Secure Your Healthcare Organization

LogRhythm®

The Complex Challenge of Protecting the Healthcare System

Key Factors Driving Healthcare Security Complexity

Fast-Evolving Threat Landscape

Threat actors are targeting healthcare organizations with a broad range of sophisticated tactics, including phishing, ransomware, credential theft, denial of service, and insider attacks.

Diverse and Dynamic IT Environments

Healthcare IT infrastructure includes a combination of specialized devices, on-premises networks and applications, and cloud services, each with their own risk profiles and security logging approaches.

Demanding Regulations and Standards

Healthcare organizations must comply with strict regulations designed to safeguard protected health information (PHI), often with explicit requirements for reporting breaches and incidents promptly.

Limited Security Resources

While many healthcare organizations are increasing their investments in security, resources remain constrained. This makes it critical to achieve security objectives as efficiently as possible.

The global healthcare system consists of many critical and highly interconnected entities, such as:

- **Healthcare Facilities**
- **Medical Practices**
- **Health Information Providers**
- **Medical Billing Providers**

Given the high-stakes role that these organizations play in daily life, they are attractive targets for threat actors. This is creating unprecedented pressure on healthcare security teams to detect and mitigate security threats quickly — before patient-impacting operational interruptions or exposure of sensitive data can occur.

The Impact is Felt Daily

Even as healthcare organizations invest in new security technologies and ramp up their expertise, there are daily headlines about devastating incidents that disrupt patient care, compromise patient privacy, or both. And the increasingly interconnected nature of the healthcare ecosystem is amplifying the impact of these incidents.

In the five years leading up to 2023, reports from healthcare organizations to the U.S. Department of Health and Human Services reflected:

256%

increase in hacking activity

246%

increase in ransomware

They also reported that large-scale security breaches alone affected 134 million individuals in 2023.

While many healthcare organizations are making steady improvements to their security capabilities and workflows, the scale of the problem keeps growing.

How Cloud-Native SIEM Can Help

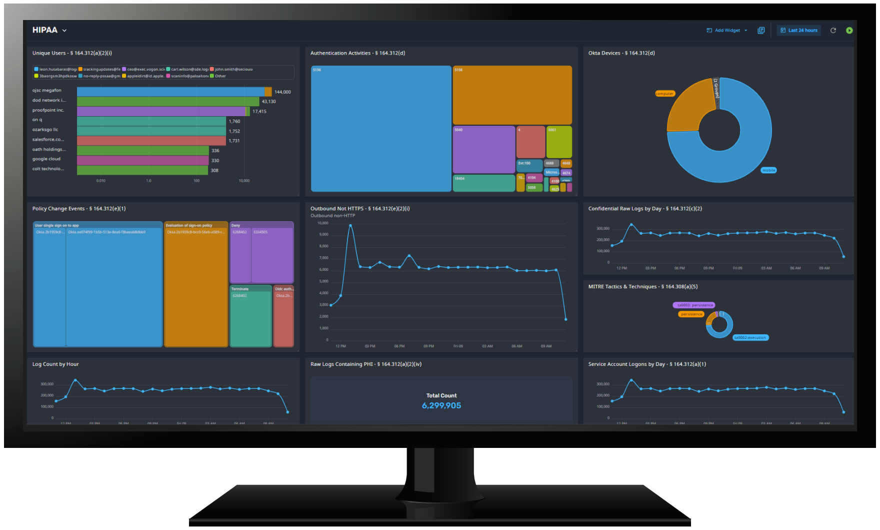
Unified Security Visibility, Detection, and Analytics for Healthcare Organizations

LogRhythm Axon is a cloud-native security information and event management (SIEM) platform that gives healthcare security teams:

- Unified visibility of threats from across environments and device types
- Fast and accurate detection of high-severity security threats
- Actionable guidance to streamline incident response, containment, and recovery
- Flexible and detailed analytics to support threat hunting, strategy, and compliance efforts

It integrates seamlessly with a wide range of on-premises and cloud data sources, such as:

- Healthcare-specific applications, including leading electronic medical record (EMR) and electronic health record (EHR) systems
- Specialized operational technology (OT) and Internet of Things (IoT) devices
- Legacy operating systems and applications


HIPAA
Add Widget
Last 24 hours
Unique Users - § 164.312(a)(2)(i)
ojsc megafon
dod network i...
proofpoint inc.
on q
ozarksgo llc
salesforce.co...
oath holdings...
google cloud
colt technolo...
144,000
43,130
17,415
1,760
1,752
1,731
336
330
308
Authentication Activities - § 164.312(d)
Okta Devices - § 164.312(d)
computer
mobile
Policy Change Events - § 164.312(e)(1)
User single sign on to app
Evaluation of sign-on policy
Deny
Terminate
Outbound Not HTTPS - § 164.312(e)(2)(i)
Outbound non-HTTP
Confidential Raw Logs by Day - § 164.312(c)(2)
MITRE Tactics & Techniques - § 164.308(a)(5)
ta0003: persistence
persistence
ta0002:execution
Log Count by Hour
Raw Logs Containing PHI - § 164.312(a)(2)(iv)
Total Count
6,299,905
Service Account Logons by Day - § 164.312(a)(1)

LogRhythm Axon ingests log event data from these and other available sources, and then normalizes and enriches it using a patented Machine Data Intelligence (MDI) Fabric to enable highly accurate detection, powerful analytics, and full searchability.

Addressing the Most Pressing Healthcare Security Challenges

LogRhythm Axon addresses many of the most significant pain points healthcare security teams face.

Healthcare Security Challenge	How LogRhythm Axon Helps
Security Tool Complexity and Sprawl Many healthcare organizations have a complex patchwork of on-premises security tools that don't scale well or support modern cloud architectures.	**Cloud-Native Deployment Model** LogRhythm Axon's cloud-native approach reduces IT administration overhead while integrating seamlessly with on-premises and cloud data sources.
Security Resource Constraints Healthcare security teams often suffer from alert fatigue and a threat landscape that grows and evolves faster than security budget and headcount.	**Automated Detections and Streamlined Response** LogRhythm Axon's sophisticated detection capabilities mapped to the MITRE ATT&CK® framework zero in on the threats that truly matter. Seamless response workflows highlight contextual information for easy investigation.
Demanding Compliance Requirements Healthcare organizations must adhere to a wide range of regulatory industry-specific and government mandated frameworks and best-practice standards for security and data privacy.	**Integrated Compliance Content** LogRhythm includes out-of-the-box detection content and analytics that is mapped to healthcare-specific regulations such as the Health Insurance Portability and Accountability Act (HIPAA).

Healthcare Security Challenge	How LogRhythm Axon Helps
IT and OT Convergence Most healthcare organizations include a blend of modern IT devices like PCs and tablets and specialized OT and IoT devices that aren't compatible with many security tools.	**Broad Data Source Support** LogRhythm's flexible data parsing capabilities can accommodate both IT and OT data sources, as well as data collection from specialized OT platforms.
Legacy Platform Security Gaps Healthcare organizations must frequently operate legacy platforms that cannot be patched against security vulnerabilities in a timely manner to support critical applications and services.	**Custom Detection Content** LogRhythm Axon makes it easy to create custom detection content that is specifically focused on attack techniques or indicators of compromise for legacy systems.
Specialized Healthcare Asset Types Healthcare organizations rely on many industry-specific IT assets, such as EHR/EMR platforms and other specialized software, hardware, and cloud services.	**Easily Customizable Data Parsing** LogRhythm's flexible data parsing interface makes it easy for IT teams to onboard new and unique log data formats, so critical systems can be included in the threat detection and analytics framework.

> "We started seeing value immediately with the visibility from the dashboards and it has been a game changer for our team. The parsing engine capabilities are a personal favorite."
>
> Director of IT and Security Operations, Leading Healthcare Technology Provider

Enhancing Your Threat Detection and Analytics with LogRhythm NetMon

Automatically detect unauthorized applications and unintentional transmission of PHI on your networks.

Healthcare organizations that deploy LogRhythm NetMon as part of their LogRhythm Axon implementation gain another dimension of visibility and a more comprehensive threat detection capability.

LogRhythm NetMon performs Layer 2-7 packet capture on your networks and then analyzes network traffic to identify unexpected application activity, inappropriate data exposure, and other threats that wouldn't be visible when analyzing log data alone.

In the healthcare setting, this is particularly helpful for discovering protected health information (PHI) and other personal information that is unintentionally transmitted in clear text over the network, creating potential compliance issues.

LogRhythm NetMon integrates seamlessly with LogRhythm Axon to form a unified threat detection and response approach. It also provides advanced capabilities to aid the incident response process, including the ability to drill down into packet and flow data and reconstruct email attachments for malware and data loss investigations.

Our Commitment to Your Success

Quick Time-to-Value and Business Outcomes

While SIEM technology is the foundation of an effective security operations model, success ultimately comes down to people. That is why, in addition to designing LogRhythm Axon to be fast to deploy and easy for analysts to use, we work alongside you to ensure your success.

With every new LogRhythm Axon deployment, we proactively schedule two onboarding sessions and provide three months of included enablement services with weekly check-in meetings. All of this is included with your LogRhythm Axon license.

You can also opt-in for premium ongoing support options and professional services to assist with more in-depth customization needs.

Learn more about our service offerings.

