SOLUTION BRIEF

exabeam

8 KEY FUNCTIONS TO PREVENT DATA LOSS WITH USER BEHAVIOR ANALYTICS

Data Loss Protection (DLP) solutions are widely-deployed as a means of finding sensitive data and detecting (and blocking) the movement of that data to the outside world by rogue or compromised insiders. DLP is used to scan data at rest and identify files and associated systems containing sensitive data, and also to scan data in motion to track sensitive data as it's copied to emails, thumbdrives, etc. While DLP can be effective at fingerprinting and identifying sensitive information, DLP products have limited context about user behavior and can suffer from false positives and negatives.

Applying User Behavior Analytics to Prevent Data Loss

User behavior analytics can provide the context required to evaluate user behavior efficiently and accurately. DLP focuses on the data itself, while UBA focuses on the user handling that data. Together, these solutions can improve analysis of the interaction between users and sensitive data.

Exabeam UBA for Data Loss Prevention

Exabeam brings unique UBA capabilities to data loss prevention, whether or not a third-party DLP product has been deployed. Unlike other UBA vendors, only Exabeam creates a new type of data structure that connects the behavioral dots across all of a user's accounts, devices, and IP addresses, over time. This ***session data structure*** auto-assembles activities and identity signals into sessions, and tracks user activity even when the user changes state, such as switching to an account with elevated privilege, moving from one system to another, etc. The Exabeam system relies on the connection data structure to model user behavior as well as the behavior of the DLP product itself. As a result, the combination provides instant insight into risk while eliminating the noise that often accompanies DLP technologies. Based on customer experience, here are the top eight capabilities that Exabeam brings to data loss prevention.

Automatic Capabilities: The Top Eight

Whether or not a third-party DLP system has been deployed, Exabeam provides eight key functions for preventing data loss and exfiltration. These include:

1. **Flight Risk Monitoring:** One of the biggest concerns with regards to DLP is a terminated employee walking away with sensitive information. Exabeam can monitor for users that save certain filetypes, such as .pst email archives, to a thumbdrive or email. Similarly, users that move abnormally large volumes of data to cloud storage will be flagged. This can be especially useful when combined with Exabeam watchlists. For example, if a division was part of a planned layoff, its employees might be added to a watchlist, with special monitoring for unusual behavior from the people on the list. Adding filetype monitoring to a watchlist provides early detection of sensitive data loss.

2. **USB Port Monitoring:** Many corporate PCs contain endpoint security software that logs the use of thumbdrives in USB ports. Exabeam can use this log data to identify risky operations such as the first time a user saves files to a USB drive, or when a user is copying files as a volume or filesize that is out of that person's normal behavior.

3. **Executive File Access Monitoring:** Exabeam performs automatic monitoring of executive assets and activities, and can determine if specific sets of files are typically only accessed by members of the executive team. If a new user begins accessing these files, Exabeam notes the discrepancy and increases that user's risk score immediately.

4. **Print Job Monitoring:** Unusual print activity is a common sign of potential data loss. Rogue insiders often send sensitive files to printers as a means of avoiding data-in-motion detection. Exabeam can monitor for unusual frequency of print jobs, sending unnamed files to the printers, and other indicators of potential data exfiltration.

5. **Cloud File Monitoring:** If an organization is using cloud security monitoring products, Exabeam uses activity logs from cloud applications to track file movement to/from Box, Dropbox, etc. and compare activities to each user's baselines as well as others in the same department. Exabeam extends its assessment capabilities to the cloud.

Exabeam Plus Third-Party DLP Products

In many instances, an organization has a DLP solution in place, monitoring both data at rest and data in motion. If so, Exabeam provides all of the benefits above, plus:

6. **Auto-classification of Sensitive Assets:** DLP "crawlers" are often used to identify sensitive data at rest, as well as the systems that hold that data. Exabeam can ingest this information to create sensitive asset classes within the data model. This can be used to automatically assign higher risk scores to anomalous accesses to sensitive systems.

7. **Increase DLP Context:** When a DLP system flags an email as containing sensitive data, it may quarantine the email until an analyst determines that it's safe to release it. However, the analyst won't see any other related user operations, and so must make a judgment call with limited information. With Exabeam, the analyst can simply enter in the user's name to instantly see all other activities around the email send. As a result, analysts can make much better calls, more quickly and with less effort.

8. **Reduce DLP False Positives:** Finally, DLP systems deployed at scale can generate quite a lot of "noise," resulting in analysts ignoring alerts altogether. Just as Exabeam can model user behavior to create baselines and prioritize only risky behaviors, it can also model DLP activity to create baselines of normal DLP system behavior. The result is significant improvement in analyst efficiency.

The most fundamental value of user behavior analytics is to provide context around security activity. Done effectively, UBA improves detection of threats and potential loss, enables better prioritization of effort, and supports dramatically faster response after detection. This is especially true when applying UBA to DLP efforts. DLP is prone to false positives and an overwhelming amount of noise, and Exabeam's session data model, called Stateful User Tracking™, can decrease DLP noise and improve the effectiveness of any DLP initiative.

For more information, please contact Exabeam at info@exabeam.com