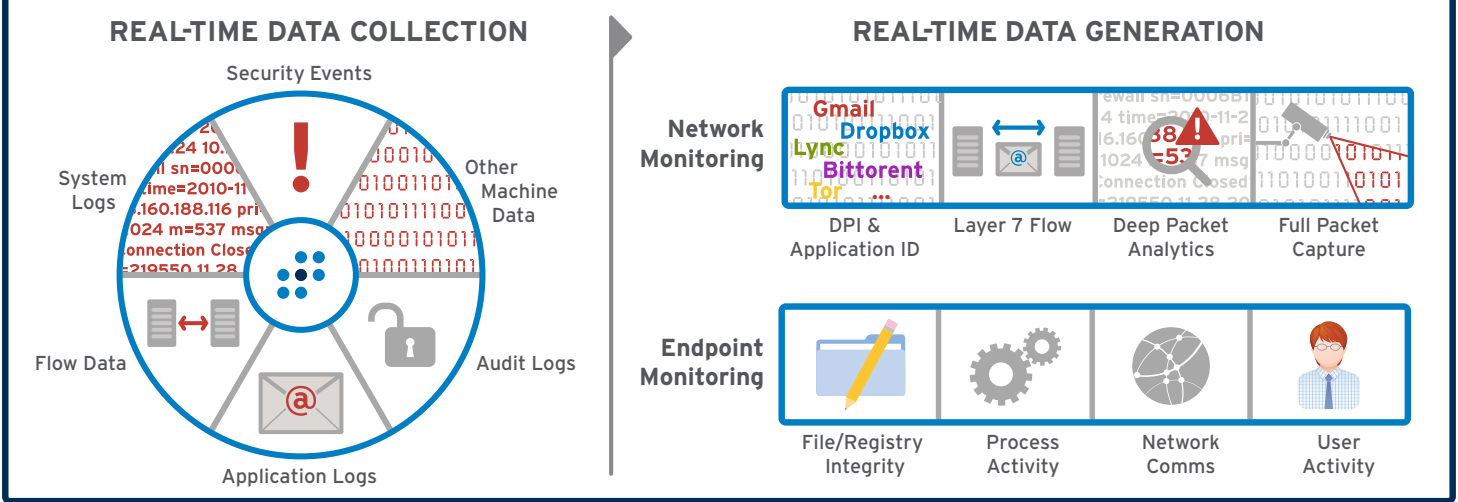


## Threat Lifecycle Management Platform

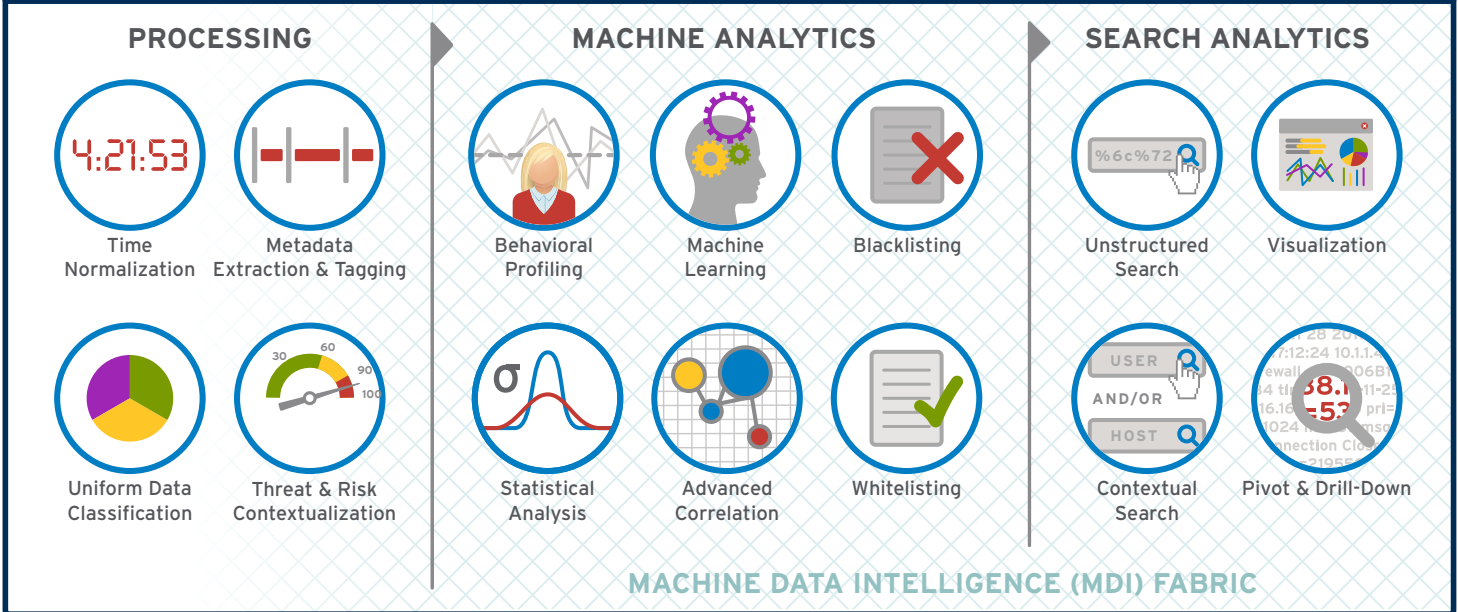
Attacks can originate from both inside and outside your environment. To stop them from resulting in a data breach or other cyber incident, you need a unified view into all threats facing your organization. Use LogRhythm to detect emerging threats and neutralize them quickly.



# INPUT

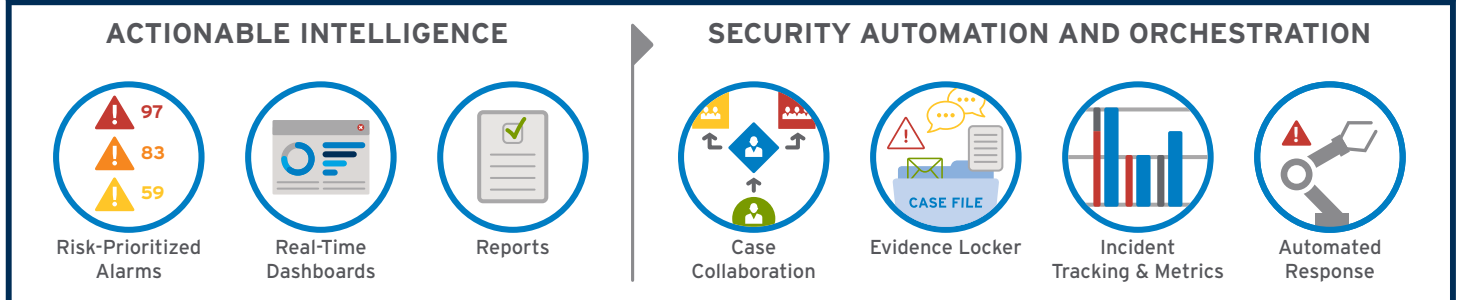


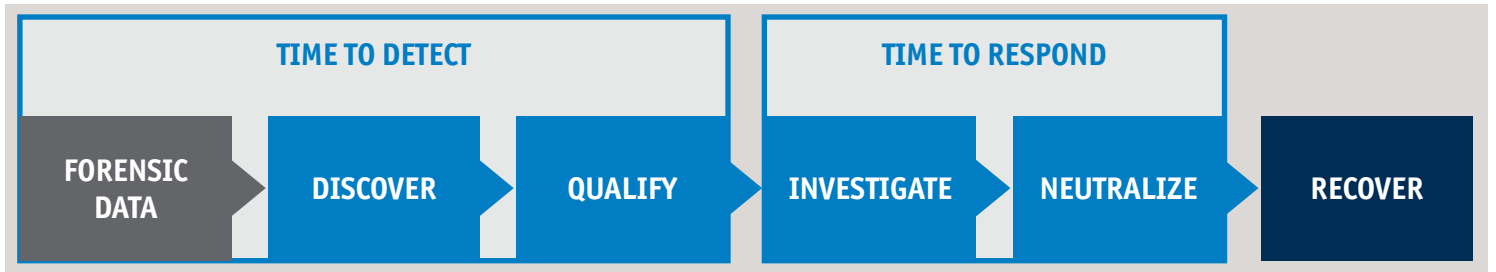
# ANALYTICS



LogRhythm Labs Research & Intelligence

# OUTPUT





## Unify Your Threat Lifecycle Management

### Accomplish Your Mission

Security is your mission. It's ours, too. Empower your valuable personnel with a platform built for security intelligence and analytics. Implement security and compliance use cases quickly and effectively. Focus your team on protecting your organization, rather than customizing a tool.

### Centralize Your Visibility

Gather all of the forensic evidence generated by your IT environment – with or without agents. Eliminate data silos and get centralized visibility with LogRhythm.

### Monitor Networks and Endpoints

Fill in your forensic data gaps with endpoint and network monitoring. Our network and endpoint sensors ensure that you have all of the forensic detail you need to detect and neutralize advanced threats.

### Understand Your Data

Get the intelligence you need, without the noise. Our Machine Data Intelligence (MDI) Fabric automatically contextualizes over 800 different data sources. By extracting metadata and classifying security events, LogRhythm helps you use log and machine data to detect, respond to, and neutralize advanced threats.

### Know the True Time of Occurrence

Don't miss critical attack sequences. Our patented TrueTime™ function records the actual time of occurrence, automatically correcting offsets tied to different time zones, device clocks, and collection latencies.

### Seamlessly Incorporate Threat Intelligence

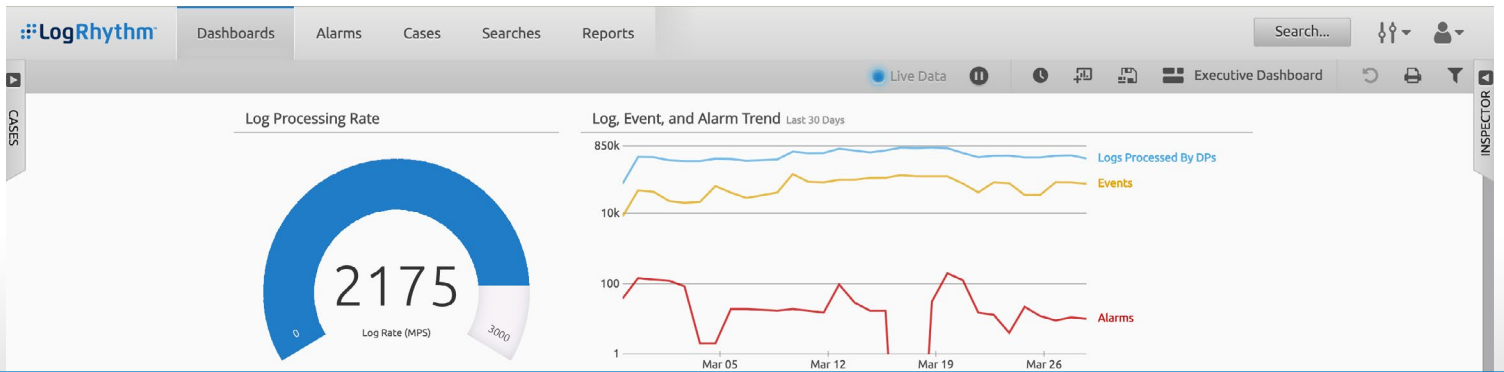
Threats are dynamic and attack vectors change constantly. Stay ahead by using the rich context enabled by threat intelligence from STIX/TAXII-compliant providers, commercial and open-source feeds, and internal honeypots. Use this data to reduce false positives, detect hidden threats, and prioritize your most concerning alarms.

### LogRhythm Labs Supports Your Team

LogRhythm Labs is a research and development team focused on security and compliance. The Labs team develops data processing rules for over 800 devices and applications, security analytics modules to protect your full attack surface, and compliance automation modules for 16 frameworks. The Labs team is comprised of recognized experts in intrusion detection, incident response, malware analysis, compliance, and other critical domains.

“LogRhythm’s security analytics completely changed our visibility and monitoring capabilities to laser focus our time on the alarms that matter the most.”

Source: Security Officer, Large Enterprise Retail Company



## Modernize Your Threat Detection and Response

### Uncover the Most Critical Threats

With machine learning and other automated data analysis techniques, LogRhythm's real-time security analytics help you detect advanced threats. Event corroboration and data-driven threat contextualization calculate a granular risk score for each alarm so your team can focus on the most concerning issues.

### Stop Insider Threats and Account Takeover

You can only shut down compromised accounts if you can see them. Our User and Entity Behavior Analytics (UEBA) illuminate insider threats and stolen credentials so you can catch imposters, identify privilege abuse, and stop user-based threats. LogRhythm Labs regularly develops new UEBA content, including behavioral profiling, peer group analytics, statistical analytics, and advanced correlation to help you stay ahead of new threats.

### Detect Network and Endpoint Anomalies

See what's happening on your network and endpoints to detect compromises like spear phishing and zero-day exploits. LogRhythm's Network and Endpoint Threat Detection Modules are continually updated to ensure you stay one step ahead of cyber adversaries.

### Search with Power and Precision

Get the answers you need, fast. Whether you're hunting for threats or investigating an incident, our search technology's Elasticsearch backend helps you work efficiently. Only LogRhythm empowers you to search with both unstructured and contextualized criteria, streamlining search creation and result analysis.

### Automate and Orchestrate Security Operations

Neutralize threats quickly using the collaborative workflows enabled by our embedded case and incident management function, and automate incident investigation and remediation with pre-staged SmartResponse™ automation actions. Track detection and response times so you can optimize processes over time.

### Streamline Compliance

LogRhythm provides pre-configured compliance automation modules for several regulatory frameworks, including FISMA, GPG 13, HIPAA, ISO 27001, NERC CIP, PCI-DSS, SOX, DoDi 8500.2, NEI 08-09, NIST Cybersecurity Framework, NIST 800-53 and NRC RG 5.71.

## See LogRhythm in Action

We can help you to detect, respond to and neutralize cyber threats before they can damage your business. To see how, watch our online demo at [www.logrhythm.com/demo](http://www.logrhythm.com/demo).



**Gartner**

A 2016 LEADER  
SIEM Magic Quadrant

