EventTracker
Actionable Security Intelligence

New York Cybersecurity Requirements for Financial Services Companies (23NYCRR 500) Solution Brief

New York Cybersecurity

EventTracker | 8815 Centre Park Drive, Columbia MD 21045

About EventTracker

EventTracker's advanced security solutions protect enterprises and small businesses from data breaches and insider fraud, and streamline regulatory compliance. EventTracker's platform comprises SIEM, vulnerability scanning, intrusion detection, behavior analytics, a HoneyNet deception network and other defense-in-depth capabilities within a single management platform. The company complements its state-of-the-art technology with 24/7 managed services from its global security operations center (SOC) to ensure its customers achieve desired outcomes—safer networks, better endpoint security, earlier detection of intrusion, and relevant and specific threat intelligence.

23 NYCRR 500 Compliance

After a period of comments, the New York Department of Financial Services (DFS) announced 23 NYCRR 500 has become effective March 1, 2017. Also known as "Cybersecurity Requirements for Financial Services Companies," these regulations were developed out of concern that financial firms are facing increased cyber threats today. 23 NYCRR 500 is intended to establish "regulatory minimum standards" to foster the creation of effective cybersecurity programs in the financial sector.

The goal is to protect customer information by securing the IT assets of regulated entities. Each financial firm must assess its risk profile and design a program that mitigates the most serious risks. 23 NYCRR 500 stays away from prescriptive advice. It's not a cookbook. Rather, it provides guidelines for senior management.

The new rules affect virtually every aspect of IT security at financial firms. 23 NYCRR 500 covers the creation (or updating) of a firm's cybersecurity program; offers guidance on establishing cybersecurity policy and clarifies the role of the CISO. Sub-sections of the rules discuss steps financial firms should take regarding penetration testing and vulnerability assessments, audit trails, access privileges, application security and much more.

At the root of all this is IT security mindfulness and the recognition that IT Security is a process, not a project. After all, projects begin and end, whereas security mindfulness is eternal. The requirements can be grouped into two general stages: Setup and Implement a Security Program that includes an Owner (CISO), and practice it on a daily basis.

The core of the regulation requires that firms base IT security decisions on sound risk management practices. This means documenting policies and procedures for incident handling and response, monitoring audit trails and training employees. It's a lot for even mid-sized organizations to satisfy, even in sprit, much less practice.

EventTracker's Co-Sourced Solution Simplifies Compliance

Recognizing that many firms may not have the necessary skills in house, the regulation allows for many of these functions to be co-sourced to specialist firms. Co-sourcing is based on a long term relationship and emphasizes values traditionally associated with partnering rather than with vending.

The SIEMphonic service offering from EventTracker is especially tailored to help organizations that must meet this degree of maturity. In particular, these aspects of the regulation are satisfied by EventTracker's SIEMphonic offering.

Statement of Compliance – 23 NYCRR 500

Section 500.02 Cybersecurity Program

Must be established, maintained and designed to ensure Confidentiality, Integrity and Availability of your systems.

23 NYCRR 500 Requirement	EventTracker Capability
IDENTIFY: Internal & external cyber risks, and nonpublic information in your network who and how it is accessed	
Asset Management The data, personnel, devices, systems and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	EventTracker provides support by collecting and analyzing all account management, access granting/revoking, and access/authentication logs. EventTracker correlation rules provide alerting on account authentication failures. EventTracker investigations, reports and tails provide evidence of system account management activity (account creation, deletion, and modification), access granting/revoking activity, and account access/authentication activity. Lastly, EventTracker investigations provide evidence of authorized/unauthorized network access.
Governance The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental and operational requirements are understood and inform the management of cybersecurity risk.	EventTracker provides support for this requirement by collecting and analyzing all account management and access/authentication logs. EventTracker correlation rules provide alerting on account authentication failures. EventTracker investigations, reports and tails provide evidence of account management activity (account creation, deletion, and modification) and account access/authentication activity to support efforts of enforcing security policies within the organization.
Risk Assessment The organization understands the cybersecurity risk to organizational operations (including mission, functions, image or reputation), organizational assets and individuals.	EventTracker provides support for this requirement by collecting and analyzing all suspicious network activity or activities indicative of cybersecurity risks. EventTracker correlation rules provide alerting on events indicative of potential cybersecurity threats or attacks on the network. EventTracker investigations, reports and tails provide evidence of cybersecurity events in support of early detection and incident response.

