MOLAPRISE

# The 6 most overlooked Microsoft 365 security gaps

Why secure by default is only a starting point

## “Security in M365 isn’t what you buy, it’s what you actively operate.”

### Identity Layer

If MFA is not consistently enforced and too many users hold elevated roles, one weak point can become tenant-wide exposure

### Authentication Layer

Legacy protocols do not support modern controls the way modern auth does, which means they can undermine MFA and access policies

### Access Layer

Use policies to enforce MFA, block risky sign-ins, require compliant devices, and shape session behavior

### Detection & Response

Risk signals are only useful when they trigger action such as MFA challenge, block, or password reset

### Collaboration and data

Guest access, spoofing protection, and phishing controls need tuning. Audit logging, DLP, device management, and mailbox controls add another layer when ignored

## Secure by default is useful, not sufficient

Default protections help, but they do not reflect your business, users, devices, or risk appetite

Review what is configured, not just what is licensed

Most gaps are operational, not theoretical

Start with a focused review of what is enabled, enforced, and monitored

**Read the full article**