Threat Research and Compliance Expertise

It's crucial to have resources that keep your healthcare organization well informed of the latest incidents and breaches that could pose a threat. LogRhythm Labs is a dedicated team that delivers use case content encompassing the latest information on emerging threats, changing compliance mandates, and security best practices to customers.

Gain insight from industry experts.

Continuous Innovation and Support

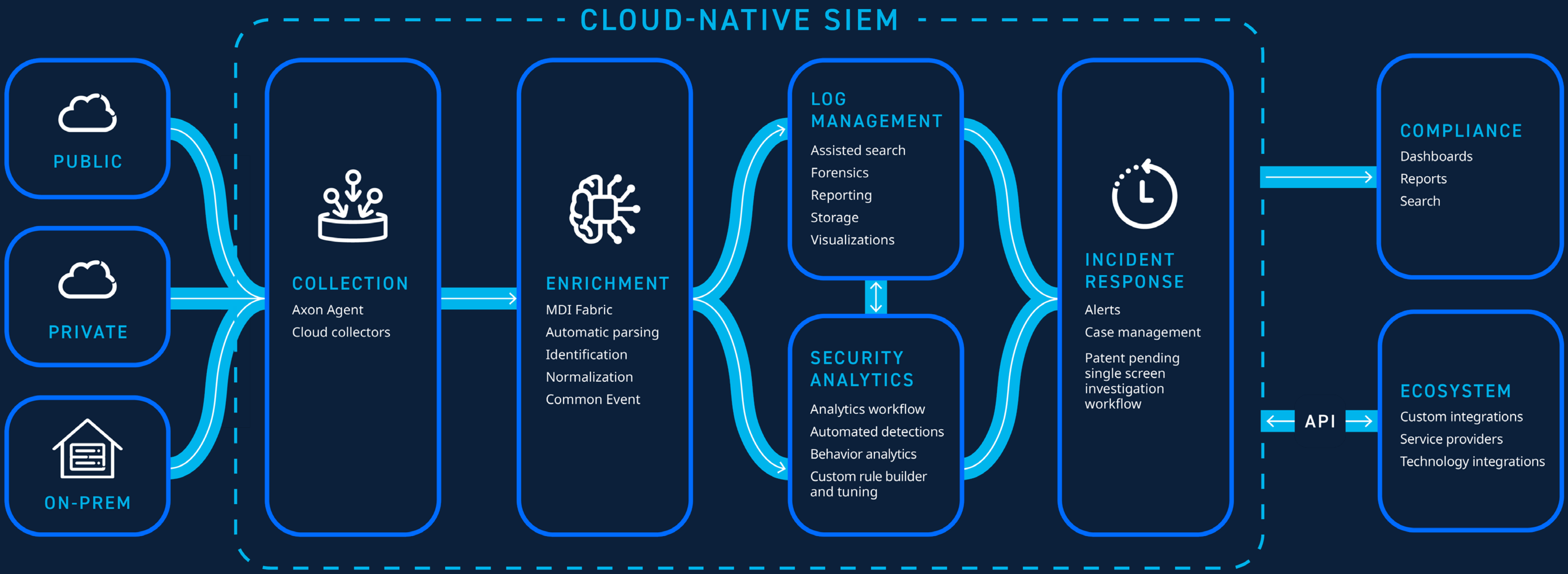
One of the inherent advantages of a cloud-native SIEM like LogRhythm Axon is that, unlike traditional on-premises software, it can be improved continuously without introducing additional workload or disruptions for your security team.

We have a proven track record of delivering innovations every two weeks that all LogRhythm Axon customers benefit from. So, the value you realize from LogRhythm Axon will only grow over time.

View our latest innovations.

> **"I can't say enough how instrumental the teams at LogRhythm have been to our success. It has been wonderful working with a security partner who is truly engaged with their customers. I know they're focused on meeting my needs and value my input as they continue to make bi-weekly releases to LogRhythm Axon."**
>
> Director of IT and Security Operations, Leading Healthcare Technology Provider

Behind the User Interface of LogRhythm Axon



CLOUD-NATIVE SIEM

PUBLIC

PRIVATE

ON-PREM

COLLECTION
Axon Agent
Cloud collectors

ENRICHMENT
MDI Fabric
Automatic parsing
Identification
Normalization
Common Event

LOG MANAGEMENT
Assisted search
Forensics
Reporting
Storage
Visualizations

SECURITY ANALYTICS
Analytics workflow
Automated detections
Behavior analytics
Custom rule builder and tuning

INCIDENT RESPONSE
Alerts
Case management
Patent pending single screen investigation workflow

