

# AIRWATCH

With AirWatch's mobile application management (MAM) capabilities, administrators can distribute, secure, and track mobile applications directly from the AirWatch Admin console, which can be integrated into your mobile environment.

The AirWatch platform allows you to add an additional level of security by setting restrictions within the security profile.

- ▲ You can enable Data Loss Prevention to protect sensitive data in applications. This setting controls copying and pasting, printing, taking pictures and screen captures, using Bluetooth, and other actions that involve the transmission of data.
- ▲ When you do not enable Data Loss Prevention, you can perform almost every out-of-the-box MicroStrategy Mobile data transfer.

## Capabilities and benefits

### PROVISIONING AND AUTHENTICATION

Adds an additional EMM-specific authentication, e.g. PIN with configurable security settings. This is in addition to the authentication required by the MicroStrategy application.

### DATA LEAKAGE PREVENTION

Controls to govern whether data can be transmitted, shared, or copied outside of the application ecosystem.

### APPLICATION ECOSYSTEM

Allows data to be transmitted to other applications in the EMM ecosystem (i.e. other applications that are integrated with the EMM SDK) in a secure manner.

### TUNNELING

Uses a secure channel or gateway provided by the EMM platform to transmit data from client to server.

### DATA ENCRYPTION

Ensures that all persisted data are automatically encrypted on the device.