

iTrent Shield

User Behaviour Analytics
(UBA)



Would you know if one of your employee's iTrent accounts was being used by a malicious actor, or if one of your employees was stealing data?

iTrent Shield User Behaviour Analytics (UBA) has been developed to provide you with an increased level of security to protect you from these threats.

iTrent Shield UBA gives you the ability to identify suspicious behaviour and stop it before it impacts your organisation.

How iTrent Shield UBA provides extra protection:

In a first for HR and payroll companies, our software will monitor user activity to detect:

- User accounts that have been compromised by a malicious external actor (e.g. through phishing)
- Rogue employees that are undertaking fraudulent actions

How iTrent Shield UBA works:

A proprietary, AI-powered algorithm is used to learn the normal pattern of activity for each user. When a user's behaviour significantly deviates from their norm, such as viewing significantly more personal data, or they undertake one-off suspicious actions, such as deleting audit records, an e-alert is generated advising you that the user's actions should be investigated.

How iTrent Shield UBA can help your organisation:

- Reduces the risk of sensitive data being stolen or employee salary payments being diverted
- Provides greater assurance over the security of staff working remotely
- Allows organisation to meet higher internal or regulatory compliance requirements

If you're interested in this solution, please contact your Customer Relationship Manager for more information.

+44 (0) 115 945 6000
info@mhrglobal.com
mhrglobal.com