

Global Fashion House Implements Teramind UAM to Protect its IP From Falling into the Wrong Hands

“In the creative industry, it's easier to safeguard your IP than defending it in the court. Teramind helped us protect our IPs and trade secrets from being exfiltrated by insiders reducing the risk of competitors access to our products and the legal expense of having to defend a copyright case.”

Senior Executive



Business Challenges

Company has faced challenges in some key areas of its core business:

- ✓ IP is difficult to protect if a design is leaked on the public domain before it's copyrighted as competitors can change it subtly and claim first-to-file trademarks.
- ✓ In the current digital age, it's very easy for employees or suppliers to leak product ideas and designs by mistake or intentionally.
- ✓ In the EU, the Company sometimes uses unregistered community design (UCD) to save time and cost. However, they have less protection than the registered versions, so needed to be guarded even more closely.

Success Factors

Company needed a solution that could constantly monitor employees and third parties who came in contact of its designs during the creative process, manage who gets access to what information and finally have accurate evidence to support any copyright claims.

Company Profile

A privately held, globally recognized high fashion house that specializes in haute couture, ready-to-wear clothes and designer accessories.



Solution

Monitoring and Prevention of Risky User Activity Automatically :

- ✔ Monitor suspicious behavior like frequent late shifts, printing a large batch of documents, or copying large amount of files to the USB drives.
- ✔ Monitor upload and download of information on cloud storages like Google Drive, Box, Dropbox etc.
- ✔ Check attachments in emails or IMs for confidential documents.
- ✔ Prevent copy/paste from design applications to other applications or websites.
- ✔ Get a copy of all files sent to the printers.
- ✔ Hundreds of other rules monitoring user interactions with 12+ objects like files, websites, applications, emails even keystrokes.

Teramind UAM

Privacy Friendly User Activity / Employee Monitoring

Teramind's UAM/User Behavior Analytics (UBA/UEBA) solution comes with everything essential you will need for employee monitoring, third-party monitoring, insider threat detection and workplace productivity optimization use cases.



Solution

Limit Exposure of IP Related Information:

- ✔ OCR, fingerprinting and tagging to identify sensitive images and documents and restrict their usage.
- ✔ Limit access to the rendering machine or where design files are stored.
- ✔ Segregate access on a need to know basis. i.e. what the design department can see vs. the marketing department.

Live View and Session Recording:

- ✔ Live view and recording of all user activities, session logs and forensic trails to pinpoint the exact source, time and user for any data breach incident.

Employee Education and Training:

- ✔ Train employees why IP should be protected and how to safeguard against mistakes with custom etiquette policies and rule violation messages.

About Teramind

Teramind is a leading, global provider of employee and user activity monitoring, workforce productivity optimization, user behavior analytics, insider threat detection, forensics and data loss prevention solutions.

Over 2,000 organizations in finance, retail, manufacturing, energy, technology, healthcare and government verticals across the globe trust Teramind's award-winning platform.



Result

Company was able to see improvements in the following areas:

- ✔ Was able to identify and stop several data exfiltration attempts by insiders.
- ✔ Reduced legal defense cost by stopping IP leaks from happening in the first place.
- ✔ Additionally, utilized Teramind's Workforce Productivity features to gain visibility into how employees spent their time and then develop processes to increase their performance.

hello@teramind.co

Live dashboard demo