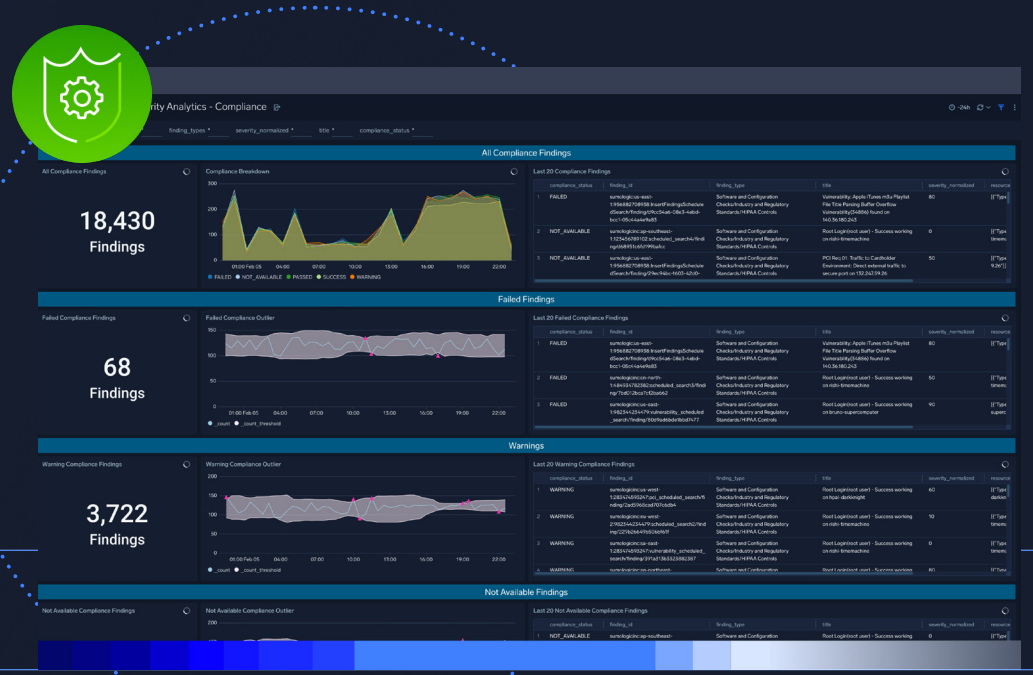
AUDIT AND COMPLIANCE GUIDE

Shorten audit cycles and ensure ongoing compliance



sumo logic

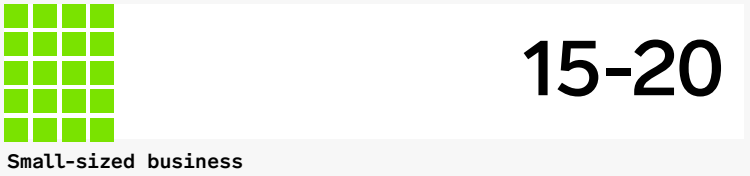
Taming mountains of data

As companies continue to adopt cloud-based software solutions and accommodate remote and hybrid working environments, more and more data is created. Our digital workspaces create a challenge: how do you gather and store this colossal amount of data, maintain the ongoing security of data systems and applications, shorten audit cycles and ensure regulatory compliance over time?

Internal tech stacks pose a big enough challenge, but compliance challenges don't end there. After all, cyberattacks are on the rise, with cybercriminals even targeting small- and medium-sized businesses. And remember that regulations shift quickly as governing bodies attempt to get ahead of cybercriminals.

These issues become especially daunting when you consider that even small businesses, on average, use 15-20 different security tools (while enterprise-level organizations may use 130 or more). Cobbled-together solutions aren't efficient for collecting data, organizing insights and developing actionable solutions to security or compliance concerns.

Security tools



Complexity is an issue for security teams of all sizes. Tools are one place where this issue surfaces.

Anomali Match, April 14, 2022

What is required of companies?

With such a complicated landscape for modern companies, piecemeal solutions to cloud security and regulatory compliance are inadequate. The solution? Leverage a reliable security analytics solution that equips your team with the visibility to easily review your security controls and quickly demonstrate compliance for security audits.

There are two important categories of compliance: regulatory compliance and security controls.

Regulatory compliance may be required depending on factors such as the industry a company operates within.

Internal security controls define how certain data types will be collected, organized, processed, or used to aid the business without creating security vulnerabilities or risking compliance penalties.

The biggest difference between regulatory compliance and security controls is that regulatory compliance mainly relates to standards set by third-party organizations and enforcement bodies. In contrast, security controls are developed, implemented and enforced internally.

