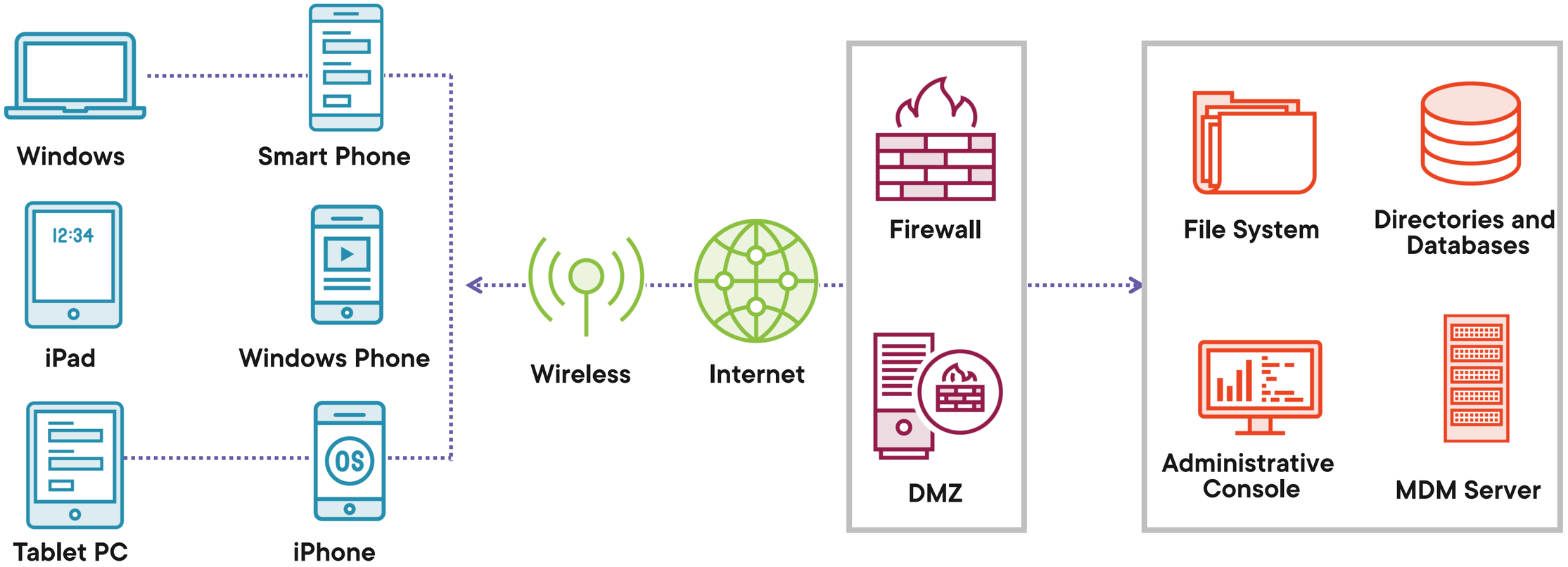
Outlining Mobile Device Management (MDM)

Dale Meredith
MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

dalemeredith.com | Twitter: @dalemeredith | Linkedin: dalemeredith



MDM Software Solutions

IBM MaaS360

System Center Configuration Manager

Miradore

MDM Software Features

- Uses a passcode
- Remotely locks device
- Remotely wipes data
- Detects if device is rooted or jailbroken
- Enforces policies and tracks inventory
- Performs real-time monitoring and reporting

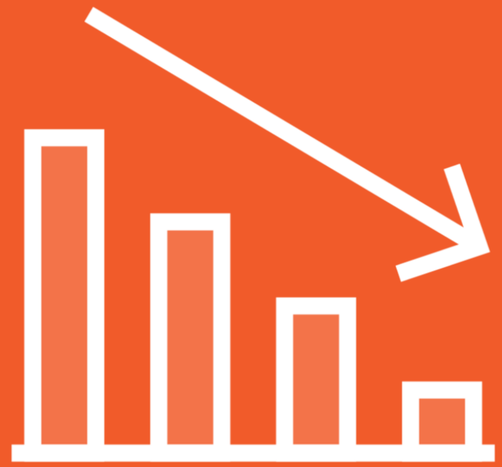
BYOD (Bring Your Own Device)

Benefits of BYOD

Increased productivity

Employee satisfaction

Work flexibility



Lower cost

BYOD Risks

- Sharing and storing confidential data on unsecured networks
- Data leakage and endpoint security issues
- Improperly disposing of devices
- Devices have limited security
- Combining personal and company data creates risk
- Create infrastructure issues
- Disgruntled employees

Implementing a BYOD Policy

Key Principles

Define company requirements

Identify approved devices

Develop policies

Keep the mobile ecosystem secure

Determine support

BYOD End-user Guidelines

- Use encryption mechanisms to store data
- Maintain a clear separation between business and personal data
- Register devices with a remote locate and wipe facility if the company policy permits
- Regularly update one's device with latest OS and patches
- Use anti-virus and data loss prevention (DLP) solutions

BYOD End-user Guidelines

- Set a strong passcode for the device and change it often
- Use strong algorithms to encrypt data
- Set passwords for apps to restrict others from accessing them
- Do not download files from untrusted sources
- Be cautious while browsing websites and opening links or attachments sent via email

BYOD Administrator Guidelines

- Secure data centers with multi-layered protection systems
- Educate and train employees on BYOD policies
- Clearly define ownership of apps and data
- Transfer data over encrypted channels
- Manage access
- Disallow rooted or jailbroken devices
- Apply session authentication and timeout policies

Demo

Miradore

Learning Check

Learning Check

- Data leakage
- Sharing confidential data
- Clearly define ownership of apps and data
- Apply session authentication and timeout policies

Up Next:
Pointing Out Security Guidelines