

securonix

SOLUTION BRIEF

# Conquer Your Compliance Monitoring Challenge

## Compliance is Complex and Expensive

Security compliance is a legal concern for many organizations. 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, NERC, FISMA, HITRUST, and many more. Security compliance teams simply select which compliance framework(s) they need 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 Benefits

### Reduce the Complexity of Compliance

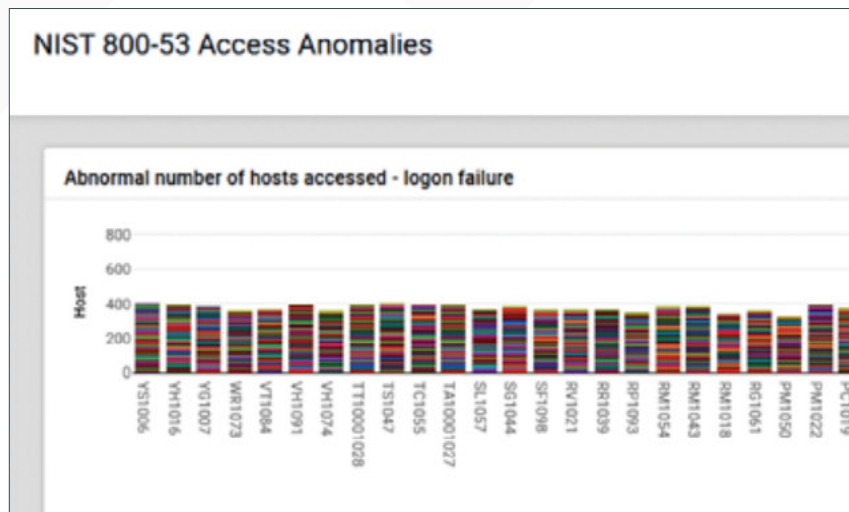
Simplify your compliance adherence using pre-built compliance frameworks that include policies, dashboards, and reporting.

### Monitor for Compliance Violations

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.

### Search Through Historic Data Quickly

Faster, more accurate search using Securonix Long-Term Search to investigate across older, historical data.



NIST 800-53 Access Anomalies

## How Securonix Helps With Compliance

### 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.

### 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. 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 164.312(a)(2)(i)	  
HIPAA - All Application Events 164.308(a)(5)(i)(C)	  
HIPAA - All Database Logins 164.308(a)(5)(i)(C)	  
HIPAA - All Network Device 164.308(a)(5)(i)(C)	  
HIPAA - All OS Logins 164.308(a)(5)(i)(C)	  
HIPAA - All Security Device 164.308(a)(5)(i)(C)	  
HIPAA - All VPN Logins 164.308(a)(5)(i)(C)	  
HIPAA - Anti-Malware Deployed 164.308(a)(5)(i)(B)	  

Securonix Compliance Reports

## 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

Compliance Frameworks Included:

- International Organization for Standardization (ISO) 27001
- Sarbanes-Oxley Axt (SOX)
- North American Electric Reliability Corporation (NERC)
- National Institute of Standards and technology (NIST) 800-53
- Federal Information Security Modernization Act (FISMA)
- Health Insurance Portability and Accountability Act (HIPAA)
- SOC Reports Daily
- SOC-Operations Report
- Health Information Trust Alliance (HITRUST)
- General Data Protection Regulation (GDPR)

For more information about Securonix, schedule a demo at [www.securonix.com/request-a-demo](http://www.securonix.com/request-a-demo).

## About Securonix

Securonix is redefining SIEM for today's hybrid cloud, data-driven enterprise. Built on big data architecture, Securonix delivers SIEM, UEBA, XDR, SOAR, Security Data Lake, NDR and vertical-specific applications as a pure SaaS solution with unlimited scalability and no infrastructure cost. Securonix reduces noise and prioritizes high fidelity alerts with behavioral analytics technology that pioneered the UEBA category. For more information visit [securonix.com](http://securonix.com)

For more information about Securonix solutions for the federal market, contact [fedsalesteam@securonix.com](mailto:fedsalesteam@securonix.com)