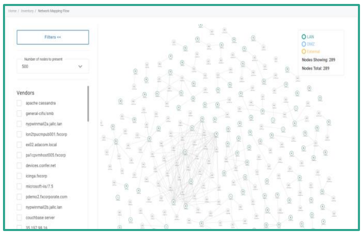
1touch.io
Data Aware Security

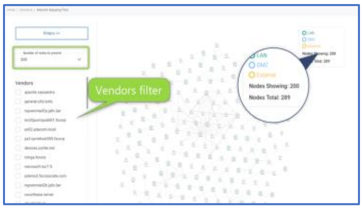
Inventa™ for NIST Cybersecurity Compliance

National Institute of Standards and Technology (NIST) guidance provides the set of standards for recommended security controls for information systems at federal agencies. Originally intended only as guidelines under then-President Obama's executive order, these standards are now being implemented at government offices under the executive order signed by President Donald Trump.

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.



Network Mapping & Discovery



Network Vendor Mapping

ID.AM-1

Physical devices and systems are inventoried

ID.AM-2

Software platforms and applications are inventoried

ID.AM-3

Organizational data flows are mapped

Inventa provides continuous discovery and network mapping features, showing the communication nodes (databases, file systems, and other network elements as PCs) discovered by the analytical appliances, links between the nodes, and the node type like database, central storage, web application and others.

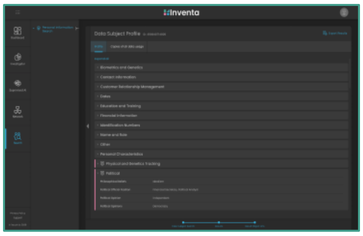
For each network element, the system also discovers metadata - node properties used for filtering the elements displayed on the network map like IP address, subnetwork, vendor, protocol, and the appliance that discovered the node.

ID.AM-5

Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value

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

This information is updated in near-real-time using Inventa's continuous discovery capabilities, providing organizations with dynamic and accurate insights into the classification, criticality, and business value of data in various repositories.



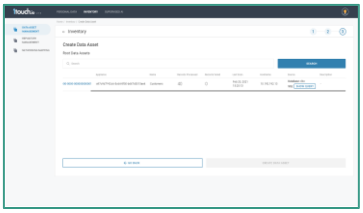
Data Classification

1touch.io
Data Aware Security

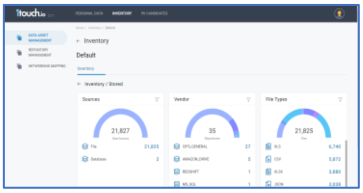
ID.GV-4

Governance and risk management processes address cybersecurity risks

Inventa provides in-depth discovery for accurate, up-to-date dynamic risk management, with full visibility into sensitive data: location, movement, encryption, and more.



Data Asset Policies



Data Asset Management

ID.RA-1

Asset vulnerabilities are identified and documented

ID.RA-5

Threats, vulnerabilities, likelihoods, and impacts determine risk

ID.RA-6

Risk responses are identified and prioritized

Inventa's network mapping & discovery supports dynamic risk profiling based on the type and location of sensitive data.

Inventa's policy implementation tools are applicable on the data asset level, enabling organizations 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.

PR.DS-1

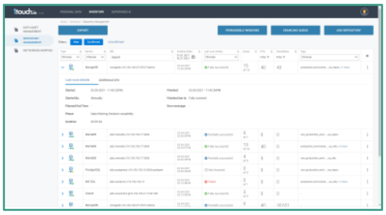
Data-at-rest is protected

PR.DS-2

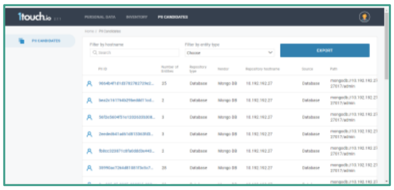
Data-in-transit is protected

Inventa's network-based discovery tools analyze and identify all data in transit and data at rest within the organizational network: including data users are not familiar with, in unknown repositories.

In addition, Inventa identifies and locates all copies of data, and monitors all data transfers, providing a full and up-to-date image of all data, in transit and at rest, allowing the organization to determine and apply appropriate protection and safety measures..



Near Real Time Data Discovery



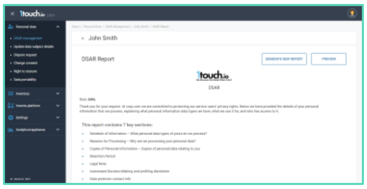
Automatic Data Matching

ID.AM-5

Assets are formally managed throughout removal, transfers, and disposition

PR.IP-6

Data is destroyed according to policy



DSAR Management

Inventa monitors and catalogs all data transfers and copies, enabling full insight and control into data movement and scope.

In addition, Inventa offers a DSAR management module, which supports data subject removal and modification requests.

1touch.io
Data Aware Security

ID.GV-4

Audit/log records are determined, documented, implemented, and reviewed in accordance with policy

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.

PR.DS-5

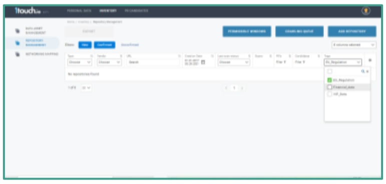
Protections against data leaks are implemented

PR.DS-6

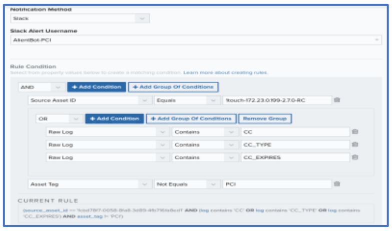
Integrity checking mechanisms are used to verify integrity

Inventa monitors network data status continuously and automatically, including identification of data transfers in and out of the organization.

