# Microsoft Security

Enable Adaptive Protection with Microsoft Purview

People-centric data protection for today's dynamic work environment

Data security risk is dynamic in today's modern workplace with various constantly changing factors, including types of content, people who interact with data, and the activities around the data, all of which make it more complex to manage. As 83% of organizations have had more than one data breach[1], the recurrence of data security incidents is rising and has become a critical vulnerability that organizations must prioritize. Meanwhile, a recent Microsoft study shows that 2 in 5 security leaders feel at extreme risk due to cybersecurity staff shortage[2]. How can organization effectively protect data with limited resources?

Optimize data protection automatically
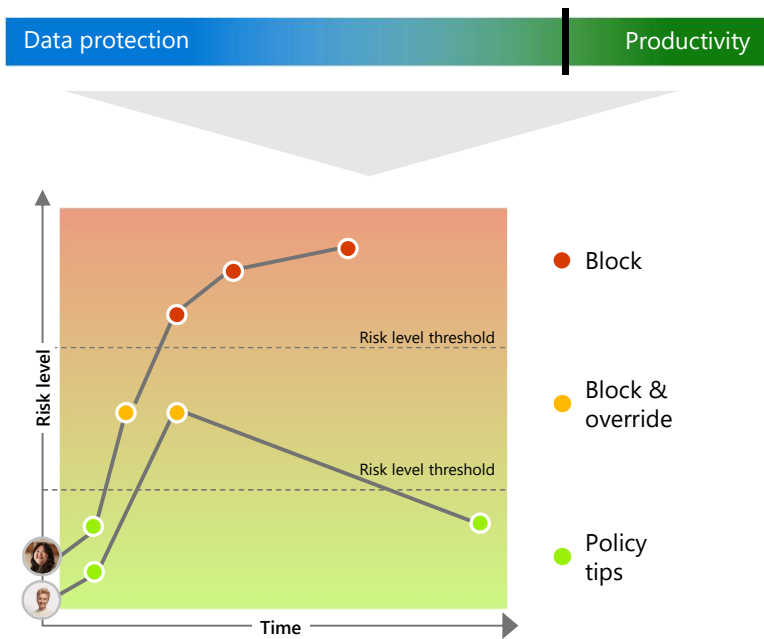
Often, attempting to find the sweet spot between data protection and productivity takes much of the security team's bandwidth. If a control is too strict, it could overload the security teams with an overwhelming number of alerts and block legitimate business activities. Most security teams may prefer a less restrictive control since it doesn't impede productivity, but the risk of data loss would increase.

What's needed is a more adaptive solution to help organizations address **the most critical risks dynamically**, **efficiently prioritizing** their limited security resources on the highest risks and minimizing the impact of potential data security incidents.
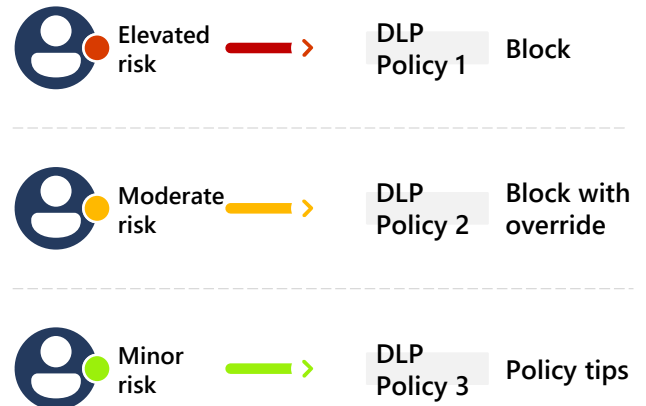
Adaptive Protection in Microsoft Purview is the solution.

Since risk is dynamic, your data protection solutions should adapt accordingly

Adaptive Protection **dynamically assigns appropriate Data Loss Prevention policies to users based on the risk levels analyzed by the machine learning models in Insider Risk Management**.

- **Context-aware detection**: Identify the most critical risks with built-in ML-driven analysis in Insider Risk Management
- **Dynamic controls:** Enforce effective DLP controls on high-risk users while others maintain productivity
- **Automated mitigation:** Minimize the impact of potential data security incidents and reduce admin overhead

The result: your security operations team is now **more efficient and empowered to do more with less**.

Elevated risk	DLP Policy 1	Block
Moderate risk	DLP Policy 2	Block with override
Minor risk	DLP Policy 3	Policy tips

Ensure better data security with an adaptive approach enabled by machine learning

Contact us to schedule a demo of Adaptive Protection in Microsoft Purview

Microsoft

1. Cost of a Data Breach Report 2022, IBM
2. "Cyber Resilience". May 2021, Microsoft Security Insider