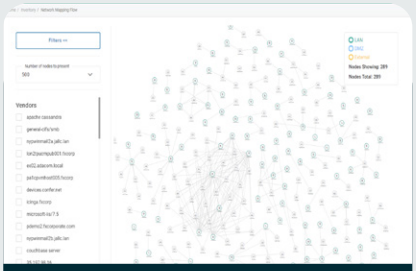
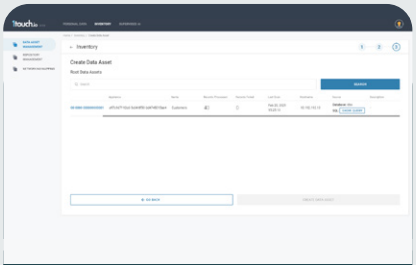
Inventa for NYDFS Compliance

In 2016, the New York Department of Financial Services (NYDFS) proposed its groundbreaking NYDFS Cybersecurity Regulation, 23 NYCRR 500 – a series of regulations that impose requirements on financial institutions that operate under the department's guidance. Banks, mortgage companies, insurance companies, etc. are required to develop and have in place a cybersecurity policy and incident response plan that prioritizes customer data privacy and risk assessment.

1touch.io's Inventa platform is designed to support adherence to regulatory requirements, offering tools that promote compliance and reduce the risk of breaches and the consequent penalties.



Data Mapping & Discovery



Data Asset Policies

Section 500.02 Cybersecurity Program

This section requires entities to implement a cyber risk assessment program, apply policies to protect the data in the organizational systems, respond to cybersecurity events, and report on the event.

Inventa provides network mapping & discovery capabilities, supporting dynamic risk profiling based on the type and location of sensitive data in the network.

Inventa's policy implementation tools are applicable on the data asset level, enabling institutions to design and implements data protection procedures.

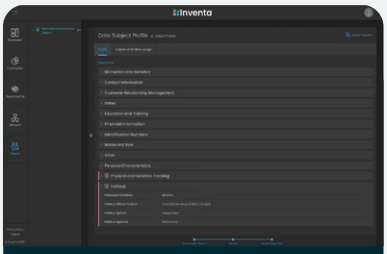
In addition, Inventa supports post-event analysis, identifying the exposed information based on breach location, and enabling prioritized response and compliant reporting.

Section 500.03 Cybersecurity Policy

This section requires entities to implement and maintain policies for sensitive data based on parameters such as data governance and classification, access and identity management, customer data privacy, and more.

Inventa provides sensitive data discovery and classification in structured and unstructured data sources across data at rest and data in motion with unparalleled accuracy.

Inventa seamlessly integrates with 3rd party SIEM/SOAR solutions, generating alerts and notifications when data is moved outside the network or permitted locations.



Data Mapping & Discovery

Section 500.11 Penetration Testing & Vulnerability Assessments

This section requires entities to implements systems that detect, on an ongoing basis, changes in Information Systems that may create or indicate vulnerabilities.

Inventa's network-based discovery identifies all sensitive information in the organizational network – including information users were not aware of.

Inventa's continuous discovery capabilities deliver near real-time insights into the status and dynamics of sensitive data in the organizational network – as well as supporting alerts and notifications in the event of sensitive data copying or transfer via integration with 3rd party solutions.

Regulatory Actions

Residential Mortgage Services, Inc.

Data breach violations

1.5M US$ Fine

First American Title Insurance Company

Exposed hundreds of millions of documents

NYDFS Seeks Fines of 1,000 US$/violation

First Unum Life Insurance Company of America & Paul Revere Life Insurance Company

Falsifying compliance

1.8M US$

Section 500.06 Audit Trail

This section requires entities to maintain systems capable of creating audit trails.

Inventa tracks all sensitive data transactions, identifying copying and movement of sensitive data files in and out of the network – as well as between repositories in the network.

Section 500.09 Risk Assessment

This section requires entities to conduct periodic risk assessments, updated as per changes in the systems and sensitive data.

Inventa provides in-depth discovery for accurate, up-to-date mapping of organizational data assets, with full visibility into sensitive data: location, movement, encryption, and more.

Section 500.11 Third Party Security Policy

This section requires entities to apply security policies to data accessible to or shared by third party service providers.

Inventa provides insights into network integration with 3rd party systems, tracking sensitive data as it enters and exists the network and provides alerts for sensitive data migration into or out of the organization via 3rd party integrations.

Section 500.13 Limitations on Data Retention

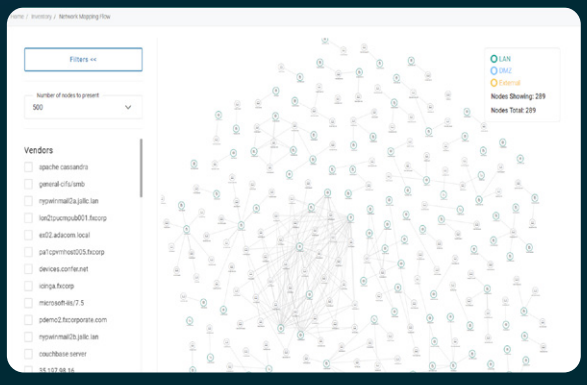
This section requires entities to periodically dispose of any sensitive data that is no longer necessary for the business operations.

To delete information – you have to be aware of both its existence and its location. Inventa provides near real-time insights into all sensitive data – including data users were not aware of. As data becomes irrelevant, Inventa's advanced AI and Search capabilities allow users to locate its existence and location and ensure all copies have been removed is gone once deletion has been implemented.

Inventa is the Future of Data Aware Security

Inventa is the only data discovery platform that automates the entire discovery process—completely hands free using a network first approach coupled with AI and NLP sensors. With Inventa, sensitive data is discovered and tracked continuously, supporting data classification, data mapping, and ongoing monitoring of transactions into and out of the organizational network.

Regulatory Need	Inventa Solution
Sensitive data inventory	Up-to-date mapping of organizational network, data, and nodes
Visibility into data sharing	Data transaction analysis
Data policy implementation	Policy implementation on data asset level
Security event response plan	Post breach insights for response prioritization and implementation
Periodic deletion	Location of all known and unknown sensitive data and all copies.



Identify data lineage for each data entity, and track data transfer into, within, and out of your organizational network

Discover and map the location of all sensitive data copies in your organizational network