Adaptive Protection in Microsoft Purview Data Loss Prevention (DLP) is a dynamic, intelligence-based feature that automatically adjusts the enforcement level of DLP policies based on user risk levels—making your data protection more targeted and efficient.

What It Does:
Instead of applying the same DLP rules to all users, Adaptive Protection tailors enforcement based on how risky a user's behavior is, as determined by Insider Risk Management.

- High-risk users (for example, those downloading large volumes of files or showing signs of data exfiltration) can be automatically subjected to stricter DLP controls such as blocking file sharing or uploads.
- Low-risk users continue to work under less restrictive DLP rules, maintaining normal productivity.

How It Works:

1. Insider Risk Management continuously monitors user behavior across Microsoft 365, including email, file access, Teams activity, and more.
2. Users are assigned risk levels—Low, Medium, or High—based on detected activity.
3. DLP policies configured for Adaptive Protection apply different actions depending on a user's current risk level.
4. As risk levels change, DLP enforcement automatically adjusts in near real-time.

Example:
A marketing employee attempts to upload a confidential client list to their personal Google Drive. Insider Risk Management flags this as suspicious and increases the user's risk level to High. As a result, the Adaptive Protection-enabled DLP policy immediately blocks the sharing attempt and alerts compliance officers. For a Low-risk user, the same action might have only triggered a warning or audit log.

Benefits:

- Enables proactive protection based on risk
- Reduces false positives for low-risk users
- Decreases alert fatigue by focusing on high-risk activity
- Automatically scales protection based on behavior patterns

Data Loss Prevention Policies for Adaptive Protection