# Comparative Study: Splunk, New Relic, and Grafana

This document provides a detailed comparative study of Splunk, New Relic, and Grafana based on key features such as monitoring capabilities, integration options, real user monitoring (RUM), data retention, alerting capabilities, reporting features, and deployment flexibility.

## Comparison Table

|  |  |  |  |
| --- | --- | --- | --- |
| **Criteria (Detailed Comparison)** | **Grafana (Advanced Insights)** | **New Relic (Comprehensive)** | **Splunk (Enterprise Level)** |
| Monitoring Capabilities | Extensive visualization tools, supports Prometheus for metrics monitoring, Grafana Loki for logs. | Advanced APM for full-stack observability, real-time AI-driven insights. | Industry-leading log monitoring, powerful search queries with SPL (Search Processing Language). |
| Integration Options | Wide compatibility, supports over 30+ open-source tools. | Seamless integrations with cloud-native platforms, APIs for custom needs. | Highly customizable connectors, native support for Splunk Enterprise plugins. |
| Real User Monitoring | Supports third-party plugins such as Google Lighthouse or New Relic RUM. | Built-in functionality for web and mobile applications. | Not included natively, requires external tools like AppDynamics. |
| Data Retention | Depends on connected data sources; can be extended up to years with external storage. | Logs: 30 days, Metrics: Up to 13 months. | Customizable but incurs high costs for extended durations. |
| Alerting Capabilities | Flexible with options to set threshold alerts on dashboards or integrate with tools like PagerDuty. | AI-powered alert systems with anomaly detection and automated workflows. | Pattern-based alerts defined through SPL scripting for logs. |
| Reporting Features | Custom dashboards that can be exported as PDFs or embedded in other systems. | Automated reports with business insights tailored for stakeholders. | Detailed log-based reports, integrated dashboards for IT operations. |
| Deployment Flexibility | Supports both self-hosted and managed cloud solutions (Grafana Cloud). | Fully managed SaaS with scalable plans. | On-premise installation or Splunk Cloud available with flexible licensing. |

## Example Use Case

Use Case: Monitoring a Multi-Region E-commerce Application on AWS  
  
Infrastructure includes:  
- Application hosted on EC2 with auto-scaling.  
- RDS for transactional data, DynamoDB for NoSQL.  
- AWS Lambda and API Gateway for REST APIs.  
  
Monitoring Needs:  
- Real-time user performance tracking (RUM).  
- Alerts for database latency and API errors.  
- Log retention for 90 days for auditing.  
- System health and application performance reports.

## Detailed Comparison for Use Case

|  |  |  |  |
| --- | --- | --- | --- |
| **Feature** | **Grafana** | **New Relic** | **Splunk** |
| Monitoring Setup | Prometheus + AWS CloudWatch | New Relic Agents, Full Integration | CloudWatch Logs + Custom Agents |
| Real User Monitoring | Supports third-party plugins such as Google Lighthouse or New Relic RUM. | Built-in functionality for web and mobile applications. | Not included natively, requires external tools like AppDynamics. |
| Data Retention | Depends on connected data sources; can be extended up to years with external storage. | Logs: 30 days, Metrics: Up to 13 months. | Customizable but incurs high costs for extended durations. |
| Alerting | Flexible Alerts via Dashboards | AI-Driven Incident Alerts | SPL-based, Log Pattern Alerts |
| Reporting | Exportable Dashboards | Automated Reports, Stakeholder Dashboards | Custom SPL-Based Reports |
| Deployment | Self-Hosted or Cloud | Fully Managed SaaS | On-Premises or Cloud |

## Recommendations

- \*\*Grafana\*\*: Best for cost-conscious teams requiring flexibility.  
- \*\*New Relic\*\*: Ideal for seamless AWS integration and advanced observability.  
- \*\*Splunk\*\*: Suited for enterprises needing detailed log analytics.