Through simple and seamless integration with 3rd party platforms such as SIEM/SOAR, Inventa enables alerts, notifications, and automatic protocol initiation when unauthorized data transfers occurs into, out of, or within the organization between different locations and repositories.



Asset Tagging for 3rd Party Integration


Notification Method
Slack
Slack Alert Username
AlertBot-PCI
Rule Condition
Select from property values below to create a matching condition. Learn more about creating rules.

AND | + Add Condition | + Add Group Of Conditions
Source Asset ID | Equals | 1touch-172.23.0.199-2.7.0-RC
OR | + Add Condition | + Add Group Of Conditions | Remove Group
Raw Log | Contains | CC
Raw Log | Contains | CC_TYPE
Raw Log | Contains | CC_EXPIRES
Asset Tag | Not Equals | PCI

CURRENT RULE
(source_asset_id == '[illegible]' AND (log contains 'CC' OR log contains 'CC_TYPE' OR log contains 'CC_EXPIRES') AND asset_tag != 'PCI')

SIEM Integration

Exposed Data Subject Analysis

Exposed Data Usage Analysis

DE.AE-2

Events are analyzed to understand targets & methods

DE.AE-4

Impact of events is determined

DE.AE-5

Incident alert thresholds are established

Inventa provides an accurate profile of data exposed in a breach, allowing operators to prioritize breach response activities, receive immediate insights into the type and sensitivity of the exposed data, and respond with the appropriate procedures.

Inventa adds business context to the post-event analysis process, with layers of data-based information. Inventa provides information regarding Data Mapping, Data Metadata, Data Copies, and more.

DE.CM-1

The network is monitored to detect potential cybersecurity events

DE.CM-6

External service provider activity is monitored to detect potential cybersecurity events

Inventa's network mapping module provides near real time insights into network usage and identifies data entry into the network- as well as data existing the network.

3rd party connections are identified, and data entering through their connection is monitored. 3rd party integrations offer alerting and notification functions.

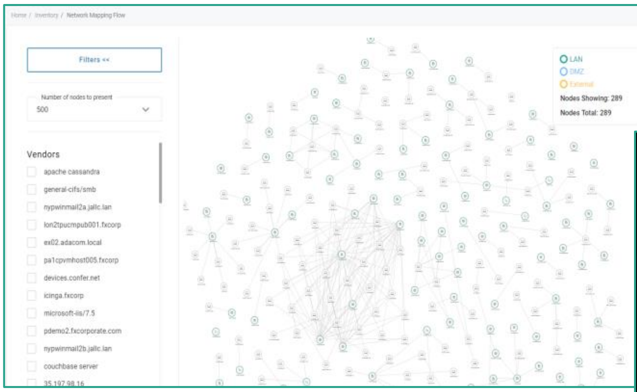
Network Mapping & Monitoring

1touch.io
Data Aware Security

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
Data & asset inventory	Up-to-date mapping of organizational network, data, and nodes
Risk & protection assessment	Accurate data classification and matching for dynamic assessment
Data policy implementation	Policy implementation on data asset level
Security event response plan	Post breach insights for response prioritization and implementation
Data deletion	Location of all known and unknown sensitive data and all copies.



Number of nodes to present: 500

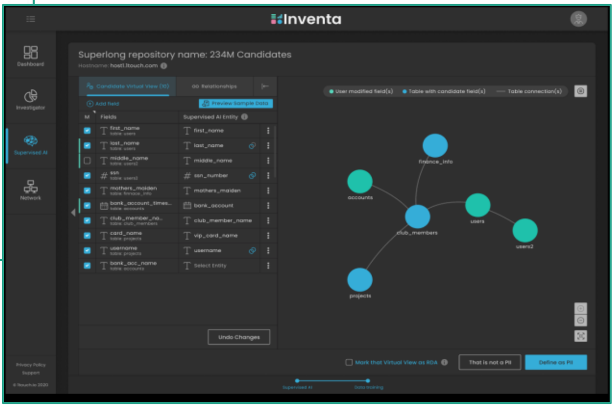
Vendors

- □ apache cassandra
- □ general-cifs/smb
- □ nypwinmail2a.jallc.lan
- □ lon2tpucmpub001.fxcorp
- □ ex02.adacom.local
- □ pa1cpvmhost005.fxcorp
- □ devices.confer.net
- □ icinga.fxcorp
- □ microsoft-iis/7.5
- □ pdemo2.fxcorporate.com
- □ nypwinmail2b.jallc.lan
- □ couchbase server
- □ 35.197.98.16

Nodes Showing: 289
Nodes Total: 289

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



Superlong repository name: 234M Candidates
Hostname: host1.1touch.com

M	Fields	Supervised AI Entity
☑	first_name table: users	first_name
☑	last_name table: users	last_name
□	middle_name table: users2	middle_name
☑	ssn table: users3	ssn_number
☑	mothers_maiden table: finance_info	mothers_maiden
☑	bank_account_times... table: accounts	bank_account
☑	club_member_na... table: club_members	club_member_name
☑	card_name table: projects	vip_card_name
☑	username table: projects	username
☑	bank_acc_name table: accounts	Select Entity

□ Mark that Virtual View as RDA

1touch.io LLC • 122 Grand Street, NYC 10013, NY USA • (475) 292-0843 • 1touch.io • info@touch.io