Regulatory framework examples

GDPR

The General Data Protection Regulation (GDPR) is a compliance framework that "imposes obligations onto organizations anywhere" if "they target or collect data related to people in the EU." It's a set of standards primarily governing data privacy and security.

HIPAA

The Health Insurance Portability and Accountability Act, or HIPAA, is a U.S. federal law that requires "the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge."

NIST

The National Institute of Standards and Technology, or NIST, is responsible for multiple compliance frameworks related to cybersecurity and privacy controls. Similar to some HIPAA applications, adherence to the NIST framework is voluntary, but its implementation helps companies identify, protect, detect, respond and recover from cybersecurity threats and attacks.

CMMC

The Cybersecurity Maturity Model Certification (CMMC) is an assessment framework developed in alignment with the U.S. Department of Defense (DoD)'s information security requirements. It generally applies to companies that are either DoD contractors or engage with the Defense Industrial Base Sector or DIB.

ISO 27001

The International Standards Organization (ISO) publishes various industrial and commercial standards. These standards — such as ISO 27001 — are vital to world trade initiatives and work to establish common standards for organizations that must adhere to different countries' requirements and priorities.

PCI-DSS

The Payment Card Industry Data Security Standard (PCI DSS) outlines best practices and drives "adoption of data security standards and resources for safe payments worldwide." It is mandatory for any organization handling payment cardholder data. Failure to adhere to it can result in financial penalties.

Security controls

So far, we've discussed formal regulations and requirements. There's another side to compliance, though, that is less standardized — security controls. A cloud security analytics solution helps companies enhance their audit and compliance capabilities through a streamlined platform that collects data, organizes it, makes it accessible and, most importantly, keeps it all secure.

Security controls refer to internally-defined protective measures taken to prevent, detect, or mitigate security risks as they apply to physical assets, information, computer networks or other assets and can include:

Physical

Security controls, which relate to physical facilities and assets — for example, restricting access to server rooms or other sensitive areas or using surveillance cameras for real-time monitoring.

Digital

Security controls, which relate to basic network and application security protocols like required formats for usernames and passwords, two-factor authentication and up-to-date antivirus software.

Cybersecurity

Controls to prevent cyberattacks or quickly mitigate them if they do occur or are suspected; examples include data encryption and firewalls.

Cloud security

Controls generally apply to the protection of cloud-based data and infrastructure across key assets and workflows. Cloud security controls can be more complex because they often involve CI/CD software development pipelines that can change and be updated frequently.

How SoSafe unifies data and shrinks audit cycles

Sumo Logic worked with software company SoSafe to develop and implement a solution to shorten audit cycles and ensure compliance through improved data observability and security.

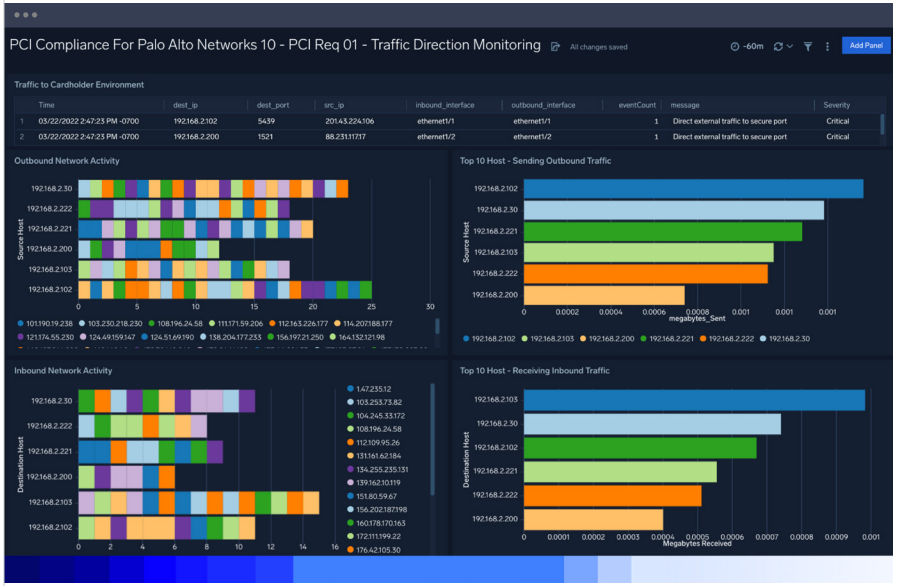
Years of rapid growth presented SoSafe with the challenge to manage, monitor and improve its applications and systems. They generated volumes of data at a rate that made it difficult to monitor across multiple tools efficiently.