23 NYCRR 500 Requirement	EventTracker Capability
PROTECT: Use 3 lines of defense with policy and procedure implementation to protect systems and the nonpublic information from unauthorized access	
Access Controls Access to assets and associated facilities is limited to authorized users, processes or devices, and to authorized activities and transactions.	EventTracker supports this requirement by collecting and analyzing all account management, network access/ authentication logs, remote and physical access. EventTracker correlation rules provide alerting on account authentication failures. EventTracker investigations, reports and tails provide evidence of account access/authentication activity
Awareness and Training The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures and agreements.	EventTracker supports this requirement by collecting and analyzing all third-party accounts or process activities within the environment to ensure third-parties are performing activities according to defined roles and responsibilities. EventTracker correlation rules provide alerting on account authentication failures. EventTracker investigations, reports and tails provide evidence of vendor account management and authentication (success/failures) activities.
Data Security Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information	EventTracker supports this requirement by collecting and analyzing all system logs relating to the protection of data integrity, availability and mobility. EventTracker' s Change Audit tracks file changes and logs the connection and disconnection of external data devices to the host computer where the Agent is running. EventTracker also monitors and logs the transmission of files to an external storage device. EventTracker can be configured to protect against external data device connections by ejecting specified devices upon detection. External USB drive storage devices include Flash/RAM drives and CD/DVD drives. EventTracker correlation rules provide alerting on remote account authentication failures. EventTracker investigations, reports and tails provide evidence of remote account access/authentication activity.
Information Protection Processes and Procedures Security policies (that address purpose, scope, roles, responsibilities, management commitment and coordination among organizational entities), processes and procedures are maintained and used to manage protection of information systems and assets.	EventTracker provides support by collecting and analyzing all logs relating to change management, backups, and those in support of incident response plans. EventTracker correlation rules provide alerting on account management activities. EventTracker investigations, reports and tails provide evidence of account management and authentication (success/failures) activities.
Maintenance Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	EventTracker provides support by collecting and analyzing all logs relating to critical and error conditions within the environment. EventTracker correlation rules provide alerting on critical and error conditions within the environment. EventTracker investigations, reports and tails provide evidence of environment conditions as well as process and system start-ups/shut-downs.
Protective Technology Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures and agreements.	EventTracker provides support by collecting logs relating to technical security solution access management and authentication activities. Further, with the use of EventTracker allows for monitoring of removable media and other audit logging events. EventTracker correlation rules provide alerting on audit logging events (log cleared, stopped). Lastly, EventTracker investigations, reports and tails provide evidence around the aforementioned activities.

23 NYCRR 500 Requirement	EventTracker Capability
RECOVER: Recover from cybersecurity events and restore normal operations and services	
Improvements Recovery planning and processes are improved by incorporating lessons learned into future activities.	EventTracker provides support by collecting and analyzing logs relating to recovery operations. EventTracker reports provide evidence around the recovery operation events
Communications Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims and vendors	EventTracker provides support by collecting and analyzing logs relating to recovery operations. EventTracker reports provide evidence around the recovery operation events.

Section 500.05 Penetration Testing and Vulnerability Assessments

The Cybersecurity Program shall minimally include:

- Penetration Testing performed at least annually Vulnerability Assessment performed at least quarterly

