Protecting Federal, State, and Local Agency Networks and Data
U.S. Governmental agencies have become a prime target for disruptive ransomware attacks.

To combat these persistent attacks, for the fiscal year 2021, the U.S. Government has proposed a $18.78bn USD cybersecurity budget, new cybersecurity regulations in the wake of the Colonial Pipeline ransomware attack and subsequent temporary shutdown, and President Biden signed an Executive Order to improve the nation’s cybersecurity.

Your job is to keep your agency’s network and data safe from cyberattacks while meeting strict federal and SLED compliance mandates. But parsing through increasing amounts of log data across disparate systems and cloud applications can leave major gaps in visibility throughout the environment. Prioritizing threats such as ransomware and phishing may become an overwhelming task when strapped with little resources while you push to meet mandatory compliance regulations.

So how do you elevate securing your agency’s operations to the next level? You need to inspire and encourage a security-first mindset across the entire agency domain.

To do so, your team must implement a resilient and adaptable security strategy that builds confidence and agency support to scale your threat detection and response. You have a lot of confidential data at stake across your agency’s network to protect.

From protecting government data in networks that are completely disconnected from the internet to dealing with insufficient cybersecurity funding and skills shortages, you need the right security partner who can provide you with government-specific security best practices and use cases you can adopt.

No pressure, right? Luckily, there is a holistic solution that can provide your security operations center (SOC) quick time to value and measurable return on investment.

Here’s how LogRhythm can help.
Detect threats earlier and faster than ever before for your governmental agency.

When it comes to stopping threats like ransomware, seconds matter. We built the LogRhythm UI for speed and efficiency. LogRhythm enables you to surface threats, search through log data, make decisions, collaborate, and respond to security incidents faster than ever before. Through machine learning and scenario-based analytics, LogRhythm surfaces emerging threats as they occur so your team can act fast.

Do more with the resources your agency has in place today.

Focus on detecting and responding to threats instead of spending your valuable time maintaining, caring for, and feeding your SIEM. LogRhythm includes a library of continuously updated data processing content and threat scenarios for government agencies, so your team won’t have to spend time writing scripts, building rules, and creating reports. With greater flexibility, your team can customize and tailor it to meet the unique needs of your entire agency’s domain.

Gain deep visibility across your agency’s operational network.

Through its security operations and analytics capabilities, the LogRhythm NextGen SIEM Platform eliminates blind spots across your entire government agency network, giving complete visibility into your IT and OT environments, helping you avoid third-party tactics employed by adversaries to exfiltrate data from your agency.

LogRhythm collects data from physical, virtual, and cloud sources to ensure that you always know what’s happening on your agencies network. You’ll spot and catch every anomaly and threat, including insider threats—enabling you to successfully keep your government’s operations and data safe from cyberattacks.

Prove reduced risk to your agency.

Your enterprise needs to feel confident in your team’s ability to identify and stop threats and keep your agency’s reputation and critical assets secure. And you need the agency to continue to invest in your security programs. With reports that illustrate the types of threats you face and your team’s detection and response trendlines, you’ll be able to readily demonstrate your team’s value.

Build for today’s federal, state, local and educational agencies. Scale for tomorrow.

The amount of data your team is responsible for protecting is large and is growing rapidly. It’s important to know that your investment will easily flex to meet your future needs. The LogRhythm platform scales to massive data volumes while delivering high performance and streamlined administration—reducing your overall operating costs. The LogRhythm platform includes file integrity monitoring (FIM) to prohibit anomalous file access and data exfiltration attempts by malicious actors such the hackers who compromised software maker SolarWinds in December 2020, enabling the hacking, monitoring, and data exfiltration of over 200 organizations around the world, including U.S. government agencies.
Government Agency
Cybersecurity Use Cases

Government agencies are an ever-increasing target for cyberthreats—even transportation systems like ferries are being targeted. Reduce cyber risks to your agency by understanding the top threats that exist, including threats from state-sponsored hacker groups that have targeted government data in the past, such as Cozy Bear, Lazarus Group, Double Dragon, Fancy Bear and Helix Kitten. Know what solutions you need to keep your data safe.

