Solution Brief

23 NYCRR 500

Simplifying compliance with STEALTHbits

The New York Department of Financial Services (DFS) announced 23 NYCRR 500 became effective on March 1, 2017. Also known as “Cybersecurity Requirements for Financial Services Companies,” these regulations were developed to address the ever-growing threat posed to information and financial systems by nation-states, terrorist organizations and independent criminal actors. 23 NYCRR 500 is intended to establish “regulatory minimum standards” while not being overly prescriptive so that organizations can implement cybersecurity programs that align to their own risk tolerance, budget and need to maintain business agility.

With privacy being a significant driver of the new regulation, the protection of customer information is the underlining goal. To achieve this, organizations are required to secure the IT assets of regulated entities (give examples…). Each financial firm must assess its risk profile and design a program that mitigates the most serious risks. 23 NYCRR 500 also covers the creation or updating of a firm’s cybersecurity program by offering guidance on establishing cybersecurity policy and clarifying the role of the CISO. These measures ensure the safety and soundness of the institution and protect its customers.

STEALTHbits Solution Simplifies Compliance

The STEALTHbits open architecture, small footprint, and powerful collection and protection capabilities ensure that our solutions are flexible enough to provide a solid foundation for 23 NYCRR 500 compliance and passing audits. STEALTHbits NYCRR 500 solutions go beyond the requirements and provide comprehensive best practices for securing sensitive information. STEALTHbits solutions can strengthen a company’s overall security posture and help satisfy requirements efficiently and cost-effectively. The chart below summarizes the capabilities within STEALTHbits and the requirements they map to in order to help you understand how the solution helps you achieve compliance.

<table>
<tr><th colspan="2"><b>IDENTIFY:</b> Internal & external cyber risks, and nonpublic information in your network who and how it is accessed</th></tr>
<tr><th>23 NYCRR500 Requirement</th><th>STEALTHbits Capability</th></tr>
<tr><td><b>Asset Management</b>
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.</td><td><b>System-level Entitlements</b> - Identify who has system-level access (i.e. Local Admin) through local users and groups or domain group memberships. Local Admins are power users that can install software, manipulate system settings, and more. If compromised, attackers can load reconnaissance tools and steal password hashes.
<b>Local Admin Entitlement Reviews</b> - Manage local group membership through Group Membership Reviews, allowing resource owners to review the membership of Local Administrator groups and remove or grant access.
<b>Service Accounts</b> - Identify accounts being used to run services to aid in privileged account management efforts.
<b>Software Application License Usage</b> - Identify all installed applications and their usage for license reclamation and reallocation.
<b>Patch Validation</b> - Determine compliance with patch and anti-virus updates to identify and remediate security vulnerabilities.</td></tr>
</table>

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.	**Entitlement Reviews** - Assign owners to sites in order to allow them to perform periodic reviews of access and make access modifications to ensure the right people have the right access to their data. **Direct Permission Reports** - Identify where direct permissions are applied which may be indicative of high-risk or otherwise toxic conditions (e.g. High Risk Permissions, Empty Group Permissions, Local User & Groups, Stale User Permissions, Domain User Permissions, Unused Security Groups, Unresolved SIDs). **Effective Access Reporting** - Understand effective access to Sites, Lists, and Libraries, as well as determine where any user or group has access. **Active Directory Inventory** - Creates a catalogue of user, group, and computer object information, including object attributes and direct group membership across the entire AD environment.
Risk Assessment The organization understands the cybersecurity risk to organizational operations (including mission, functions, image or reputation), organizational assets and individuals.	**Toxic Conditions Assessment** - Identifies where "toxic" group/user conditions exist such as Circular Nesting, Empty, Stale, Large, or Similar groups **Sensitive Security Group Membership** - Keep track of the members of specified Active Directory Sensitive Security Groups **Effective Group Membership** - Enumerates group membership to report on all user objects with effective membership through both direct and nested sources. **Password Status** - Identify the password status of all users to highlight potential issues and security vulnerabilities. **Active Directory Clean-up** - Programmatically or automatically clean-up stale AD objects through embedded and customizable workflows. Actions include creating and deleting users, modification of user, group, and computer attributes, enabling and disabling users, moving objects, clearing or setting SID History, and more.

