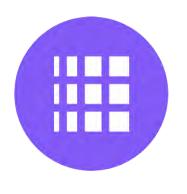## Finding PII At Greater Scale & Accuracy Than DLP

Data Discovery Beyond DLP

You cannot protect what you cannot find. The challenge that many organizations first face when they look to enhance data security or meet proliferating privacy regulations is accurately identifying what is and isn't personal identifiable information. Legacy tools like DLP with their dependence on Regular Expression matching and lack of context awareness struggle distinguishing between similar looking data, can't always scan both structured and unstructured data sources, fail to measure data sensitivity and can't discern residency. BigID's data science based discovery, correlation and classification gives organizations a first of its kind protection and privacy solution, purpose-built for identity data.

Heat Maps

Without understanding where personal data is stored, it's difficult to implement policies and controls for how that data is moved, used and secured. Knowing where to look, and what to look for is critical in the PII discovery process. For that reason, in addition to performing detailed attribute level discovery, BigID can also provide fine-grained analysis to rapidly 'heat map' PII concentrations across data center endpoints and cloud. This has benefits in multiple use cases, including cloud migrations where assessment of server data sensitivity is essential as well as developer environments where data stores and micro-services should be monitored for potential PII contamination.

PII Inventory

Locating sensitive PII is essential to protecting it. However data maps alone can't provide a complete protection or privacy picture. New privacy protection regulations mandate an individual's right to access their own data, the right-to-be-forgotten, the right to port their data and the right to be notified of a breach. All these require knowing what data belongs to whom. BigID's patent-pending data discovery technology determines which data belongs to which data subject and with what level of correlation. This way BigID enables organizations to protect their customers' privacy and comply with the emerging privacy regulations.

Finding PII At Greater Scale & Accuracy Than DLP

Accuracy at Scale

Personally identifiable data is a legal concept, not a technical concept. The challenge with pattern matching based on regular expressions is the approach doesn't integrate enough context to distinguish between data that may have similar formats (such as Social Security number and a telephone number), but have very different implications for privacy protection. BigID utilizes a combination of machine learning and analytics to automatically calculate the identifiability of attributes and sets of attributes (including pseudo identifiers) improving accuracy of what gets classified as personal data. Moreover by distributing search across big data end points, limiting discovery scope to known or learned PII and by pre-sampling the data using heat map surveys, BigID is able to find the PII both more accurately and at scale.

Data Minimization

Increasingly organizations are adopting data minimization strategies for security and privacy reasons. By deleting or reducing inessential duplicate or unused data, organizations can minimize potential attack vectors. Unlike prior discovery tools, BigID can both quickly report on duplicate data but also provide residency and usage detail so minimization strategies can be based on secondary factors like jurisdiction and activity history.

How BigID Can Help

BigID is transforming enterprise protection and privacy of personal data. Organizations are facing record breaches of personal information and proliferating global privacy regulations with fines reaching 10% of annual revenue. Today enterprises lack dedicated purpose built technology to help them track and govern their customer data. By bringing data science to data privacy, BigID aims to give enterprises the software to safeguard and steward the most important asset organizations manage: their customer data.