Insider Threats
Upset employees are more willing than most to take intellectual property with them as they leave. Security teams must perform retroactive analysis, real-time analytics of their behavior, and enable automatic alerts and daily reports during their transition. LogRhythm’s user entity behavioral analytics (UEBA) solution, UserXDR, automatically prioritizes and points your team to anomalous user behavior to stop user-based threats quicker.

Meet DoDI 8500.2 Guidelines
The LogRhythm NextGen SIEM Platform helps your team effectively monitor log data applicable to DoDI control guidelines while reducing the cost to meet others. Your team can automate DoDI 8500.2-specific reports helping you meet reporting needs easier.

Keep Up With the Scale and Complexity of APTs
Federal, state and local governments are dealing with an increasing number of advanced persistent threats (APTs). Threat actors target government agencies for many reasons, including ideological beliefs, financial gains, proprietary information, influence elections, and much more. Catching these requires real-time analysis of the visible message and the invisible metadata.
Solutions

Manage Your Agency’s Digital Transformation with Security Information and Entity Management (SIEM)

The LogRhythm NextGen SIEM Platform centralizes data across disparate agency systems, correlating that data to provide a holistic overview of an agency’s environment, helping analysts to stop threatening behavior before damage is done.

Network Detection and Response Ensures Vulnerable Assets are Protected

MistNet NDR by LogRhythm provides a machine learning-driven network threat detection and response solution that eliminates blind spots and monitors your agency’s network and data in real time, helping to maintain control and protect vulnerable assets, even as the Internet of Things (IoT) connectivity continues to accelerate.

User Entity Behavior Analytics

UserXDR, LogRhythm’s UEBA solution, automatically identifies and prioritizes anomalous user behavior, bringing enhanced efficiency to the detection of malicious threats.

Ensure Compliance

Government agencies face increasingly intense regulatory and compliance oversight. LogRhythm keeps up with security frameworks, government regulations, and the latest security developments, continuously updating and maintaining the compliance modules, enabling you to streamline your compliance efforts. LogRhythm’s solutions also support auditing requirements through Compliance Automation Suites with embedded content, which provide for long-term and secure data storage as well as wizard-based data recovery.
To protect your agency from risk, your team must be able to detect and respond to a threat—before your network is compromised. How do you do this successfully? Shorten your mean time to detect (MTTD) and mean time to respond (MTTR) to a cyberthreat.

The LogRhythm NextGen SIEM Platform
Our NextGen SIEM solution operates as your team’s central nervous system to alert on threats and enact countermeasures—all in real time. With LogRhythm, your team will detect and respond to threats measurably faster. Your agency’s security operation will become more effective and efficient through automated workflows and accelerated threat detection and response capabilities.

The LogRhythm NextGen SIEM Platform is comprised of the LogRhythm XDR Stack and LogRhythm UserXDR.

Deploy On-Prem or in the Cloud
LogRhythm Cloud has “In Progress” status for FedRamp Moderate certification to ensure the appropriate level of security is in place for your agency to use our cloud products. Our flexible deployment options ensure that you get the best fit for your agency—no matter what your goals and environmental needs may be. LogRhythm Cloud provides our complete NextGen SIEM experience with the ease and flexibility of a SaaS solution.

LogRhythm XDR Stack
With the LogRhythm XDR Stack, your team has an integrated set of capabilities that deliver on the fundamental mission of your SOC: threat monitoring, threat hunting, threat investigation, and incident response at the lowest total cost of ownership.

Detect
Swiftly search across your governmental agency’s vast data stores to easily find answers, identify IT and security incidents, and quickly troubleshoot issues.

MistNet NDR by LogRhythm
Secure your network against pervasive threats that works alone or in combination with the LogRhythm NextGen SIEM Platform. MistNet NDR by LogRhythm combines machine learning, rules-based detection, and threat intelligence to discover and identify threats across desktops, data centers, and the cloud, enabling agencies to secure their networks against Advanced Persistent Threats (APT). Powered by patent-pending TensorMist-AI™ technology, MistNet NDR uses distributed computing that easily scales data collection and analytics and lowers operating costs.