Ultimately, SoSafe needed a single source of truth across different functions to make data available for efficient auditing and ongoing regulatory compliance. With Sumo Logic, SoSafe is equipped with efficient data intake and analysis capabilities that provide the company with meaningful insights to continue to drive its phenomenal business growth. The platform provides a single solution that supports all of SoSafe's many tools and use cases — from optimizing software security and delivery to monitoring the security of the environment and ensuring adherence to GDPR requirements.

In their own words, they needed a cloud-native platform "that could unify and support our observability, intelligence, and security needs. Immediately after our purchase, we were able to send data to Sumo Logic and increase our visibility to 100 percent."

sosafe

With the Sumo Logic implementation, SoSafe was able to shorten its audit cycles and power its compliance initiatives.



Out-of-the-box integration apps include pre-built searches and granular dashboards to demonstrate continuous PCI compliance across cloud and on-premises environments, thereby reducing manual effort spent for time-intensive security audits.

Sumo Logic empowered SoSafe to:

- Unlock 100 percent visibility immediately following deployment.
- Reduce tool sprawl with a unified platform for observability, security and compliance.
- Enable rapid security insights with out-of-the-box security content.
- Experience fast return on investment with an easy ramp-up, short learning curve and built-in scalability.

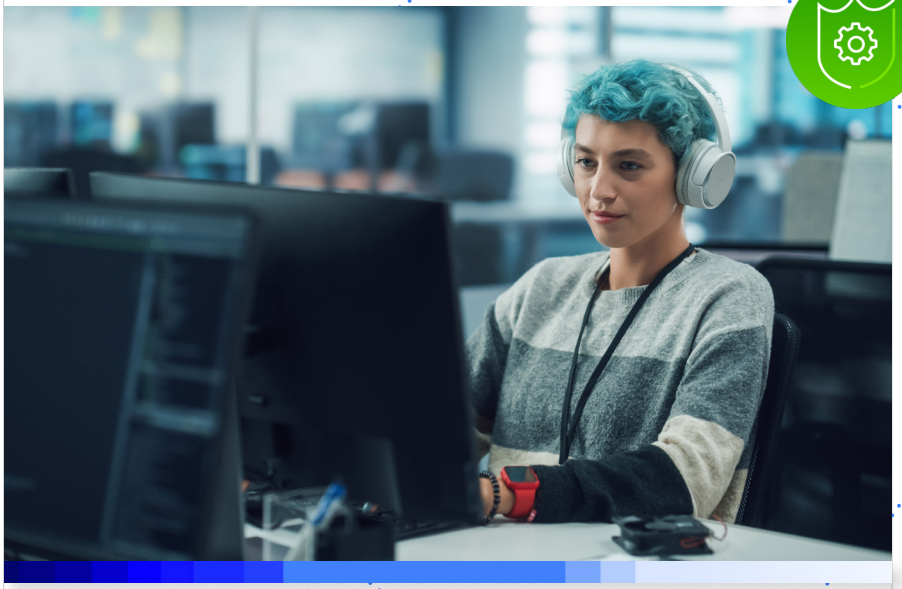
To learn more about how SoSafe uses Sumo Logic to enable a more effective compliance program find the details here.

Ready to dive in?

Your step-by-step guide to shorten audit cycles and ensure compliance

A platform like Sumo Logic streamlines audit cycles and strengthens regulatory compliance. With Sumo Logic, you're partnering with a company that invests millions yearly to maintain attestations, such as SOC2 Type II, HIPAA, PCI Service Level 1 Provider, and a FedRAMP moderate authorized offering.

Many regulatory agencies require organizations to collect and monitor access events (logins) for potentially anomalous behavior. By collecting and organizing data in a centralized and accessible security data lake, it becomes much easier to review and report on.



On the following page is a list of how companies can save time, demonstrate compliance and avoid risk with Sumo Logic Cloud Security Analytics.

1 Centralize data collection

Capture and collect a wide range of organizational data from wherever it originates, empowering organizations to monitor and learn from it.

2 Increase visibility

Make various types of data available with 100% visibility and visualize it in compelling, configurable dashboards for real-time monitoring and insights.

3 Find insights fast

Use our query language to create filters and search parameters, to find any data at any time — whether it relates to regulatory compliance or internal security controls.

4 Use out-of-the-box content

Leverage machine learning analytics to improve and streamline audit processes and expedite compliance using tools like our PCI Dashboard. Out-of-the-box integrations mean our platform can monitor many security tools you already use.

