# Inventa ™ for Educational Institutions

Institutions of learning manage a wide range of personal and sensitive data: not just student and faculty names and addresses – but also grades, performance reviews, and medical information. According to a CyberSecurity industry report, 2020 marked a "record-breaking" year for cyber attacks against schools, and education managers and policy managers are seeking ways to make sure the sensitive data under their charge is safe.

EXPOSURE RISK MANAGEMENT

The diffusion of data across school systems - grading systems, submission portals, email servers, etc. – increases the danger of a data breach or unauthorized transfer of sensitive information. Data minimization helps manage this risk by reducing the potential attack surface.

K-12 Cyber Center 2020 Report
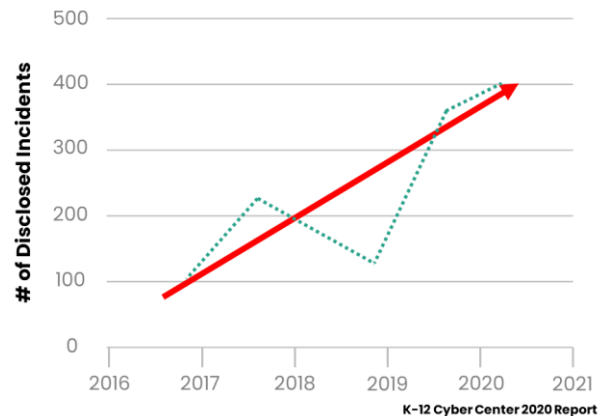
IDENTITY VALIDATION

Students and faculty require access to different types of sensitive data across a range of systems. The result is many avenues for DDOS and phishing attacks– either to flood and crash the system, or to trick systems into releasing protected data. The solution is a secure and efficient user validation system that is as close to foolproof as possible.

June 2020

Microsoft Security Intelligence discovers that over the course of a single month the education sector was subject to
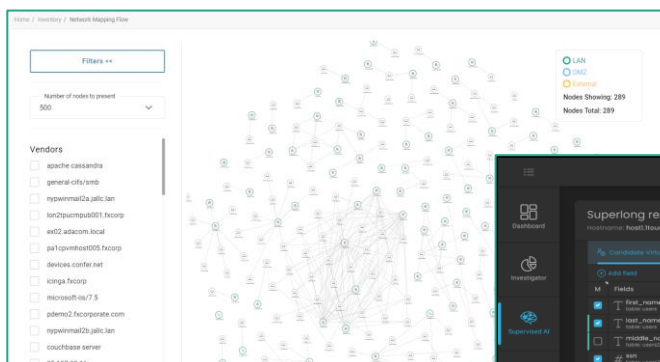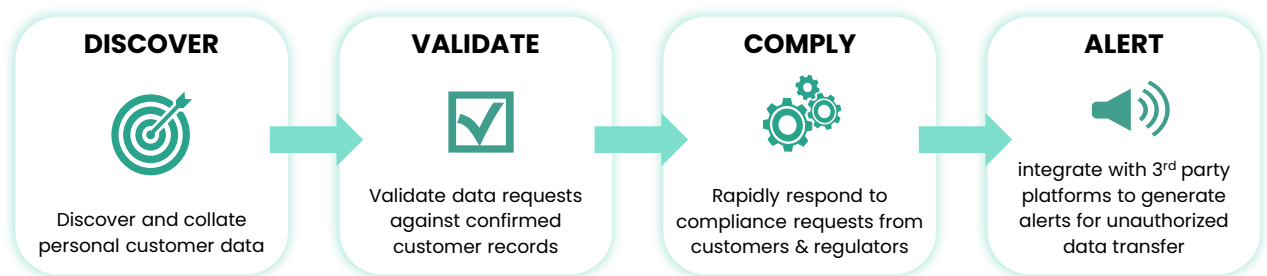
4.6M Malware Attacks

COMPLIANCE

While the Family Educational Rights and Privacy Act of 1974 (FERPA) does not require educational institutions to adopt specific security controls, breaches can lead to a violation of FERPA – along with a host of legal, PR, regulatory implications..

1touch.io offers educational institutions an effective, efficient, and secure solution that helps protect the sensitive information in their network by minimizing data exposure, validating user identities, tracking student and faculty records, and supporting compliance needs and IT security operations.

Inventa™ is the Future of Data Discovery

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, lineage identification, and ongoing monitoring of transactions into and out of the organizational network.

DISCOVER

Discover and collate personal customer data

VALIDATE

Validate data requests against confirmed customer records

COMPLY

Rapidly respond to compliance requests from customers & regulators

ALERT

integrate with 3rd party platforms to generate alerts for unauthorized data transfer

Discover, map, and merge all sensitive data copies in your organizational network

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