UserXDR
Detect anomalous user behavior before data is corrupted or exfiltrated with user and entity behavior analytics (UEBA).
Behind the UI of our NextGen SIEM

**Input**
- Real-Time Data Collection (on-prem and cloud-sourced)
  - Security Events
  - System Logs
  - Other Machine Data
  - Flow Data
  - Audit Logs
  - Application Logs

**Analytics**
- Machine Analytics
  - Behavioral Profiling
  - AI & Machine Learning
  - Black/Whitelisting
  - Advanced Correlation
  - Statistical Analysis
  - Deep Packet Analytics
- Search Analytics
  - Unstructured Search
  - Log Analysis
  - Contextual Search
  - Pivot & Drill-Down
  - Visualizations
  - Contextual Lookups

**Output**
- Actionable Intelligence
  - Incident Tracking & Metrics
  - Risk Prioritized Alarms
  - Reports
  - Real-Time Dashboards

**Workflow**
- Security Orchestration, Automation and Response
  - Case Collaboration
  - Evidence Locker
  - Automated Response
  - Playbooks

**Persistence**
- Data Storage and TTL
  - Hot/Warm Tiered Storage
  - Configurable TTL
  - Cold Data Archiving and Retrieval

**Real-Time Data Generation**
- Network Monitoring
  - Gmail, Bittorrent, Dropbox, Lynx
  - DPI & Application ID
  - Full Packet Capture
- Endpoint Monitoring
  - File & Registry Monitoring
  - Process Activity

**Real-Time Context**
- Internal
  - Users
  - Hosts
  - Threat Intelligence
- External
  - Threat Intelligence

**MACHINE DATA INTELLIGENCE (MDI) FABRIC**
- Uniform Data
  - Classification
  - Metadata Extraction
- Threat & Risk Contextualization
- Time Normalization
- Machine Analytics
- Search Analytics
- Input
- Output
An Award-Winning Platform

We’re proud of our accolades. We’ve earned every one of them.

From being a Leader in the Gartner Magic Quadrant for the better part of a decade to receiving the Gartner PeerInsights™ Customers’ Choice designation four years in a row, the recognition we’ve received points to our innovation and dedication to delivering security solutions that help you protect your government agency and its reputation.

At LogRhythm, we understand the complexity of your job. Our laser focus on security translates into targeted innovation to give your team the solutions it needs to overcome the challenges it faces every day. The LogRhythm NextGen SIEM Platform is designed to improve your overall security posture and defeat any threat that attempts to breach your agency.

From R&D to our customer success team, we see ourselves as your partner in the fight against cyberthreats. Customer success is one of our core company values. Let our customers tell you about their experiences firsthand.

Visit www.logrhythm.com to read and watch in-depth reviews from real customers.
Our Commitment to Your Success

LogRhythm Labs

It’s crucial to have resources that keep your agency well informed of the latest incidents and breaches that could pose a threat. LogRhythm Labs can help with a dedicated team that delivers use case content encompassing the latest information on emerging threats, changing compliance mandates, and security best practices for government agencies.

We Can Help

Dealing with the change that comes with running a SOC takes guts, grit, and the ability to establish confidence when faced with uncertainty and doubt. To be resilient, you need to ensure that security is a top priority in your agency and that you can show the value of your program. For this to happen, you must be a change agent and establish a security-first mindset in your company.

Our Professional Services can help you keep pace with a changing security landscape, boosting the performance and effectiveness of your security team and platform. Customers use our service offerings to accelerate time to value, ensure seamless deployment, and tune their platform. Customers also rely on our subscription services to augment their security team with our experts.

LogRhythm lives and breathes the security-first mindset that creates resilience — from being one of the frontrunners to implement the Zero Trust framework for our own organization to our dedication to innovation and education. Together, we can be security first.
LogRhythm’s award-winning NextGen SIEM Platform makes the world safer by protecting organizations, employees, and customers from the latest cyberthreats. It does this by providing a comprehensive platform with the latest security functionality, including security analytics; network detection and response (NDR); user and entity behavior analytics (UEBA); and security orchestration, automation, and response (SOAR).

Learn how LogRhythm empowers companies to be security first at logrhythm.com.

Schedule a demo today.
www.logrhythm.com/demo