23 NYCRR 500 Requirement	EventTracker Capability
Regarding Penetration Testing 1. Targets systems and users to identify weaknesses in business processes and technical controls. 2. Mimics a threat source's search for and exploitation of vulnerabilities to demonstrate a potential for loss. 3. Management determines the level and types of tests employed to ensure effective and comprehensive coverage. 4. The frequency and scope of a penetration test should be a function of the level of assurance needed by the Firm and determined by the risk assessment process. 5. Test can be performed internally by independent groups, internally by the organizational unit, or by an independent third party. 6. Management should determine the level of independence required of the test. **Regarding Vulnerability Assessments** 1. Process that defines, identifies, and classifies the vulnerabilities in your computer network. 2. Similar to penetration testing, the frequency of the performance of vulnerability assessments should be determined by the risk management process. 3. Scanners/tools can be run continuously or periodically, generating metrics that are reported and acted upon. 4. Can be performed internally or by external testers, but they are often run as part of internal testing processes	EventTracker's ETVAS Vulnerability Scanning helps an organization identify and remediate vulnerabilities within their IT environment before hackers and thieves gain access to, modify or destroy confidential information. ETVAS Vulnerability Scanning services help our clients manage their vulnerabilities more rapidly and cost effectively. All vulnerabilities that are identified are presented to the client together with an assessment of impact and recommendations for mitigation or a technical solution. Vulnerability scans can be a one-time event or can be scheduled at an agreed-upon cycle (i.e., weekly, monthly, quarterly, bi-yearly, etc.).

Section 500.06 Audit Trail

The cybersecurity program for each Firm shall, at a minimum, include implementing and maintaining audit trail systems that:

23 NYCRR 500 Requirement	EventTracker Capability
1. Track and maintain data that allows for the complete and accurate reconstruction of all financial transactions and accounting necessary to enable the Firm to detect and respond to a Cybersecurity Event; 2. Track and maintain data logging of all privileged Authorized User access to critical systems; 3. Protect the integrity of data stored and maintained as part of any audit trail from alteration or tampering; 4. Protect the integrity of hardware from alteration or tampering, including by limiting electronic and 5. Physical access permissions to hardware and maintaining logs of physical access to hardware that allows for event reconstruction; 6. Log system events including, at a minimum, access and alterations made to the audit trail systems by the systems or by an Authorized User, and all system administrator functions performed on the systems; Maintain records produced as part of the audit trail for not fewer than 6 years.	EventTracker makes it easy for you to comply with regulatory requirements for log data collection, review, archival, reporting and alerting, as well as file integrity monitoring. EventTracker also helps users realize efficiencies and new capabilities in the audit process. Some of the many capabilities of the EventTracker solution that provide substantial assistance to compliance and audit challenges include: 1. Collecting and archiving cross-platform log data in real time 2. Compressing logs for efficient long-term storage 3. Simplifying search and retrieval of specific logs for analysis and forensic investigation 4. Automatically identifying important audit events and alerts appropriate individuals 5. Providing an easier and more affordable way to automate log & event management and file integrity monitoring for compliance EventTracker protects its customers' networks from insider threats and helps them meet specific requirements by allowing them to keep track of what their privileged users are doing. This includes business users with direct access to confidential data systems, as well as administrators with the ability to create and modify permissions, privileges and access to any device. Privileged User Monitoring provides enormous value by delivering automated monitoring and secure and reliable access to what privileged users are doing when, and how they are doing it. With EventTracker you can immediately address and automate specific log data collection, review, archiving, reporting and alerting requirements as well as those requirements mandating File Integrity Monitoring.

Section 500.07 Access Privileges

The cybersecurity program for each Firm shall limit access privileges to Information Systems that provide access to Nonpublic Information solely to those individuals who require such access to such systems in order to perform their responsibilities and shall periodically review such access privileges.

23 NYCRR 500 Requirement	EventTracker Capability
1. Track and maintain data that Management should develop a user access program to implement and administer physical and logical access controls to safeguard the Firm's information assets and technology. This program should include the following elements: 2. Principle of least privilege, which recommends minimum user profile privileges for both physical and logical access based on job necessity. 3. Alignment of employee job descriptions to the user access program. 4. Requirements for business and application owners to define user profiles. 5. Ongoing reviews by business line and application owners to verify appropriate access based on job roles with changes reported on a timely basis to security administration personnel. 6. Timely notification from human resources to security administrators to adjust user access based on job changes, including terminations. 7. Periodic independent reviews that ensure effective administration of user access, both physical and logical	EventTracker' s real-time, automated, centralized and secure collection of log data provides independent access to privileged user activity logs without relying on the privileged user for collection. EventTracker monitors privileged-user activity to reduce the risk of insider attacks. Provides a detailed audit trail of privileged-user activity across Microsoft Windows and Active Directory, UNIX and Linux environments. Delivers real-time alerting on suspicious behavior to provide immediate visibility to changes that could lead to a breach.

