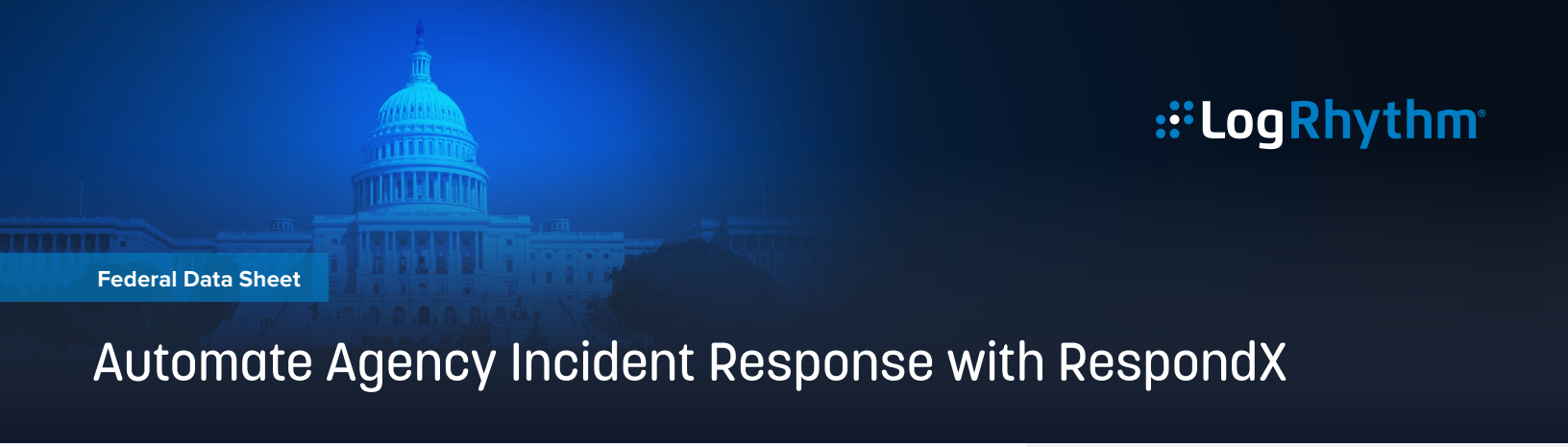


Federal Data Sheet

Automate Agency Incident Response with RespondX

Cybersecurity remains a key concern for federal agencies as threats evolve and infrastructure expands. As enemy nation states and hacktivists invest in new and diverse cyber capabilities, SOC analysts and admins must do more with the same resources. Without changes, federal agencies will continue to face false positives and alarm fatigue that result in periods of threat exposure and fragmented workflows. You need a security solution that frees your team from manual tasks.

With LogRhythm's out-of-the-box automation capabilities and playbooks, your SOC team can automate standard responses to common alerts and alarms, moving the workload to the LogRhythm NextGen SIEM Platform to focus on mission-critical threats. LogRhythm delivers tools to simplify complex processes, speed workflows, and make your team more efficient at addressing cyberthreats.

Amplify Your Team

LogRhythm RespondX, embedded in the LogRhythm NextGen SIEM Platform, simplifies complex processes. RespondX streamlines security workflows by coordinating and automating multiple steps in the response workflow. RespondX enables analysts to quickly collaborate, qualify, and manage incidents, providing drill-down, search pivoting, context enrichment, and other investigative capabilities.

Security teams at any operational maturity level can use RespondX to respond efficiently, address complex use cases, and increase security maturity—without adding more personnel or another solution.

Automate Your Processes

As your security team becomes more efficient, it can take on more complex use cases at scale. RespondX simplifies use cases and reduces workload with orchestration and automation, allowing your SOC team to focus on the most critical incidents. With RespondX, your agency can break down complex use cases into manageable pieces using LogRhythm's Case Management dashboard. LogRhythm SmartResponse™ automation reduces the workload of manual tasks, accelerating response times and decreasing the number of workflow steps. By using standardized processes with Case Playbooks, your team can execute tasks quickly and efficiently. Analysts can also generate reports and show adherence to audit and compliance requirements with LogRhythm's Consolidated Compliance Framework.

