Achieving Compliance with New York State Department of Financial Services Cybersecurity Requirements for Financial Services Companies

Cybercriminals have sought to exploit technological vulnerabilities to gain access to sensitive electronic data and financial transactions, and can cause significant financial losses for any regulated entities and consumers whose private information may be revealed or stolen for illicit purposes. The financial services industry is a significant target for cyber threats due to the direct impact of monetary gain by targeting the industry.

Given the severity of the issue and the risk to all regulated entities, certain regulatory minimum standards are warranted to mitigate flaws in technological advancements. BeyondTrust has been monitoring the legislation from [The New York State Department of Financial Services ("DFS"), 23 NYCRR 500](#), to combat the ever-growing threat posed to information and financial systems by nation-states, terrorist organizations and independent criminal actors. This regulation is designed to:

- Promote the protection of customer information
- Promote the protection of information technology systems of regulated entities
- Requires each company to assess its specific risk profile
- Design a program that addresses its risks in a robust fashion.
- Annual certification confirming compliance with these regulations by senior management.

Achieving Compliance with 23 NYCRR 500

BeyondTrust and the New York State Department of Financial Services encourage all financial entities with business in New York state to act promptly to adopt a cybersecurity program that meets these objectives. BeyondTrust solutions can meet the requirements in [23 NYCRR 500](#):

Section	Description	BeyondTrust Solution
500.0	Introduction	Not Applicable
500.01	Definitions	Not Applicable
500.02	Cybersecurity Program	Not Applicable
500.03	Cybersecurity Policy	BeyondTrust has generic policy templates for financial organizations to implement best practices as a part of their cybersecurity program.
500.04	Chief Information Security Officer	Not Applicable
500.05	Penetration Testing and Vulnerability Assessments	BeyondTrust's Retina family of solutions can meet or exceed the requirements for vulnerability assessment and seamlessly integrate into multiple penetration testing solutions.

Section	Description	BeyondTrust Solution
500.06	Audit Trail	BeyondTrust's PowerBroker Privileged Access Management solutions provide complete audit logging, session monitoring, and privileged access reporting to meet this requirement.
500.07	Access Privileges	BeyondTrust's PowerBroker Privileged Access Management solutions provide managed access based on privileges, assets, and users for any platform from Unix, Linux, Mac, and Mac OS.
500.08	Application Security	This requirement is focused on procedures and guidelines and application security. While BeyondTrust's solutions can help with application security, the requirement is more procedural than documentation.
500.09	Risk Assessment	BeyondTrust's PowerBroker Privileged Access Management and Retina Vulnerability Management solutions provide detailed risk assessment information on assets and users with documentable best practices for risk management.
500.10	Cybersecurity Personnel and Intelligence	Not Applicable
500.11	Third Party Security Policy	Not Applicable
500.12	Multi-Factor Authentication	BeyondTrust's PowerBroker Privileged Access Management solutions support multi factor authentication natively per module and with the BeyondInsight IT Risk Management Platform.
500.13	Limitations on Data Retentions	BeyondTrust's solutions have adjustable options to keep raw and normalized data to meet these requirements.
500.14	Training and Monitoring	Not Applicable
500.15	Encryption and Nonpublic Information	Not Applicable
500.16	Incident Response Plan	Not Applicable
500.17	Notices of Superintendent	Not Applicable
500.18	Limited Exemption	Not Applicable
500.19	Enforcement	Not Applicable
500.20	Effective Date	BeyondTrust's solutions are generally available for the effective date for execution of January 1, 2017 and Cybersecurity Security Regulation date of January 15, 2018.
500.21	Transition Date	Not Applicable
500.22	Severability	Not Applicable

The number of cyber events has been steadily increasing and estimates of potential risk to financial services industry are irrefutable. Adoption of this cybersecurity program and standardization on policies and procedures is the only way to insure the security of the financial systems within New York State. BeyondTrust solutions for Privileged Access Management and Vulnerability Management can meet the requirements and provide coverage for many of the sections in 23 NYCRR 500.

The PowerBroker Privileged Access Management Platform

The PowerBroker Privileged Access Management platform is an integrated solution to provide control and visibility over all privileged accounts and users. By uniting capabilities that many alternative providers offer as disjointed tools, the PowerBroker platform simplifies deployments, reduces costs, improves system security and closes gaps to reduce privileged risks.
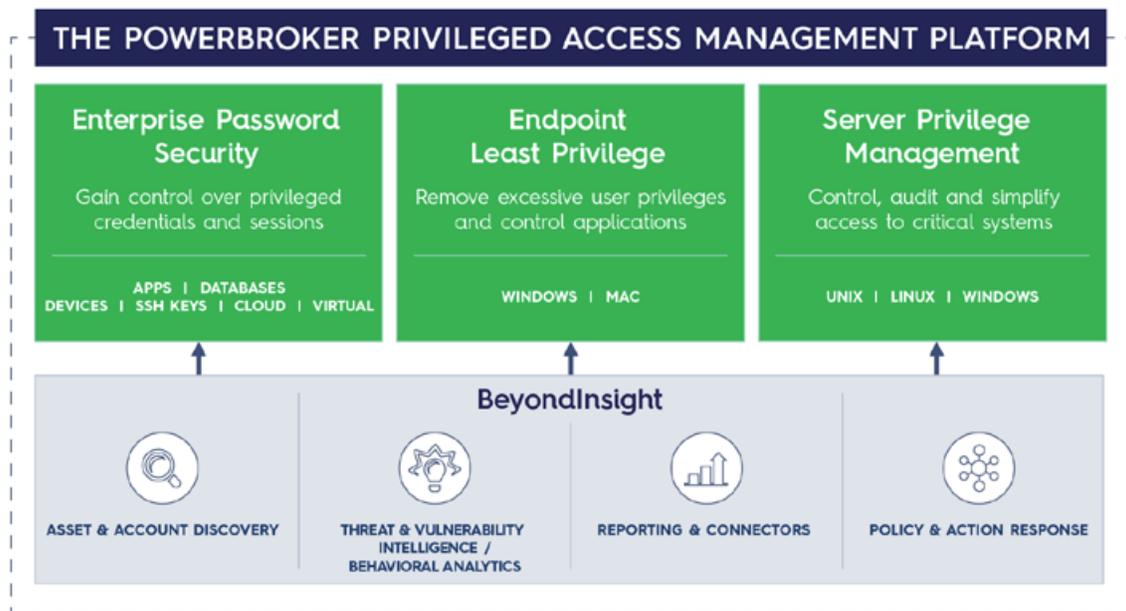
Retina Enterprise Vulnerability Management

For organizations looking to coordinate their cyber defenses, BeyondTrust Retina shares real-time threat and vulnerability information with other systems to pinpoint high-risk assets and shorten remediation times. Unlike other vulnerability solutions, Retina helps organizations break the endless loop of find and fix by connecting with third-party network and security solutions to automate their interactions, synchronize their intelligence and stop threats before they exfiltrate your data.

About BeyondTrust

BeyondTrust® is a global cyber security company that believes preventing data breaches requires the right visibility to enable control over internal and external risks.

We give you the visibility to confidently reduce risks and the control to take proactive, informed action against data breach threats. And because threats can come from anywhere, we built a platform that unifies the most effective technologies for addressing both internal and external risk: Privileged Access Management and Vulnerability Management. Our solutions grow with your needs, making sure you maintain control no matter where your organization goes.

BeyondTrust's security solutions are trusted by over 4,000 customers worldwide, including over half of the Fortune 100. To learn more about BeyondTrust, please visit www.beyondtrust.com.