Account Takeover Protection

https://campus.barracuda.com/doc/81395763/

Account takeovers are a major threat to business data. Barracuda can detect suspicious sign ins to Microsoft 365 accounts that may indicate account takeover. If detected, Barracuda will alert the IT administrators.

> For important information about suspicious sign-in data and your environment, refer to Getting Started.

Barracuda is able to detect suspicious sign ins by:

- Tracking IPs that exhibit suspicious behavior across our customer base. In other words, Barracuda tracks failed sign ins on multiple account that belong to different customers, and shares this intelligence across accounts and alerts IT administrators when there is a successful sign in.
- Tracking each user’s access patterns and alert IT administrators when Impersonation Protection observes unusual sign-in activity from an unusual device or geography. Impersonation Protection tracks both user-level pattern and organization wide level patterns.

In this section: