

WHITE PAPER



# PREVENTING INSIDER THREATS WITH UBA

Insider threats refer to security risks caused by **malicious users** within a corporate network. This type of attack is different from one caused by a compromised credential, where an external hacker has used valid, stolen account credentials to impersonate an employee and access a network. In the case of a malicious insider, the user typically is acting with intent and likely knows that he is breaking policy and potentially the law.

**Insider threats can come from a wide variety of users within the corporate network. These include:**

- Current employees
- Former employees
- Contractors
- Business partners
- Outsourcers
- Suppliers
- Service Providers



In many cases, any of these users might have inappropriate access rights. For example, in many organizations, employees' system access rights are not revoked as the employees change roles. They accumulate rights but rarely lose them. As a result, long-term users may be able to access systems more readily than their current jobs require. In other cases, a termination workflow doesn't complete correctly, and an ex-employee is still able to access sensitive applications or servers remotely. In short, the set of potential malicious insiders tends to be both much larger and also harder to identify than most CIOs imagine.

Moreover, the amount of sensitive data at risk from a malicious insider tends to grow very quickly. Targets include financial reporting data (early access enables illegal trading in a company's stock), customer data (valuable to competitors), product or technical documents (again, valuable to competitors), employee data, and more. These datasets live in multiple places, as they are duplicated for a variety of uses, including backup, compliance, dev/test, and reporting.

**Real-world examples run from the mundane to the extreme:**

- A sales manager copies current customer and pipeline forecasts before joining a competitor
- An engineer decides to launch a startup that competes with his employer, and copies product plans and design docs before leaving
- An IT manager peeks at quarterly earnings data ahead of the reporting date, with the intention of illegally trading his company's stock
- A scientist copies thousands of design and technical documents, to sell to a foreign country (In 2012, a Dow Chemical scientist was imprisoned for five years for doing exactly this)
- An intelligence agency contractor downloads massive amounts of internal program data to leak to the press...

In each of these instances, the user access systems in ways that were unusual or prohibited. In retrospect, each breach seems obvious. For example, in the case of the Dow Chemical scientist, he accessed the secure file server system well over 10x more than the next employee. Detecting risk early is difficult because the signals reside in many places and are challenging to combine.

## Detecting Insider Threat Risk Signals

The signals that point to a malicious insider may live in multiple places, including:

### Detecting At the endpoint

Is this employee copying files onto a local USB key? Has she done so before? Is she copying a different set of files and are they confidential? Is she copying a much larger number of files than she normally does?

### Detecting At the badge readers

Does this contractor normally badge in and out at these times? Has he ever entered this building and server room before? Is he supposed to do so?

### Detecting On the file server

Is this contractor accessing confidential files and copying them locally? How many files is he reading? Is this unusual for him or for others with his title? Has the contractor accessed this server before?

### Detecting At the printer

Is this employee sending unnamed files to the printer (a common data theft trick is to copy sensitive data, paste it into a new, empty Word doc, and print it)? Is she printing files after hours when others aren't around?

### Detecting In the identity management system

Is this user an employee or a contractor? Which department is he in, and what files do his peers access? Are his access rights accurate for his current role?

### Detecting In the cloud

Is this contractor moving files to Box or OneDrive? Are those files sensitive?

### Detecting In the database server

Is this person supposed to be accessing this database? Which tables is she reading?

Each of these are logical areas to inspect for data theft. However, reading activity from all of these, combining it with DLP results, building baselines and then evaluating activity against those baselines in real time requires a level of expertise and horsepower that few systems and no humans have.

## Data Loss Prevention and UBA

A key question in many of the examples above is “is the information sensitive?” This is not always easy to answer, and DLP products are designed to help do so. DLP products scan and assess data, whether at rest or in motion, for sensitivity. As a result, DLP logs can be combined with user behavior analytics to build a very useful confidential-asset model: which systems are potentially risky because they contain sensitive information, who normally access them, and at what rate?

## Exabeam Fits the Pieces Together

So far, we have described the input to an analytics system that identifies all the places where sensitive data resides, who accesses it, where they copy it, and whether that makes sense or is unusual. Tying this all together in real time is essentially impossible for a human analyst; it requires automation and machine learning. Exabeam's UBA platform provides the missing piece. It does this by combining multiple types of asset and identity data with classification data and activity data. For example, Exabeam can automatically model, using DLP, endpoint, and other log data:

- Where sensitive data lives in a corporate network
- Who normally accesses those systems
- How often does each person access, and how much data do they normally access?
- Which data have they touched, copied, or saved locally or through the cloud?
- What is normal and what is unusual?
- If we are seeing something unusual, why is it unusual?
- If someone is doing something unusual, are they slated to be terminated or have they given notice?

## How it Works

Exabeam detects insider threats through a **four-step process**:

### 1. Extract and Enrich

Exabeam begins by ingesting a variety of data, including log data from a SIEM, identity data from Active Directory or LDAP, and other context data such as DLP scan results. The base activity data might contain only minimal identifying information, such as an IP address. This data is automatically enriched with the identity and context information. At this point, Exabeam has the raw fuel for machine learning.

### 3. Behavior Analysis

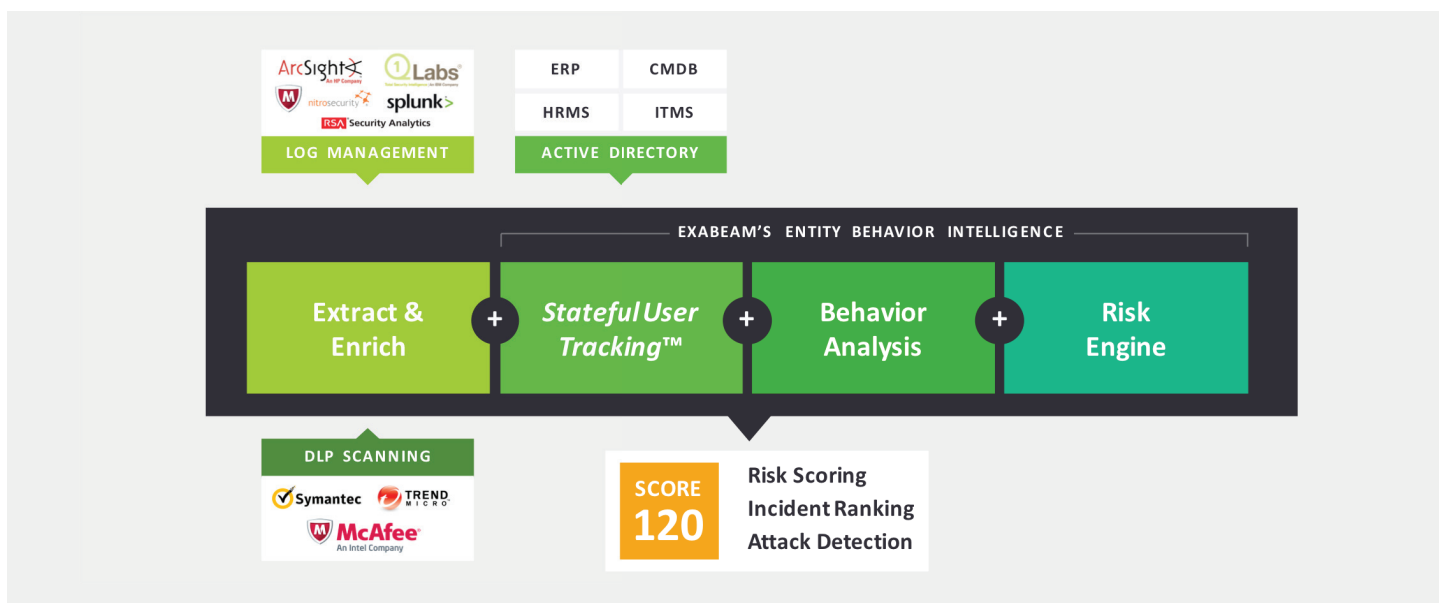
The behavioral engine creates baselines for each user, of normal behavior. This provides useful context for evaluating an insider's activity, i.e. does this person normally access this system or this data? Has the access changed in some way?

### 2. Stateful User Tracking™

This is the process by which Exabeam automatically stitches together all of a user's activity, across multiple accounts and devices, into coherent sessions. The resulting session data ensures that complex attempts to access data are detected, and also provide incident responders with a complete story of an attack.

### 4. Risk Scoring

Finally, the risk scoring process evaluates stateful sessions and activities against a user's baselines, via rules, correlations, and other techniques. The end result is a clear picture of risk, on a per-use basis, of potential data loss from insider threat.



## Data Science Insider Threat Evaluation

Exabeam includes a variety of machine-learning techniques for evaluating insider threats, powered by Stateful User Tracking™ across credentials, IPs, and devices. Common techniques within the Exabeam platform include:

- **Behavioral baselining:** Exabeam creates, on a per-user and per-system basis, baselines of normal behavior. These are used by the risk scoring engine to determine if new activity is anomalous and potentially risky.
- **Peer group analysis:** Exabeam automatically compares each user's behavior and access patterns to those of others with the same role.

- **Privileged account analysis:** Admins typically have elevated access rights, with the potential to access significant amounts of sensitive data. Exabeam includes privileged rights in its analysis of risk.
- **Shared account analysis:** Shared accounts are often a special area of concern for organizations, as they make it difficult to identify the specific user that is performing risky activities. In many cases, an organization might not even be aware of credentials that are being shared. Exabeam can identify shared accounts, attribute activity to specific people using those accounts, and apply customizable risk scoring to these activities.
- **Locked account analysis:** Account lockouts can occur for many reasons, both benign and malicious. For inside threat analysis, Exabeam can identify a user that has attempted to log in to an account for the first time, as well as accounts that might have been tied to a previous job role. Exabeam can identify unusual activity around the lockout, so that SOC analysts can pay special attention to a potential insider breach.

## Common Data Feeds for Exabeam Insider Threat Evaluation

- **Local and Remote Access Logs:** VPN, Domain controller, and Wifi access point logs can provide strong signals of risky activity.
- **Identity Services:** Active directory, LDAP, PeopleSoft and other services provide useful information regarding location, roles, peers, etc.
- **DLP Scans:** DLP products, such as Symantec Vontu, use a variety of methods to identify confidential data residing in systems and flowing through the network.
- **Endpoint Feeds:** PC/laptop security solutions such as Bit9+Carbon Black provide useful context around user file activity as well as system configuration.
- **Network Feeds:** While netflow data provides weaker behavioral signals, it can augment data coming from SIEM and endpoint solutions.
- **Database Activity:** Pulled either from the database logs directly, or via database firewalls such as Imperva, database activity can provide useful insight into sensitive table access.
- **Application Activity:** Application activity includes both access-related logs, as well as functional activity, where available.
- **Cloud Activity:** Most organizations have integrated cloud services into their architectures, and Exabeam can either pull directly from services (e.g. Salesforce.com ELF), or from CASB solutions (e.g. Skyhigh Networks).
- **USB Thumbdrive Access:** Local file copy, usually to a thumb drive, can provide significant signals, particularly when combined with DLP file scan verdicts.
- **Print Servers:** Malicious insiders may print out tables as a means of avoiding other scanning techniques.
- **Physical Security:** Badge readers can provide context regarding entry and exit times, as well as entry into new buildings or server rooms.

Exabeam has integrated all of these feeds, and more, at customer sites.



## Automating Response

When Exabeam has identified the number of users that are acting unusually, it can take any number of actions, ranging from the most passive (notify a security analyst), to informational (send an email to an employee reminding them of their confidentiality duties) to the extreme (lock down access and instigate a response). Exabeam can integrate via scripting with any workflow or security solutions in place, thereby bringing advanced intelligence and context to enterprise security and compliance programs.

## Additional Behavioral Scenarios

While insider threat is a top concern for many CISOs, Exabeam UBA can support a wide variety of security use cases. These include:

- Compromised credential (i.e. user impersonation) detection
- Dormant account detection
- Shared account usage
- Executive asset access
- Security alert investigation
- Breach investigation
- Red Team support
- And many others

**For more information**, please download the paper “UBA for Data Loss Prevention” from the Exabeam website, or send an email to [info@exabeam.com](mailto:info@exabeam.com).