Understanding what employees and applications have access to what data is critical for stopping data overexposure, insider threats and meeting critical security and privacy regulations like NY DFS Cybersecurity Regulation (NYCRR), SOX, as well as EU GDPR and California Consumer Privacy Act (CCPA). However, traditional approaches to data access governance have poor identification of sensitive data, have limited data source coverage, and don’t provide insights across both accessing employees and applications. BigID’s new data access insights capability expands its core data intelligence platform with new visibility into who and what is accessing unstructured data in the data center or cloud.

Data Intelligence Meets Access Intelligence

Organizations face mounting urgency to identify sensitive data across their data landscape to both better protect it and satisfy emerging privacy regulations. Traditional data classification tools don’t have the ability to find all personal information, look across all data, or sort data by both type and person. BigID provides a first of its kind identity-centric data intelligence platform that can look across unstructured, structured, Big Data, cloud and more while simultaneously classifying data by type and correlating by person - essential for meeting privacy data rights. Now BigID has added access insights so enterprises can both know what sensitive data they have where, but also whether specific data objects have open access permissions.

Detect Open Access

The best protection for sensitive data is to close accidental open access to the data. Blocking open access can stop hostile internal employees or outsider actors. Using BigID, organizations can now know whether sensitive personal data is over-exposed, to address both emerging privacy mandates like EU GDPR and CCPA as well as reinforce SOX, GLBA and NYCRR compliance. With BigID data access insights, enterprises can prevent data leaks or theft owing to exposed data while demonstrating to auditors and regulators that they have a proactive program in place to identify and protect data from unauthorized access.
Minimize Data Risk

BigID provides a risk-centric view of personal data so organizations can be proactive in reducing risk. The BigID risk module scores risk based on a variety of data parameters like data type, location, and residency. With the new data access intelligence capabilities, enterprises now have any additional dimension of risk analysis they can use to inform risk management decisions. Highly sensitive data that is over-permissioned can be secured, minimized or quarantined until access rights are remediated. Moreover, in the event of a breach, investigators can quickly determine which employees or applications had access to the sensitive data, reducing response times.

Protect Privacy

Security teams are increasingly responsible for finding and protecting personal data. To meet privacy mandates like EU GDPR and CCPA, security teams need to be able to locate PII and PI (personal information), contextualize back to person and also ensure compliant usage. BigID provides a first-of-its-kind data discovery technology for finding and mapping personal data. BigID's access insights capability augments this unique identity-centric data intelligence with access intelligence so that privacy professionals can ensure data usage that is consistent with regulations and continuously monitored.

How BigID Can Help

BigID is redefining personal data protection and privacy in the enterprise. Organizations are facing record breaches of personal information and proliferating global privacy regulations, with fines reaching 4% of annual revenue. BigID gives enterprises software to automate the security and management of structured and unstructured PI across datacenters and cloud. Using BigID, enterprises can better steward their most vital assets: their customer, employee and client data.

For more information, email info@bigid.com or schedule a demo at bigid.com/demo