PROTECT: Use 3 lines of defense with policy and procedure implementation to protect systems and the nonpublic information from unauthorized access	
23 NYCRR500 Requirement	STEALTHbits Capability
Access Controls Access to assets and associated facilities is limited to authorized users, processes or devices, and to authorized activities and transactions.	**AD Object/Attribute Change Auditing/Blocking** - Monitor and record any or all changes to objects and attributes, by whom, from where, along with before and after values. Additionally, block any particular changes from occurring regardless of natively supplied access rights. **Nested Group Membership Change Detection** - Automatically resolve group membership changes of nested groups to parent groups in real-time. **Group Policy Object (GPO) Change Auditing/**Blocking - Detect or optionally prevent changes to Group Policy Objects such as the Default Domain Policy or Default Domain Controllers Policy. **Authentication Monitoring/**Blocking - Detect and/or block all or specific authentication traffic within Active Directory, including who and what, when, from where, and the security protocols being leveraged (e.g. Kerberos vs. NTLM) **Privileged Account Usage & Abuse** - Monitor, record, block, or alert upon changes and authentication activities made by or to Privileged Accounts such as Domain Admins, BUILTIN Administrators, or other organization-specific Privileged Accounts. **User Lockout Monitoring** - Highlight the source of user lockout events. Additionally, correlate lockout events with recent password change activities to further expedite issue resolution.
Data Security Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information	**Sensitive Data Discovery** - Identify files (including images using OCR) containing sensitive content such as Credit Card and Social Security numbers, personal health information, and dozens of other types of Personally Identifiable Information (PII). Also search for custom criteria specific to an organization such as Employee ID numbers, trade secrets, product formulas, and more. **Data Classification (File Tag Collection)** - Collect file metadata including classification tags that have been implemented via internal processes or third party solutions. **Sensitive Data Reviews** - Enable data custodians to review the sensitive data found within their shared folders and SharePoint sites. This review type allows owners to mark "hits" as false-positives and inspect the files that have sensitive information in them to decide which files require remediation. **File Activity Monitoring & Reporting** - Understand File System activities such as reads, modifications, creations, deletions, and permission changes.

Protective Technology Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures and agreements.	**Authentication-based Attack** Detection - Detect advanced threats and suspicious activity patterns indicative of Brute Force Attacks, Horizontal/Lateral Account Movement, Breached Passwords, Concurrent Logins, Account Hacking, and more. **Authentication-based Attack Detection** - Detect advanced threats and suspicious activity patterns indicative of Brute Force Attacks, Horizontal/Lateral Account Movement, Breached Passwords, Concurrent Logins, Account Hacking, and more. **File System Attack Detection** - Detect unusually high volumes of file activity indicative of crypto ransomware attacks and data exfiltration attempts. **Sensitive File Access Alerting** - Monitor and alert on access to sensitive files, folders, or shares for security intelligence and compliance fulfillment. **File Access Blocking (Windows only)** - Block access to particularly sensitive shares, folders, or files regardless of natively assigned access rights. **Non-Owner Mailbox Access Auditing/Blocking** - Detect and optionally prevent non-owner mailbox access events for VIP mailboxes **Mailbox Permission Change Auditing/Blocking** - Detect and optionally prevent changes to Exchange mailbox permissions, with before and after values. **Exchange Configuration Change Auditing/Blocking** - Detect and optionally prevent changes to Exchange configuration settings that can effect security, compliance, or the operational integrity of Exchange.

RECOVER: Recover from cybersecurity events and restore normal operations and services	
23 NYCRR500 Requirement	STEALTHbits Capability
Enterprise Resiliency Organizations must understand how to be resilient, planning how to operate in a diminished capacity or restore services over time based on services' relative priorities	**Granular attribute rollback and recovery** - Rollback and recover single or multiple attributes to a previous point in time of one or more objects using Active Directory snapshots. **Restoration of Deleted Objects** - Restore deleted Active Directory objects with attributes prior to deletion using StealthRECOVER's restore page. **Point-in-time Backups of Active Directory** - Schedule backups of an Active Directory environment to run hourly, daily, or weekly. Additionally, run backups ad-hoc using the "backup now" functionality.

Conclusion

STEALTHbits is uniquely positioned to help with many aspects of the regulation with our portfolio of audit and security solutions. STEALTHbits can automate the reporting that accompanies every audit and put effective controls in place to ensure those reports have only the news you want your auditor to see. But we don't stop at reporting. STEALTHbits provides flexible workflows to control and remediate issues that may lead to compliance violations. Our solutions will identify the business owners of personal information, and allow them to run an access certification program to ensure data access and usage is in line with appropriate business needs. Our solutions can also monitor privileged users to ensure they are not using their rights to access sensitive data. All of these automated controls allow organizations to ensure that compliance guidelines are not circumvented.

To ensure effective coverage across a wide range of environments STEALTHbits is engineered to work across all NAS, Windows File Systems, SharePoint, Exchange, Dropbox, Box, and Office 365.

About STEALTHbits Technologies

STEALTHbits Technologies is a cybersecurity software company focused on protecting an organization's credentials and data. By removing inappropriate data access, enforcing security policy, and detecting advanced threats, we reduce security risk, fulfill compliance requirements and decrease operations expense.

Identify threats. Secure data. Reduce risk.

STEALTHbits Technologies, Inc.
200 Central Avenue
Hawthorne, NJ 07506
P: 1.201.447.9300 | F: 1.201.447.1818
sales@stealthbits.com | support@stealthbits.com