Zero Trust for Sustainable Data Discovery

THE CHALLENGE

Former Forrester analyst John Kindervag introduced us to "Zero Trust" in 2010, and since then, it has become one of the more popular frameworks in cybersecurity. **Massive data breaches, regulatory fines and growing risk associated with data protection has proven that companies need to be more proactive about cybersecurity, particularly around data discovery for privacy**, security, and governance, and a Zero Trust model might be the right approach.

THE SOLUTION

Zero Trust is based on the premise that not even users behind the firewall can be trusted. User error and insider threats continue to be a significant risk for organizations.

To ensure data security in the face of both internal and external threats, data discovery and control should be at the heart of organizational risk management. **Organizations need complete visibility into their data - where it is saved, how many copies exist, and where the data has moved over time** - in order to identify any unusual patterns or unauthorized activities that may point to the existence of an internal - or external - security risk.

> Companies need to be proactive about cybersecurity, particularly around data discovery

> Organizations need complete visibility into their data - where it is saved, how many copies exist, and it has moved

1touch.io Zero Trust Model

Zero Trust People

Zero Trust Network

Zero Trust Applications

Zero Trust Devices

Implementing a Zero Trust Framework can protect companies from advanced cybersecurity threats and data breaches and regulatory risk while helping achieve compliance with CPRA, CCPA, GDPR, HIPAA, and any future requirements.

Data privacy and security is at the center of Zero Trust – and data discovery & monitoring is the most crucial step to ensure privacy, security, and governance.

AUTHENTICATION & VERIFICATION

The first principle of Zero Trust is to authenticate and verify existing data discovery processes:

- **What kind of sensitive information does your company have in its network?**

- **Do you have a complete and updated knowledge of different networks, repositories, and applications where sensitive information is saved?**

- **Do you have a robust process to respond to DSAR requests as part of regulatory requirements - and can you ensure that the process is secure and private?**

- **Do you have a vetting process that only allows authorized personnel to access sensitive data?**

- **Do you have a comprehensive process to determine if/when data can be shared with a third party?**

- **Can you monitor data transfer and identify where and when copies of sensitive information are moved and saved?**

The underlying assumption here is that every attempt to access data is a threat, and every instance of data transfer and copying is a risk - regardless of the location of access or hosting model.

DISCOVERY & MAINTENANCE

Zero Trust principles require inspection and verification of every bit and byte of data in your organizational network: discovering and monitoring data at rest and at motion, logging every network call, file access, and email for malicious activity, and identifying the location of every data instance in every repository. This is not something a human or an entire team of humans can accomplish - and certainly not in the continuous, ongoing manner required to keep up with the mutable datascape of a large organization.

Traditional data discovery tools are no more than data mapping solutions that require the customer to point them towards the location and type of PII they wish to discover: they cannot locate or identify sensitive information in unknown locations across unstructured and structured files, databases, and repositories - or discover data beyond standard PII.

They cannot monitor the transfer of all sensitive data records - or provide a detailed breakdown of the location of every record instance. Their limited classification capabilities make it impossible to build a full and sustainable picture of data usage.

Continuous discovery, monitoring, and cataloging are the most critical capabilities for maintaining a Zero Trust security model

SUSTAINABLE DISCOVERY

The right system will offer fully automated data discovery for continuous discovery

Continuous discovery, monitoring, and cataloging are the most critical capabilities for maintaining a Zero Trust security model. With robust discovery, monitoring, cataloging, and data analytics in place, you can identify sensitive data stored in different repositories, pinpoint the source and target locations of sensitive record transfer processes, and use this information to make informed decisions regarding privacy, security, and governance mandates.

Zero Trust starts with data discovery. Here are some key recommendations for effective data discovery, monitoring, and cataloging.

Data Discovery

Figure out where your sensitive data lives, how many copies of the data exist, and who has access to it. **You have to know where your sensitive data lives and who has access to your data before you can protect it.**

Data Patterns

Analyze the movement of data in your organization: who is making copies, and where are those copies located? How much data is being moved around, which kind of data is being transferred, at what volumes – and who is doing most of the moving?

You need to understand the patterns of data movement in your organization – and to be able to identify unusual data activity in order to identify risks and threats.

Network Mapping

You need to understand the topology of your network: which nodes are connected? Which elements can and do communicate with one another? Which elements have traffic between them – and when and how does that traffic start and stop? **You have to understand communication within your network** to identify potential leaks and breaches.

1touch.io's network-first approach offers:

- **Sustainable Automated Discovery:** Locate sensitive data at rest/ motion (transit), structured/ unstructured, and known/unknown

- **Fully Updated Catalog:** Rationalize sensitive data saved in different formats and files and create a smart catalog of all the PII data

- **Accurate Data Lineage:** Provides continuous and full visibility in the data life cycle, including data origin and where it moves over time and identifies how many copies of that data, exist

- **Transfer Logging:** Delivers accurate breakdown of data transfer activities, including identification of which sensitive data records have been transferred, where from - and where to.

- **Automatic Mapping:** Continuous mapping of network topology and communications.

Organizations need complete visibility into their data: location, all copies, and transactions

1touch.io provides an accurate view of data socmpanies can make informed decisions

1touch.io's network-first approach offers:

- **1touch.io** requires far less operational overhead and is mucheasier to manage

- **1touch.io** provides business leaders with an accurate view of their data to make informed decisions for privacy, security, and governance

- **1touch.io** fully supports any kind of operational topology: fully on-premises, hybrid, or 100% cloud.

About 1touch.io

Founded in 2017 and backed by the world's largest Cyber Security investor group, **1touch.io**'s vision is to lead the market with the only sustainable Sensitive Data Discovery Solution.

Our 3 Founders have extensive experience in Data Discovery, Data Analysis and Network Security; Together they developed a joint US Homeland Security and Israeli Defense solution to identify personal profiles of individuals in real-time across dozens of Security Services and Border Control organizations.

About Inventa

Inventa offers a unique and proprietary passive network packet capture process , identifying repositories and network transactions containing personal data throughout the organizational network. This process allows **Inventa** to discover any data, on-prem or in the cloud, structured or unstructured, in motion or at rest, to create a master catalog of personal data.

Inventa leverages artificial intelligence and machine learning to consolidate and normalize identities to provide a unified view of personal data across disparate repositories, data sources, applications & use cases.

Inventa consolidates personal data in a catalog that allows user to see data lineage, respond to subject access requests, identify production data in non-production locations, and many other privacy, security, and data governance tasks