5 Retain data

Solutions must retain data for longer periods, at a cost-effective price. But not just any “storage” will do — a security analytics solution must itself be highly invested in security and compliance. This commitment separates the most reliable solutions from the rest of the pack.

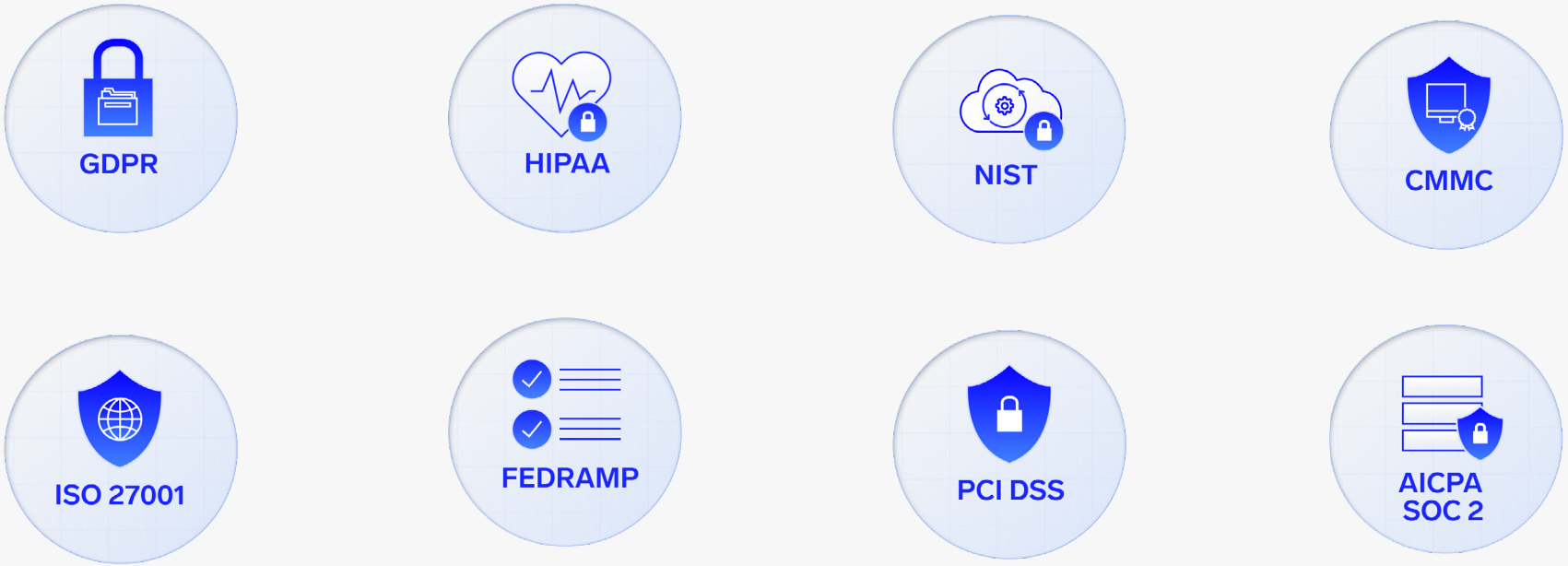
6 Monitor in real-time

Sumo Logic monitors incoming data and security controls to identify anomalies that could signal a vulnerability, threat or non-compliance.

7 Create a unified system

Countless data integrations and out-of-the-box applications ensure that all data is properly collected and cataloged as it’s generated.

When it's time for an audit, the Sumo Logic platform increases understanding, streamlines the auditing process, and ensures ongoing compliance with various security regulations and frameworks.



A multi-use solution for audit and compliance

As organizations grow and mature, keeping log data available in an easily accessible centralized location is an absolute necessity. As new regulations emerge and evolve, and auditing demands rise, the importance of a reliable and comprehensive solution for data storage, visibility and accessibility only increases. Especially for companies with complex or changing needs, identifying a software solution that's trustworthy and up for identifying a software solution that's trustworthy and up for the task is vital..

Sumo Logic Cloud Security Analytics provides a streamlined solution for audit and compliance. With hundreds of custom integrations, compliance-related data comes to life through pre-built searches, visual dashboards and more. These features enable organizations to move quickly in the face of changing regulations or impending audits.

In addition to audit and compliance discussed here, Sumo Logic covers other critical use cases that include:

- **Security data lake —** To store and manage information
- **Threat detection and investigation —** To identify problems quickly
- **Application security —** To embed security throughout the application lifecycle

When you are ready to take audit and compliance to the next level contact us or start your free 30 day trial.

Sumo Logic.
The infinite power of log analytics.