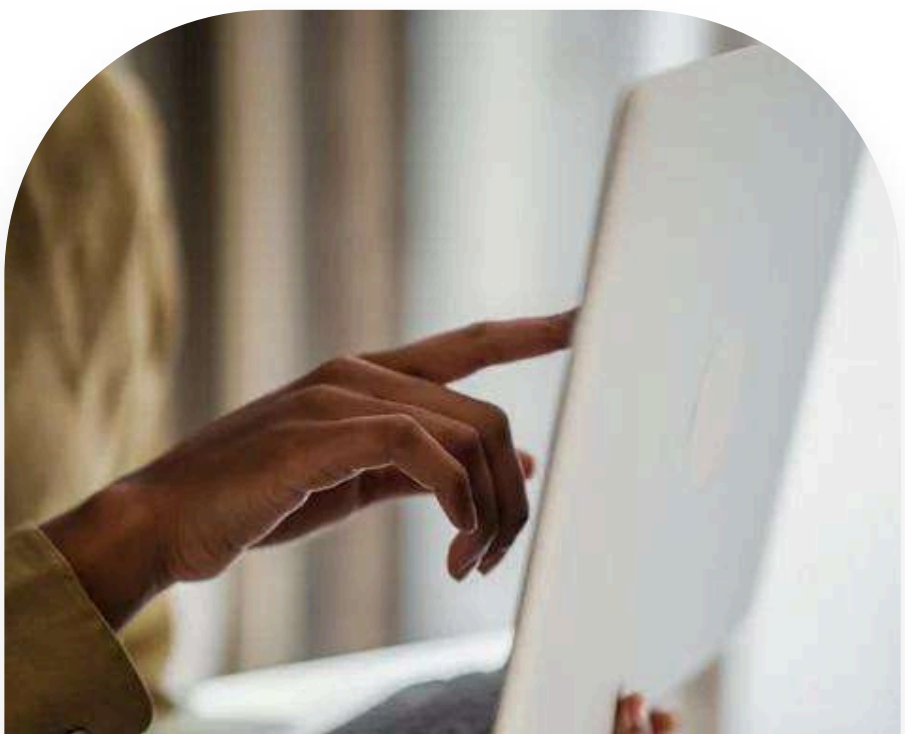
4

Defenses Against Cloud-Based Malware

1. Strengthen Access Controls

A great first step is tightening who can log into your cloud. Using multi-factor authentication (MFA) ensures that only authorized users get access. This might mean requiring a code sent to a phone or email in addition to a password.



2. Encrypt Your Data

Encryption keeps your data unreadable to outsiders. You'll want to encrypt both stored files and data being transferred across networks. Most cloud providers offer built-in encryption tools. AWS Key Management Service (KMS) or Azure Disk Encryption are good places to start.

3. Implement Real-Time Monitoring

Monitor your cloud activity with tools like AWS CloudTrail or Microsoft 365 Security to detect threats early. Unfamiliar logins or unexpected data changes could signal a breach. Act quickly by blocking access or resetting passwords to protect your system.

4. Educate Your Team

Employees are key to cloud security. Regular training on spotting phishing attempts and suspicious links strengthens your defenses. Simulated attacks can test and enhance their awareness, ensuring your team is well-prepared to protect your cloud environment.