DB CyberTech

Technology Brief

How Deep Visibility Reduces Your GDPR Business Risks

Reducing Your GDPR Risks

Coping with data subject's requests together with the threat of data loss pose enormous business risks to a company's GDPR compliance. As a result, GDPR has been elevated directly into the boardroom. It's typical for company databases to hold highly sensitive data including large amounts of personal data. Having deep visibility along with continuous monitoring of data in motion to and from databases significantly reduces a company's overall GDPR business risks.

Deep Visibility into Data in Motion

Cyber criminals rely of the fact that for most companies data in motion is opaque. The unfortunate result is that once a company's perimeter has been breached the attack dwell time will likely be measured in months. A lot of data can be stolen over that length of time. It's nearly impossible to prevent data loss when you don't have deep visibility into your data in motion.

DB CyberTech's deep visibility into database conversations together with our field proven machine learning technology provides two key benefits to privacy professionals responding to GDPR requirements. These benefits include:

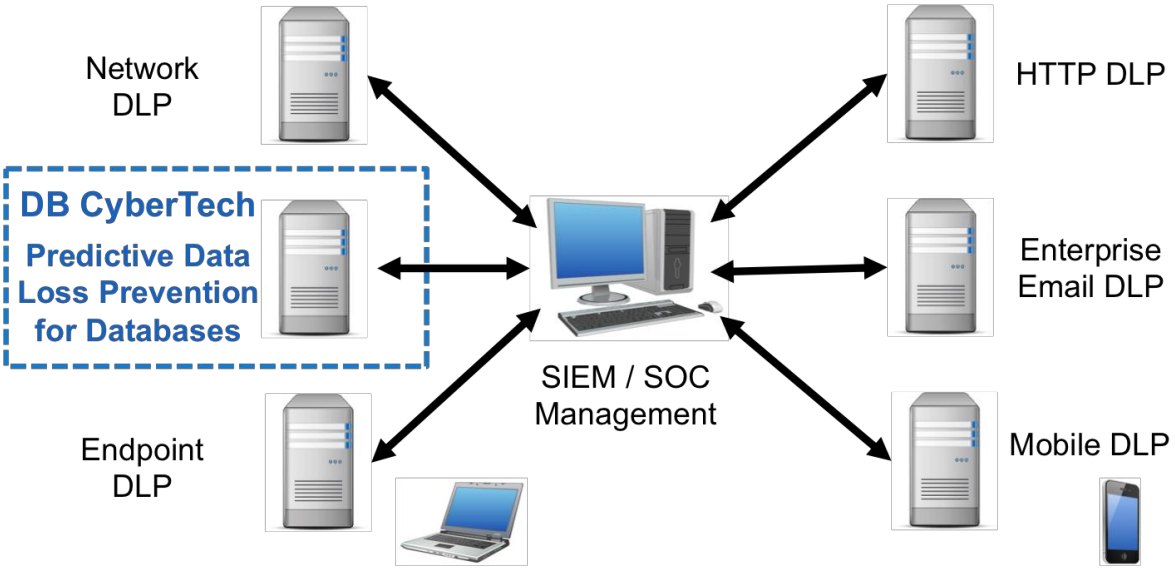
1) Automating the accurate construction of the personal data inventory
2) Ability to predict potential data loss before it happens

Personal Data Inventory

With GDPR, EU residents have the right to request and review their personal data that has been collected on them by companies. EU residents can request that their information be deleted, any errors be corrected, or have all of their personal data sent to them. To facilitate such requests it's necessary to have a current and continuously accurate personal data inventory. However, an individual's personal data may be scattered over numerous databases and throughout a variety of other data stores. It's not possible to respond to a request from a data subject within the required 30-day period without a comprehensive and accurate personal data inventory. Failing to promptly respond to the data subject's specific request could result in legal actions and fines.

Predictive Data Loss Prevention

DB CyberTech utilizes machine learning and behavioral analysis to automatically identify anomalies and to predict potential data theft before it actually occurs. DB CyberTech's predictive data loss prevention for databases seamlessly integrates into enterprise DLP solutions to finally offer full spectrum visibility end to end.



DB CyberTech's Predictive Data Loss Prevention for Databases Integrated into an Enterprise wide DLP

Equifax Breach as a GDPR Case Study

In the fall of 2017, Equifax announced that they had experienced a breach resulting in the loss of database records containing personal and financial data on 143 million individuals. Had this personal data breach occurred under the purview of GDPR, Equifax could have faced over $125 million in fines. Not only did Equifax suffer a massive database breach they didn't issue a notification of the breach for forty days. Forty days is an extremely long period of time for 143 million individuals to be kept unaware that their personal data and financial details have been stolen and are likely being marketed for profit on the dark web. The GDPR requires data controllers to notify a national supervisor data authority "not later than 72 hours" of any breach of personal data once the data controller has become aware of an intrusion. Under GDPR the fines for not reporting a personal data breach within the 72-hour window could have alone exposed Equifax to a fine of over $60 million.

The Equifax breach is proof point that it's impossible to prevent data loss when you don't have deep visibility into your data in motion. Had Equifax implemented predictive data loss prevention for databases they would have become aware of the breach very early in the attack chain such that they could have reacted long before they lost any data.

Conclusion

DB CyberTech Compliance Solutions supports Data Protection Officers and privacy professionals with a completely new paradigm for preventing data loss while ensuring the integrity of the personal data that companies retain. Deep visibility enables companies to proactively respond to threats for potential personal data loss before the data is stolen rather than reacting months after the incident in an attempt to determine the scope of their data loss.

The information data privacy professionals require is derived from our deep visibility into database conversations. From this deep visibility we're able to accurately and automatically classify personal data, including previously unknown and undocumented databases. Deep protocol analysis identifies all assets on all databases, maps databases to their connected applications, and gathers database user behavior analytics. Intelligent data classification extracts the meaning of each query and identifies where personal data resides facilitating the construction of an accurate personal data inventory. This personal data inventory is kept continuously up to date so that requests from data subjects can be rapidly addressed. Finally, machine learning based predictive data loss prevention immediately alerts to the potential for data loss.