Achieving NYDFS 23 NYCRR 500 API Security Compliance with Salt Security

The New York Department of Financial Services (NYDFS) Cybersecurity Regulation (23 NYCRR 500) mandates comprehensive cybersecurity programs for financial institutions, with a key focus on API security. Salt Security aids NYDFS-regulated institutions in complying with 23 NYCRR 500 by offering solutions for API discovery, threat detection, access control monitoring, and posture governance. This guide outlines NYDFS API security requirements and highlights how Salt Security can help meet and exceed these expectations.

Key Requirements and How Salt Security Helps:

Asset & Data Inventory (23 NYCRR 500.02, 500.03)

- Have you inventoried all internal and external APIs?
- Do you know which APIs transmit or store NPI (nonpublic information)?
- Can you map sensitive data flows across services and third parties?
- **Salt Delivers:** Panoramic, continuous API discovery - including shadow, zombie, and undocumented APIs - with sensitive data classification.

Risk Assessment & Governance (23 NYCRR 500.09, 500.03(e))

- Are APIs evaluated in your formal cybersecurity risk assessments?
- Is API posture (auth, data exposure, access controls) continuously reviewed?
- **Salt Delivers:** Automated API risk assessments based on authentication gaps, sensitive data exposure, and policy violations.

Access Controls & Identity Management (23 NYCRR 500.07)

- Do your APIs enforce least-privilege access?
- Are access tokens, keys, and credentials secured and rotated?
- Can you detect privilege escalation attempts via API misuse?
- **Salt Delivers:** Continuous monitoring for auth flaws, excessive access, and broken object-level authorization (BOLA).

Threat Detection & Anomaly Monitoring (23 NYCRR 500.02(b), 500.03(g))

- Can you detect behavioral anomalies like API scraping, brute force, or token reuse?
- Are API abuse patterns baseline-aware and context-driven?
- APIs must be monitored for anomalies.
- Continuously monitor third-party exposed APIs (as per 500.11).
- **Salt Delivers:** AI-driven behavioral analysis to detect and alert on malicious API activity, including zero-day threats.

Incident Response & Reporting (23 NYCRR 500.16, 500.17)

- Can you detect and respond to an API-based breach within 72 hours?
- Do you maintain incident logs for API abuse attempts?
- **Salt Delivers:** Automated forensic timelines, incident drill-down, and integrations with SIEM/SOAR tools for rapid reporting.

Auditability & Logging (23 NYCRR 500.06)

- Are all API calls logged and retained securely?
- Can you trace sensitive data access by user and API method?
- **Salt Delivers:** Granular API call logging with metadata - ideal for compliance audits, IR reviews, and reporting.

Secure Development Lifecycle (SDLC) (23 NYCRR 500.03(c), 500.03(h))

- Are APIs scanned for misconfigurations before and after deployment?
- Is API security embedded in your SDLC or CI/CD pipeline?
- **Salt Delivers:** Shift-left posture analysis integrated with developer workflows and CI/CD pipelines to fix risks early.

Why NYDFS Compliance Matters:

NYDFS compliance is crucial for financial institutions operating in New York State, ensuring the stability and security of the financial sector. Compliance protects customer data from cyber threats and maintains the integrity of the financial system.

Summary of Salt Security's Role in Achieving Compliance:

Salt Security enables entities regulated by NYDFS to fulfill and surpass API security requirements outlined in 23 NYCRR 500, focusing on visibility, governance, monitoring, and incident response. The company offers API discovery, posture governance, monitoring and threat detection to assist organizations in achieving compliance.

By effectively addressing these critical areas with comprehensive solutions like those from Salt Security, financial institutions can enhance their API security posture in accordance with NYDFS 23 NYCRR 500, safeguarding essential assets and sensitive information.

Take Control of Your API Security:

Discover your externally exposed APIs and identify vulnerabilities with our **Free API Surface Scan**. Rapidly gather API inventory and enhance visibility across your cloud environments with **Salt Cloud Connect**. Contact us to learn more!