Sponsored content
CSO FROM IDG

Data Privacy:
The New Security Standard

The modern digital organization has quickly realized that protecting private and sensitive data requires more than simply restricting access to said data. Cybersecurity solutions that protect or limit access to information from hackers as well as internal threats are essential, but they are only the starting point.

What's needed to fully protect the organization: continuous data knowledge leveraging data privacy requirements. These solutions identify, classify, protect, and monitor sensitive and private data; create access rules; and actually execute technical controls for data/security policies. As the name implies, they do this continuously. Constant vigilance and evaluation are critical to ensure that protection is up to date and compliant with changes in governance, risk, and compliance requirements.

Data privacy management requires successful completion of several tasks; it is an evolution. Organizations should be ready for an audit within the rules of statutes and regulations that govern data privacy, in every geography they operate in. All too often, companies that have completed a data classification project feel they are "finished," but classification is just a small component of any legislation.

Things are always changing, as evidenced by 2020. The past several years have seen expanding use of cloud services. It is nearly guaranteed that one result of those changes is private data migrating to Microsoft 365 documents and myriad cloud file services without the organization's knowledge. The best solution not only finds data anywhere but also looks for it regularly. You might be surprised to find out what is being stored in the Notes field in a third-party SaaS platform.

Businesses must start with the assumption that effective data privacy management requires looking everywhere: cloud services, servers, endpoints, third-party SaaS providers, partner organizations, and anywhere else information is stored, managed, or otherwise processed. Simply looking at databases in the on-premises data center isn't enough. What's more, this is not a static task. Data is fluid, and data privacy solutions must be built with continuous discovery and identification activities in place.

Just as a business changes data sensitivity requirements frequently, any data privacy management solution should be agile enough to deal with new or changing rules and statutes. Not only are there regular updates to the known data privacy regulations but new ones arrive all the time. For example, many individual states in the U.S. are enacting data privacy statutes, and the rules vary from one state to another.

Data443's Global Privacy Manager solution provides the protection that organizations need in order to meet today's and tomorrow's data privacy challenges. Organizations can be confident that they are protected by leveraging one comprehensive view, for all privacy requirements, across all enterprise data, all at once.

This unmatched visibility into an organization's data assets ensures that all private and sensitive data can be identified and protected and that enterprises can obey all relevant privacy laws in any jurisdiction. Global Privacy Manager can also protect organizations from the constant movement of data around the business and contains out-of-the-box workflows for businesses of any size, including automated processes to reduce demands on internal staff. End customers benefit from a full privacy portal with customizable consent management and simplified reporting. The portal meets all privacy needs in one location, with accurate explanations of how data is collected and used.

For more information on Data443's Global Privacy Manager, visit https://data443.com/

DATA443