Section 500.09 Risk Assessment

At least annually, each Firm shall conduct a risk assessment of the Firm's Information Systems. Such risk assessment shall be carried out in accordance with written policies and procedures and shall be documented in writing.

As part of such policies and procedures, each Firm shall include, at a minimum:

23 NYCRR 500 Requirement	EventTracker Capability
1. Criteria for the evaluation and categorization of identified risks; 2. Criteria for the assessment of the Confidentiality, Integrity and Availability of the Firm's Information Systems, including the adequacy of existing controls in the context of identified risks; and 3. Requirements for documentation describing how identified risks will be mitigated or accepted based on the risk assessment, justifying such decisions in light of the risk assessment findings, and assigning accountability for the identified risks	EventTracker supports this requirement by collecting and analyzing all suspicious network activity or activities indicative of cybersecurity risks. EventTracker correlation rules provide alerting on events indicative of potential cybersecurity threats or attacks on the network. EventTracker investigations, reports and tails provide evidence of cybersecurity events in support of early detection and incident response.

Section 500.10 Cyber Security Personnel and Intelligence

In addition to the requirements set forth in 500.04(a), each Firm shall:

23 NYCRR 500 Requirement	EventTracker Capability
1. Employ cybersecurity personnel sufficient to manage the Firm's cybersecurity risks and to perform the core cybersecurity functions specified in section 500.02(b)(1)-(5); 2. Provide for and require all cybersecurity personnel to attend regular cybersecurity update and training sessions; and 3. Require key cybersecurity personnel to take steps to stay abreast of changing cybersecurity threats and countermeasures. 4. A Firm may choose to utilize a qualified third party to assist in complying with the requirements set forth in this Part, subject to the requirements set forth in section 500.11.	SIEMphonic provides qualified cybersecurity personnel of the Covered Entity to perform services. Our staff are provided updates and training to maintain current knowledge. The regulation specifically encourages the use of qualified Third Parties to meet this requirement.

Section 500.11 Third Party Security Policy

Each Firm shall implement written policies and procedures (Vendor Management Policy and Procedures) designed to ensure the security of Information Systems and Nonpublic Information that are accessible to, or held by, third parties doing business with the Firm. Such policies and procedures shall address, at a minimum, the following areas:

23 NYCRR 500 Requirement	EventTracker Capability
1. The identification and risk assessment of third parties with access to systems or Nonpublic Information; 2. Minimum cybersecurity practices required by third parties for them to do business with the Firm; 3. Due diligence processes to evaluate the adequacy of cybersecurity practices of third parties; and 4. Periodic assessment (i.e. annually) of third parties and continued adequacy of their cybersecurity practices.	SIEMphonic maintains detailed written policies based on a Risk Assessment.

Section 500.13 Limitations on Data Retention

23 NYCRR 500 Requirement	EventTracker Capability
As part of its cybersecurity program, each Firm shall include policies and procedures (Data Retention and Destruction Policy) for the timely destruction of any Nonpublic Information identified in 500.01(g) (2)-(4) that is no longer necessary for the provision of the products or services for which such information was provided to the Firm, except where such information is otherwise required to be retained by law or regulation.	The EventTracker software solution supports auto purging of data past retention settings. This, in addition to the analyst's active involvement, assures that data is securely disposed when it outlives its need.

Section 500.14 Training and Monitoring

23 NYCRR 500 Requirement	EventTracker Capability
1. Implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users; and 2. Provide for and require all personnel to attend regular cybersecurity awareness training sessions that are updated to reflect risks identified by the Firm in its annual assessment of risks.	EventTracker provides support by collecting and analyzing all account management, access granting/revoking, and access/authentication logs. EventTracker correlation rules provide alerting on account authentication failures. EventTracker investigations, reports and tails provide evidence of system account management activity (account creation, deletion and modification), access granting/revoking activity, and account access/authentication activity. Lastly, EventTracker investigations provide evidence of authorized/unauthorized network access.