



Maintain Compliance While Keeping Costs Down

Category:

Security

Looking For:

Compliance

Industry:

Healthcare

Size:

5,000+ employees

Government regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) Act can pose challenges to companies because they define and limit the ways companies should manage and monitor that data, across the complete IT infrastructure, all staff, and the data's full lifecycle. Adding to this challenge is the need to prove compliance by generating comprehensive reports.

"The healthcare industry is expected to suffer more cyberattacks in 2019 than the average amounts for other industries."

Source: [Cybersecurity Ventures](#)

Example Situation

- Information security and compliance challenges are substantial because of the sensitivity of patient data.
- Government regulations pertaining to the management of healthcare data require not just strict compliance, but also the swift demonstration of compliance on demand.
- Proving compliance means generating comprehensive reports but data volume growth and inadequate infrastructure for managing data increases costs and introduces compliance risks.
- Pressure from senior executives to simplify IT management and reduce operational complexity overall.

Graylog in Action

Both established and start-up healthcare companies are always looking for a way to reduce the costs, complexity, and time required to demonstrate regulation compliance. Using Graylog, the IT department easily keeps costs down, meeting security and compliance needs, including managing growth and demonstrating and reporting on compliance.

Meeting Compliance Needs with Real-time Answers

When new compliance requirements come up, Graylog makes it easy to create new processes for tracking data through its lifecycle. For example, the older data of deceased patients was shifted from high-performance SSD tiers to optical disc for long-term storage. The team built and configured a report using Graylog's Dashboard functionality and built-in chart types, relative time frames, and sophisticated target data rules to show that the transfer process involved only the correct staff members, with the correct privileges. Further, they were able to leverage application logs to demonstrate that the data was subsequently encrypted using AES-256 to secure it against any form of improper access in future.

To address specific audit requirements or align with future changes in regulation requirements, the team created queries that generated formal reports of covering a standard set of data and delivered them via on a scheduled basis to key stakeholders throughout the company. By using Graylog's GUI-based report builder they were able to make sure people got the information they wanted, formatted to showcase the information they wanted without having to ask for it.

For example, an indicator on one of the routers from green to red, the system administrator notes the spike on the widget charting all routers in the infrastructure and immediately drills down into the data, identifies the device causing the issue. The next step is to add the source ID into the parameter field and Graylog will display the results in a new tab. The sys admin clearly sees the root cause of the issue and quickly resolves it before there is any noticeable impact on company operations.

In these types of scenarios, companies have found that the dashboards significantly reduce the time to resolve application or service failure. Faster resolution brings the added benefit of better host maintenance, which extends the life of the host, resulting in reduced replacement costs and subsequently capital expenditure. While every company wants to save money, this is particularly useful for non profit companies, education, government, etc. where the bottom line is scrutinized to stretch every dollar.

Identifying Security Risks Before They Become a Problem

Since IT compliance requires maintaining system security, catching the problem before it impacts compliance is vital. Luckily Graylog's automated alerts make it easy to address different situations that might pose a current or future challenge to compliance. For example, when employees are off-boarded according to HR, all companies, but in particular, companies that are required to comply with regulations such as HIPAA and HITECH, need to immediately delete those employees' logical access to patient data (as is required by law in the case of compliance). The IT team has set up an Alert to fire whenever a former employee tries to access patient data. This alert is combined with a dynamic list of all former employees. When an employee leaves, the team terminates all access and adds the name to the list, which saves time and prevents errors that might arise if you had to update the alert every time.

Lower Ops Cost and Managing Growth

Having a scalable, reliable, and manageable infrastructure is a necessity as the volume of data continues to increase. Graylog is built to open standards for connectivity and

interoperability for seamless collection, transfer, storage, and analysis of log data. Graylog is also SIEM-agnostic by design—Graylog log streams can pass unaltered or enriched data to any application in your monitoring, alerting, and analysis stack. Graylog is the best solution to address increasing data volumes, reduce complexity, enable flexible analysis, and let you do more with your security and performance data while providing a scalable solution that supports current and future technologies.

Summary

Any company involved in healthcare faces numerous compliance challenges along with the need to deliver reports on demand and during audits. Graylog delivers a fast and cost-effective way to meet regulation compliance for all patient data, across its full lifecycle, while also reducing IT complexity and operational costs. Clients consistently note that Graylog offers unmatched performance and query speed make it easy to meet all requests.



ABOUT GRAYLOG

Graylog is a game-changing cybersecurity firm, revolutionizing the way organizations protect against cyber threats. Our solutions are crafted with the latest advancements in AI/ML, security analytics, and intelligent alerting, offering unparalleled threat detection and incident response capabilities. Graylog stands out by making advanced cybersecurity accessible and affordable, ensuring businesses can easily implement robust defenses against the evolving landscape of cyber threats, including the critical vulnerabilities associated with APIs. Our commitment to innovation and simplicity positions Graylog as the go-to partner for businesses seeking to enhance their cybersecurity posture without the complexity and high costs of traditional solutions. For more information on how Graylog can fortify your cybersecurity, visit our website at graylog.org.