COMPLIANCE
Dashboards
Reports
Search

API

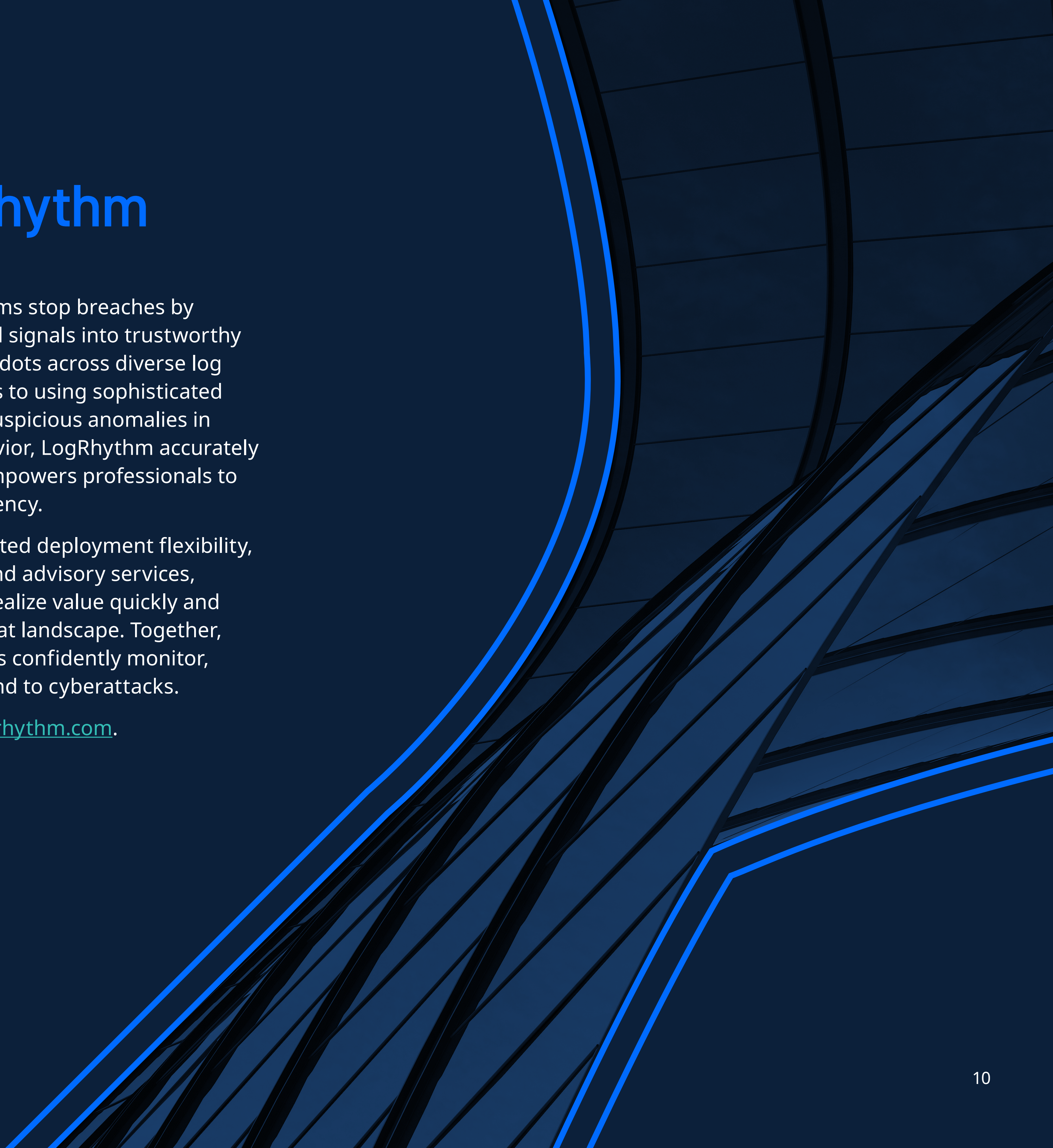
ECOSYSTEM
Custom integrations
Service providers
Technology integrations

About LogRhythm

LogRhythm helps security teams stop breaches by turning disconnected data and signals into trustworthy insights. From connecting the dots across diverse log and threat intelligence sources to using sophisticated machine learning that spots suspicious anomalies in network traffic and user behavior, LogRhythm accurately pinpoints cyberthreats and empowers professionals to respond with speed and efficiency.

With cloud-native and self-hosted deployment flexibility, out-of-the-box integrations, and advisory services, LogRhythm makes it easy to realize value quickly and adapt to an ever-evolving threat landscape. Together, LogRhythm and our customers confidently monitor, detect, investigate, and respond to cyberattacks.

To learn more, please visit logrhythm.com.



LogRhythm®

1.866.384.0713 // info@logrhythm.com // 385 Interlocken Crescent, Broomfield, CO 80021

www.logrhythm.com