For responses that require coordination between multiple tools and technologies, the LogRhythm graphical user interface (GUI) can be used to manually trigger response workflows that initiate actions by Technology Alliance Partner solutions.

Benefits

- **Combat Incidents Faster** by using built-in Playbooks to qualify and investigate threats
- **Improve Collaboration** between agency analysts with Case Management
- **Accelerate Incident Response** and reduce analysts' manual workload via automation
- **Automate Workflows** with approval-based SmartResponse actions

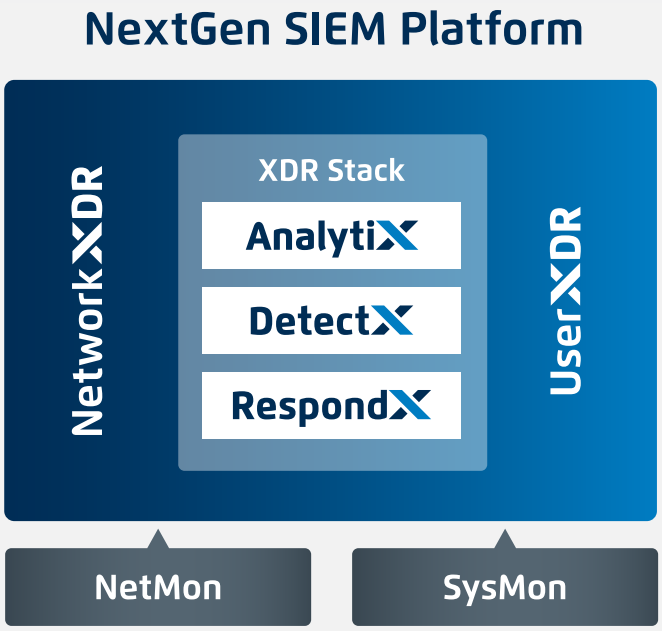
Features

- **Contextualization** enriches agency investigations with instant context lookups
- **Plain-text Search** allows untrained/junior analysts to interact with LogRhythm's platform as experienced users
- **Case Playbooks** standardize incident response processes and knowledge sharing across the security team
- **Case Management** improves compliance with federal regulations by centralizing collaborative incident management and evidence collection
- **Case Metrics** capture key incident response milestones and complete audit trails for reporting
- **SmartResponse** automation integrates LogRhythm's platform with our network of Technology Alliance Partners, enabling faster incident response to help your agency get back to its mission

Advance Your Security Operations Maturity with the XDR Stack

The NextGen SIEM Platform is a comprehensive set of capabilities that include the XDR Stack and other supporting elements:

- AnalytiX is a log management solution that centralizes your log data, enriches it with contextual details and applies a consistent schema across all data types.
- DetectX allows you to focus your efforts with targeted and prioritized threat detection.
- RespondX is a seamlessly integrated security orchestration, automation, and response (SOAR) solution that enables your team to effectively collaborate, qualify, and manage incidents with improved quality and speed.
- NetworkXDR helps you detect and respond to network-borne threats like lateral movement and internal access abuse.
- UserXDR helps you identify user-based threats such as compromised accounts and malicious insiders that can be difficult to detect.
- NetMon provides real-time visibility and security analytics to monitor your organization's entire network.
- SysMon helps you gain access to rich endpoint data to detect and respond to threats faster.



Deployment Options

Software offerings can be pre-deployed on a LogRhythm server or on a server or VM with appropriate specs.

The LogRhythm NextGen SIEM Platform has been awarded Common Criteria Certification at Evaluation Assurance Level (EAL) 2+. The solution has also been awarded a Certificate of Networthiness (CoN) from the United States Army.

LogRhythm solutions are available for purchase via GSA, SEWP, ITES, and all major GWACs or agency BPAs. Contact federal@logrhythm.com for a full list of LogRhythm's certifications and contract vehicles.

Interested in seeing RespondX and the XDR Stack in action?
Request a demo today!

1.866.384.0713 // info@logrhythm.com // 4780 Pearl East Circle, Boulder CO, 80301

www.logrhythm.com