behavior analytics (UBA) runs as a separate limited app on AppExchange, which limits the functional threat detection and the tactics, techniques, and procedures (TTPs) it can identify. QRadar's UBA solution is not fully featured. It provides only high-level functionality, including user behavior but not entity behavior.

QRadar's Analyst Workflows app consolidates information to reduce clicks but does little to streamline investigations, as it lacks many administrative features that were available in the old interface. This leaves the organizations with two interfaces, and most still prefer the old legacy one. Advisor with Watson makes investigations a bit less manual manual, but it is an add-on. Pricing is extremely high and it's difficult to implement. Also inconvenient: QRadar's new Analyst Workflows UI requires users to pivot back and forth between interfaces, as they are not integrated.

Moreover, QRadar UBA provides only a rudimentary mapping of IP to machine names and users, a feature that defines true user entity and behavior analytics (UEBA) solutions. The result is a legacy reliance on correlation rules and fewer machine-learning-based anomaly detections, which may lead to missed threats and longer dwell times in the network.

QRadar UBA is limited to viewing:

- Monitored users
- Recent offenses
- System score
- Risk category breakdown
- Active investigations

In contrast, Anomali Security and IT Operations Platform provides complete real-time, historical security telemetry across your environment. Security Analytics combines the core functionalities of ETL, SIEM, Next-Gen SIEM, XDR, UEBA, SOAR, and TIP into one intuitive platform. Curated native threat intelligence enriches alerts with contextual insight on potential adversaries and their attack flows, empowering you to stop breaches in their tracks.

Anomali's integrated, nimble UEBA approach and superior threat intelligence offers clear attack modeling and flow visualization. It provides analysts with answers to the most important questions — what, where, when, and how — so they can quickly investigate and remediate threats.

Additionally, you'll save money on licensing costs, maintenance, and support. The QRadar Suite can be cost-prohibitive (both from purchase, maintenance, and usage perspectives), particularly for smaller enterprises. Anomali's base price and faster time to value significantly lowers the total cost of ownership.

2. Speedy Search

QRadar Suite was touted as the solution for legacy onsite and bare metal limitations, namely scalability, speed of scoping new data flows, and sources of expansive data sources. Whether it lives up to the hype is debatable.

QRadar's data lake is backed up to AWS. However, scaling your infrastructure to accommodate increasing data volumes and new data sources requires additional licensing, and QRadar will throttle event flows to keep you under your licensed limits. It relies on a legacy architecture for storing data and retention which in turn, lacks speed and performance. If you are in the middle of a ransomware or other large-scale systemic attack, this event throttling impedes the mean time to detect and respond. In addition, it is difficult to access anything beyond the 90 days of hot searchable data, and it is very expensive to increase the amount of data beyond that period.

Anomali's Data Lake keeps all your data hot and available, so you can search seven-plus years of your data almost instantaneously. It can search up to 2 PBs in 9 seconds. One Anomali customer reduced correlation search time from 48 minutes to 44 seconds!

What Makes Anomali So Fast?

Anomali's integrated Data Lake uses AI to run queries in the most efficient way possible, dynamically spinning up the processing power for the length of time necessary to obtain results and then shutting it down when you don't need it anymore. Because Anomali's Data Lake is cloud-native and has serverless architecture, you won't be running an inefficient environment mismatched to your needs 24x7.

3. Superior Threat Intelligence

IBM's X-Force Threat Intelligence Plug-in is required to integrate threat intel into QRadar's platform. It is a smaller, specialized tool that does not offer a comprehensive software solution for collecting, analyzing, and distributing threat intelligence data from various sources. In addition, the IBM QRadar Security Threat Monitoring Content Extension is required to gain access to rules, as well as to build blocks and customize rules. Basically, it enhances an existing system with threat intelligence — such as enriching alerts with threat insight — but it does not manage the entire threat intelligence lifecycle. QRadar limits both feed ingestion and total number of indicators of compromise (IoCs) that can be integrated into the platform. Gaining more intelligence would require subscription to more premium offerings from XForce, still doesn't provide the aimed visibility into threat intelligence and its IoCs.

Anomali ThreatStream is a dedicated platform built around the entire threat intelligence lifecycle. It is the leading TIP, providing curated access to more than 200+ threat intelligence feeds from diverse sources, including OSINT, commercial feeds, dark web monitoring, and proprietary research. Users can also add premium 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.

Anomali's threat intelligence doesn't live in a silo. The Anomali Security and IT Operations Platform infuses it into all alerts and incidents. This integration ensures seamless data analysis and better contextualization of threats, leading to more efficient detection and response.

