



# Conquer Your Compliance Monitoring Challenge

## Compliance is Complex and Costly

Security compliance is a legal concern for many organizations across industries. Regulatory bodies levy heavy fines on non-conforming organizations. Even worse, organizations that do not stay in compliance receive negative headlines and IT leaders can even be held personally responsible.

Compliance frameworks, such as HIPAA or FedRAMP, require specific data security practices, policies, and procedures to be followed. These mandates continue to be refined and expanded, placing an increasingly larger burden on companies to adhere to these regulatory frameworks.

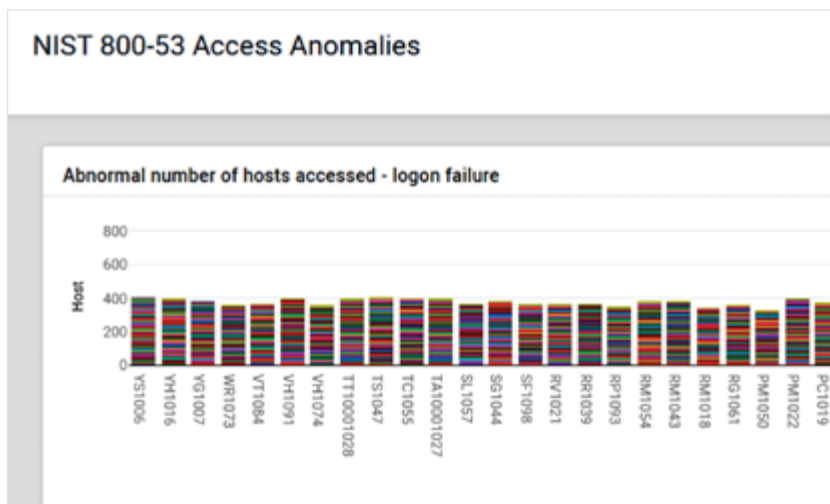
## Simplify Compliance with Securonix

Securonix can help alleviate the complexity and cost of compliance with Securonix Next-Gen SIEM. We provide out-of-the-box compliance content for all major compliance frameworks including: NIST 800-53, GDPR, HIPAA, ISO, PCI DSS, SOX, CCPA, CMMC, and many more. Security compliance teams simply select which compliance framework(s) they need in order to enable compliance monitoring. Once enabled, Securonix compliance capabilities are available in easily configurable dashboards, allowing the team to quickly begin monitoring for compliance violations.

For organizations with a dedicated compliance team, the security team can improve security by allowing limited access to only the data sets necessary for compliance enforcement using granular role-based access.

## Securonix Compliance Dashboards

Securonix compliance dashboards help you focus on critical data for compliance frameworks. Each dashboard is easily modified within the user interface to suit the needs of your unique organization.



## Solution Benefits

- Simplify your compliance adherence using pre-built compliance frameworks that include policies, dashboards, and reporting.
- Save time when investigating compliance-based alerts by using enriched data, which provides additional context and removes the need for “swivel-chair” analysis across multiple tools to solve compliance issues.
- Faster, more accurate search using Securonix Long-Term Search to investigate across older, historical data.

## Securonix Compliance Policy Tags

Implementing policies that monitor compliance frameworks is easy. Simply select the framework monitoring package you need and choose which policies to implement.

|     | Name ID   | Type             | Analytical Type | DataSource | Database Type | Functionality     | Last Update Date      | Violation Entity | Enabled?                            | Actions |
|-----|---|------------------|-----------------|------------|---------------|-------------------|-----------------------|------------------|-------------------------------------|---------|
| Low | HIPAA - User Account Deleted - 164.308(a)(3)-i(C) | Real Time Policy | -               |            |               | Compliance        | 2020-07-29 18:07:32.0 | Activity Account | <input checked="" type="checkbox"/> |         |
| Low | Password Safeguard - 164.308(a)(5)-i(D)           | Real Time Policy | -               |            |               | Microsoft Windows | 2020-07-29 18:07:42.0 | Activity Account | <input type="checkbox"/>            |         |

If you'd prefer to tune policies before implementation, the Securonix Sandbox feature allows you to tune policies on production data without bombarding your analysts with false positives.

## Securonix Compliance Reports

No compliance framework would be complete without robust reporting. Securonix provides compliance reports that are easily shared and distributed for proof of compliance. Reports can be scheduled or edited through the Securonix user interface.

| Report Name   | Actions |
|---|---------|
| HIPAA - Account Sharing Summary<br>164.312(a)(2)(i)   |         |
| HIPAA - All Application Events<br>164.308(a)(5)(i)(C) |         |
| HIPAA - All Database Logins<br>164.308(a)(5)(i)(C)    |         |
| HIPAA - All Network Device<br>164.308(a)(5)(i)(C)     |         |
| HIPAA - All OS Logins<br>164.308(a)(5)(i)(C)          |         |
| HIPAA - All Security Device<br>164.308(a)(5)(i)(C)    |         |
| HIPAA - All VPN Logins<br>164.308(a)(5)(i)(C)         |         |
| HIPAA - Anti-Malware Deployed<br>164.308(a)(5)(i)(B)  |         |

## Securonix Compliance and Long-Term Search

One frequently overlooked requirement for compliance monitoring and investigations is the ability to search on data sets over a long period of time without paying a huge fee or buying more storage from a vendor. Compliance teams need access to all of their data quickly and efficiently – something very few security vendors can offer without a large cost involved. Securonix Long-Term Search provides historic search on months' worth of older data, making Securonix Next-Gen SIEM a strong partner for compliance.

## Compliance Frameworks Include

- National Institute of Standards and Technology (NIST) 800-53
- General Data Protection Regulation (GDPR)
- Health Insurance Portability and Accountability Act (HIPAA)
- International Organization for Standardization (ISO)
- Payment Card Industry Data Security Standard (PCI DSS)
- Sarbanes-Oxley Act (SOX)
- California Consumer Privacy Act (CCPA)
- Cybersecurity Maturity Model Certification (CMMC)

## About Securonix

Securonix transforms enterprise security with actionable intelligence. Using a purpose-built security analytics platform Securonix quickly and accurately detects high-risk threats to your organization. For more information visit [www.securonix.com](http://www.securonix.com).