Addressing Gaps in DLP for Insider Threats with Data Behavior Analytics (DaBA)

Executive Summary

Many organizations struggle to implement enterprise data loss prevention tools effectively. Unfortunately, security teams lack the visibility tools to show the business where the risks are. Data Loss Prevention programs can address only some of the root problems.

Building DLP policy around data movement is becoming even more challenging. IT may be completely unaware of evolving business practices and the ever growing number of cloud apps that employees rely on.

In contrast, **Data Behavioral Analytics** (DaBA) provides instant visibility by automatically recording and reporting on data movement within the organization without any policies, data classification or file manipulation.

> DaBA *is a new approach which provides complete contextual visibility into the behavior and movement of all data, across on-premise and cloud environments. It immediately detects the improper handling of sensitive data by insiders.*

Finally, a tool that provides instant visibility to quickly identify and respond to data exposure and help enterprises reduce business risk from careless or malicious insiders.

Gaps in Data Loss Prevention (DLP)

DLP solutions are effective for organizations that have the staff to coordinate, implement and maintain complex policies. Unfortunately, legacy DLP solutions cannot address the modern scenarios that cloud apps like Office 365 and new business practices create. Some of the top gaps with legacy DLP include the following:

Data Dispersion: Data is being shared dynamically in real time across a multitude of applications and users. As files are fragmented, encrypted, and sent around the world – organizations can't keep track of all the locations where sensitive data resides. DLP policies and IT/security teams cannot keep up with how people are sharing and exposing data.

Requires Known Policies: DLP effectiveness requires a comprehensive understanding of all sensitive data and the many ways it might leak. If each and every data loss scenario is not identified and then translated into policy, data goes unprotected.

Unrealistic expectations: DLP is not capable of protecting against every type of data theft. Insider threats are increasing in a world of the gig economy where employee turnover is higher and there are more contractors and remote workers. A higher percentage of employees and contractors can easily, accidentally or maliciously expose more sensitive information than ever before.

Lack of relevance to the business: Organizations resist when employees are prevented from using the tools that make them productive. DLP does not directly address any business problems. As a consequence, business leadership is typically unaware of the benefits of DLP for anything other than compliance purposes.

Gaps in Data Loss Prevention (DLP) continued..

Content vs Context: Legacy DLP focuses heavily on content. Unfortunately, malicious users will manipulate sensitive data to hide their actions and bypass DLP content controls, such as encrypting files. Context can provide more value for identifying suspicious activity. In many DLP solutions, contextual elements are limited to file type, sender/recipient, source/destination, ect. In DaBA solutions contextual detection extends further to reveal more relevant detail, such as the network share where a file originated. By protecting against the dispersion of sensitive data, from dedicated servers/files (for financial data or any intellectual property associated with a special project), DaBA provides deeper insights to identify malicious or careless users.

Inspects only on Data Egress Events: DLP's primary role is to prevent data from leaving the organization and is typically limited to data leaving the network or end user workstation. Since most DLP solutions are only capable of inspecting sensitive data at the point of egress, all pre-egress activity goes unchecked and unmonitored, allowing users to extract and manipulate sensitive data to bypass DLP controls.

False Negatives: DLP ignores false negatives. There is no way to assess if DLP is working – until it is not. Activity that doesn't trigger an existing policy is allowed and data surrounding that activity is not retained in any form. As a result, it's impossible to forensically investigate an event that was not in violation of existing policy.

Data Behavior Analytics (DaBA) - Instant Visibility

Data Behavior Analytics (DaBA) provides complete visibility into the behavior and movement of all data, across on-premise and cloud environments. It immediately detects the improper handling of sensitive data by insiders. Via data tracing technology, relevant events are linked together to create a data journal that shows how sensitive data is being improperly exposed.

DaBA records all events (including non-egress) such as:

- All data movement by source/destination
- All data movement by file, type, or content
- All files downloaded from sensitive data repositories
- All files containing sensitive data or keywords
- All files originating in network shares moved to external websites, cloud or removable storage
- All files containing regulated data (PII, PHI, PCI, GDPR, CCPA, PIPEDA, NIST)
- All files containing intellectual property based on content and more importantly **context**
- All cross-domain file sharing (e.g. Employee A data shared with Contractor B or Finance to Sales)
- Specific user file movement
- And more....

DaBA reveals more scenarios that expose risky behavior and potential insider threats. With deeper visibility, even organizations with mature data protection programs will find holes in their DLP strategies and identify new sources of data risk. Scenarios such as users sharing files with PII and employees who are downloading trade secrets to personal storage devices or to the public cloud are more readily visible with a DaBA solution.

Summary

DaBA allows organizations to continue to adapt their forensic and data protection strategies. DaBA records the complete journey of data including new types of locations or new cloud applications. There is no need to predict where data may go because DaBA will be able to reveal all behavior including any new locations your sensitive data is going to.