Anomali is also an active member of the threat-sharing community. ThreatStream's Trusted Circles facilitates secure and efficient threat intelligence sharing among predefined groups, such as industry-specific consortia, government bodies, or partner organizations. These circles enable participants to immediately share relevant threat data, while maintaining control over what is shared and with whom. This collaborative approach improves individual organizations' security while contributing to the broader cybersecurity ecosystem.

4. Tools to Empower the Tier-1 Analyst

QRadar Sigma, which automatically converts to Kusto Query Language (KQL), is no longer available with the on-premises solution, and is only available with the Watson Add-on for the cloud-native solution that is now being discontinued. Without Sigma or KQL, QRadar won't help new analysts who are unfamiliar with query languages or scripting. Also, if you are trying to augment your team by recruiting from other disciplines, such as network operations, IT support, or other application or help-desk functions, you'll be looking at a major ramp-up period and training investment (even if your new hires have domain knowledge). Given the uncertain future of the product, this may be an unwise investment.

Anomali Copilot uses LLMs with curated access to the industry's largest repository of global threat intelligence, providing actionable insights in plain language. It bridges the gap between lower tiers of SOC analysts and threat hunters with easy-to-use AI-based tools and automated threat summarization. Analysts can pull web-based threat summaries into Anomali to compare with internal telemetry, enabling them to flag suspicious events as soon as they occur. Anomali's AI empowers your Tier-1 analysts to be more proactive in fighting threats.

5. Wanted: A Simple Interface

QRadar is known for having an out-of-date, difficult-to-utilize user interface. The product is hard to maintain, deploy, and learn, and has limited functionality in both prebuilt analytics and custom rules. In addition, since the platform's threat intelligence service is a plugin that feeds the platform, there is no way to pull in new threat information or advisories from the web. The net result is a woefully disconnected user experience.

As a cohesive platform, Anomali integrates the entire workflow from threat detection to response. Visualizations allow SOC analysts to pivot around based on event, IP, credential, or indicators of compromise (IoC) before responding. This helps the SOC team answer the burning questions faster:

- What activity is critical in priority?
- Have we seen a published attack or advanced persistent threat (APT) group in our environment? If so, when?
- Can we stop this activity right now?

Has QRadar's Roadmap Hit a Dead End?

Neither IBM nor PAN require QRadar customers to migrate to the new platform immediately. While this allows time to evaluate next steps, it also signals the end of innovation. IBM has diverted resources away from QRadar, moving some product teams to other company divisions and laying off many others in a reported effort to "rebalance" its workforce.

Many will attest that when it comes to QRadar R&D, IBM has been phoning it in for quite some time. Its dashboards and visualizations are somewhat antiquated. For example, there's no way to quickly pivot into an entity-level discovery of what's going on. Likewise, there's no simple process to unearth the scope of incidents or grasp what happened or in what order.

Anomali: The Future of SIEM

Even though QRadar customers don't have to make an immediate decision about what to do next, it's clear that the product they purchased is not the same one they'll have going forward, making this the perfect time to explore other options, such as the Anomali Security and IT Operations Platform.

Anomali was built from the ground up to work seamlessly with every device, cloud, and log source in your environment. And unlike other security operations platforms with suites of loosely coupled applications, Anomali's groundbreaking Security and IT Operations Platform combines ETL, SIEM, Next-Gen SIEM, XDR, UEBA, SOAR, and TIP into one integrated, easy-to-use AI-Powered solution.

Anomali enables you to detect, investigate, respond to, and remediate threats at blazing-fast speed at a fraction of the cost of competing offerings. Anomali provides comprehensive visibility and world-class threat intelligence. It delivers first-in-market scale and performance, consolidates your tech stack, gives you unrivaled time to value, and empowers your team to do more with less.

Innovative, Effective Technology

An AI-Powered intelligence-driven platform 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 security posture.

Security and IT Operations Done Differently.

Anomali delivers the leading AI-Powered Security and IT Operations Platform. Only Anomali integrates ETL, SIEM, Next-Gen SIEM, XDR, UEBA, SOAR, and TIP into one powerful platform. At the center is the Anomali Copilot that navigates a proprietary cloud-native security and IT data lake to drive first-in-market speed, scale, and performance at a fraction of the cost. Modernize security and IT operations to protect and accelerate your organization with better analytics, visibility, productivity, and talent retention.

Be Different. Be the Anomali. **Request a demo** to learn more.

ANOMALI