THE EMERGING NETWORK APPROACH

TO THE CONTINUOUS DISCOVERY, MAPPING AND FLOW DETECTION OF PERSONAL DATA

SYSTEMS VS NETWORK BASED APPROACH

We are now in an evolving era of automated personal data usage detection in the enterprise. This is a necessity due to the current and anticipated proliferation of regulations surrounding the use of personal data (**GDPR, CCPA....**). We find that manual responses to this burgeoning problem have fallen short of the demands placed by the regulators and the people. In addition, this becomes a very time consuming and costly procedure.

In the digital age, consumers and regulators expect instant answers and accountability. In an answer to these automation requirements, two approaches have emerged: **The System Approach and the Network Approach.**

THE SYSTEM OR SEMI-AUTOMATED APPROACH

During 2016 and 2017, with the publication and ongoing coverage and panic over **GDPR** requirements, legacy solutions that weren't created for regulation pivoted their technologies to meet the demands of privacy regulation, in particular the holy grail - the 'discovery' of personal data usage.

The System Approach treats each system separately and requires manual identification of the systems to discover whether they hold personal data. Following this, the question of whether a solution can detect structured data or personal data was dealt with, resulting in a haphazard effort to track a unique identity through the network whether it is structured or unstructured data, data in rest or data in motion. This piecemeal effort results in a substantial amount of heavy lifting by the customer with unacceptable operational overload.

This has led to an excess of solutions that do some of the above, and with very few truly doing all of the above.

The glaring problem with this approach is simply put 'you don't know what you don't know' or as our customers like to state, "these legacy systems can tell you where your personal data is...once you can tell it where your personal data is!"

The blindness to all personal data usage within the organization exposes the enterprise to risk, not only from non-conformity to regulatory requirements, but also to excess hoarding of personal data when not needed. It's a security issue as well, not just a privacy one.

By creating a relationship-based network map of personal data usage, virtually any regulatory or security question related to the use of personal data can be answered:

OPERATIONAL VALUE

Ease of implementation and management. Simply send a copy of network Ital traffic to the system, and define an Initial Asset (to make sense of the personal data usage — e.g. HR, IR VIP Customers, Partner etc.) and you are good to go.

BUSINESS VALUE

Be sure that you have the most up-to-date and relevant information to avoid fines and bad publicity so you can focus on growth instead of regulation.

FINANCIAL

Pay directly according to the risk your hoarding of personal data poses. The less personal data you store, the less you pay in annuities. Don't pay for replicated personal data or to crawl systems that don't have personal data at all.
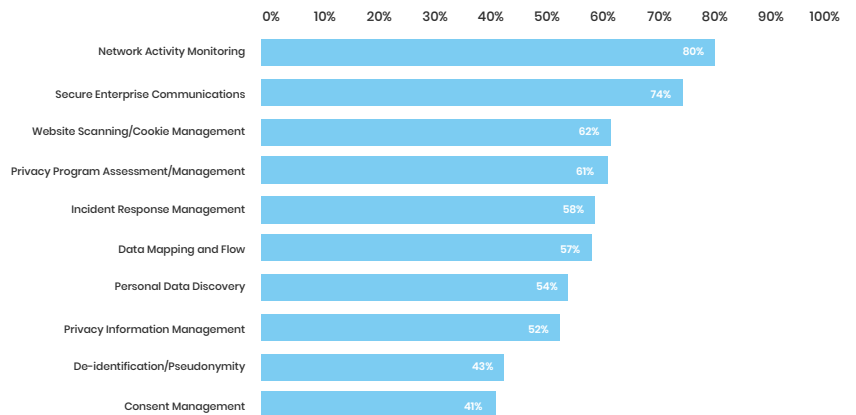
TECHNICAL

We do all of the heavy lifting for you, so you can focus your technical expertise on mission critical projects.

THE NETWORK APPROACH

A recent joint report by **TrustArc** and **IAPP** discovered that 80% of enterprises were looking to purchase a network activity monitoring based solutions to answer the challenges relating to Privacy.

Organizations that have purchased or are planning to purchase:

Network Activity Monitoring	80%
Secure Enterprise Communications	74%
Website Scanning/Cookie Management	62%
Privacy Program Assessment/Management	61%
Incident Response Management	58%
Data Mapping and Flow	57%
Personal Data Discovery	54%
Privacy Information Management	52%
De-identification/Pseudonymity	43%
Consent Management	41%

The reason is clear. By analyzing traffic on a continuous basis as well as repository stores connected to that network, a network-based solution can, in real-time, detect all elements on the network that are storing, processing and sharing personal data, both outside and inside the network. Such a system can, at will, crawl any repository or database either confirmed to or suspected of processing personal data, whether it is known or unknown to the enterprise. In this way a solution can give a truly holistic view as to how and where personal data is being used. Whether it is data in motion or data in rest, structured or unstructured data and especially if known or unknown.

Contact us to discover our innovative way of handling encrypted traffic and database crawling — that's pretty cool too!

1touch.io