

MOBILE DEVICE MANAGEMENT & BYOD SECURITY.



A personal phone with corporate email on it is corporate attack surface — MDM decides whether that surface is managed or invisible.

- MOBILE DEVICE MANAGEMENT (MDM)
- BYOD CONTAINERIZATION
- CONDITIONAL ACCESS
- REMOTE WIPE & COMPLIANCE

01 THE MECHANISM

Mobile Device Management (MDM)
Enforcing **device-level policy**, **encryption**, and **compliance** across managed endpoints.

Containerization
Separating **corporate data** from **personal apps** on the same physical device.

Conditional Access
Blocking access to corporate resources **from devices that fail a compliance check**.

02 THE FLOW

The Managed Device Lifecycle ENROLLED

1

A device is enrolled and a **compliance policy** is pushed automatically.

2

Corporate data stays inside an **encrypted, managed container** on the device.

3

A lost or compromised device is **remotely wiped without touching personal data**.

The Unmanaged Shadow Device LIVE EVENT

1

An employee's personal phone syncs **corporate email** with **no policy enforced**.

2

The device is lost, sold, or compromised **with corporate data still on it**.

3

There's no wipe capability and **no way to prove the data was ever contained**.

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Mobile Device Management (MDM)	Enforces encryption, passcodes, and compliance policy on managed devices.
BYOD Containerization	Isolates corporate data and apps from personal use on the same device.
Conditional Access	Grants resource access only to devices that meet compliance requirements.
Remote Wipe & Compliance	Enables selective or full data removal when a device is lost or non-compliant.

04 MOBILE SECURITY APPROACHES COMPARED

SIGNAL	SUFFICIENT ALONE?	WHAT IT MISSES
No Mobile Policy At All	No	Corporate data on personal devices with zero visibility or control.
BYOD Without Containerization	No	Corporate and personal data mixed with no separation boundary.
MDM Without Conditional Access	No	Compliant devices are enrolled, but non-compliant ones still connect.
Manual Device Approval Only	No	Doesn't scale and misses devices added outside the process.
MDM + Containerization + Conditional Access	Yes	Separates data, enforces compliance, and blocks access from non-compliant devices.

MOBILE DEVICE MANAGEMENT.

ENROLL · CONTAIN · WIPE

05 PROGRAM OPERATIONS

BYOD isn't a security exception — it's a managed policy surface. Personal ownership doesn't remove the corporate data risk.

Remote wipe only works if enrollment happened first. Unmanaged devices can't be selectively wiped.

Containerization removes the false choice between privacy and control. Personal apps stay untouched while corporate data stays protected.

Compliance policy has to travel with the data, not the device owner. Ownership shouldn't determine whether corporate data is protected.

06 CONTROL MAPPING

NIST SP 800-124

Mobile security guidelines defining considerations for managing and securing mobile devices.

CIS MOBILE COMPANION GUIDE

Mobile hardening baseline providing configuration benchmarks for mobile devices.

OWASP MASVS

Mobile app security standard defining verification requirements for mobile applications.

GDPR / STATE PRIVACY LAWS

Personal-device data boundaries governing how corporate data must be separated.

07 WHAT THIS DOES NOT SOLVE

Jailbroken or rooted devices

Containerization can be bypassed on a device with compromised OS-level controls.

Personal app risk

MDM doesn't vet every personal app installed alongside the managed container.

Offboarding lag

A wipe command only works if it's triggered before the device goes offline.

Network-level trust

A compliant device on an untrusted network still needs additional controls.

08 MYTHS VS. REALITY

MYTH	REALITY
"If it's their personal phone, it's not our security problem."	Corporate data on the device is still the organization's liability.
MYTH	REALITY
"MDM means we control the whole device."	Containerization limits control to the work container, not personal data.
MYTH	REALITY
"Employees will use their phone for work anyway."	Without policy, that use happens with zero visibility or control.
MYTH	REALITY
"A strong password is enough mobile security."	An unencrypted device still exposes data once it's lost, password or not.
MYTH	REALITY
"One MDM enrollment covers the device forever."	Compliance status needs continuous revalidation, not a one-time check.

09 SPEAK THE PROGRAM — KEY TERMS

MDM

Mobile Device Management — centralized enforcement of security policy on mobile endpoints.

BYOD

Bring Your Own Device — a policy allowing personal devices to access corporate resources.

CONTAINERIZATION

Isolating corporate apps and data from personal use on the same device.

UEM

Unified Endpoint Management — managing mobile, desktop, and IoT devices from one platform.

CONDITIONAL ACCESS

Granting resource access only when a device meets defined compliance criteria.

SELECTIVE WIPE

Removing only corporate data and apps, leaving personal content untouched.