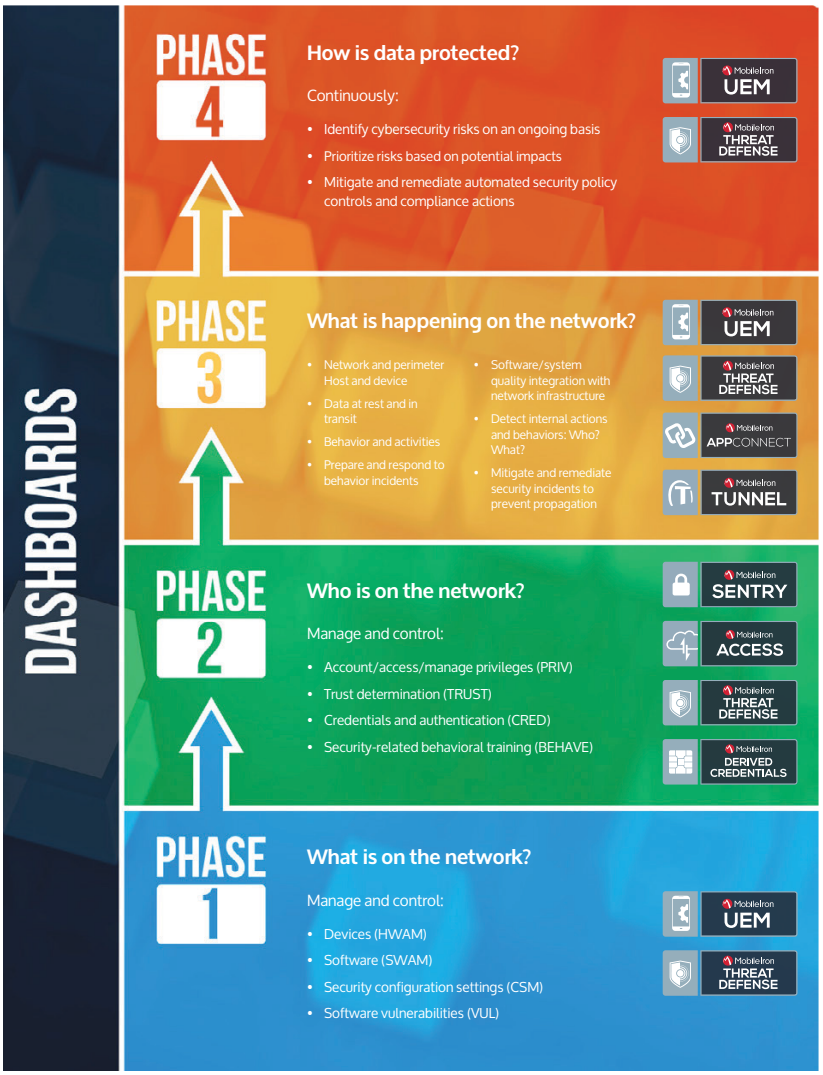
MobileIron supports all phases of CDM compliance

Today, many U.S. government agencies are realizing the benefits of modern work by taking advantage of a broad range of mobile devices, apps, and cloud services. However, the promise of productivity gains and increased employee satisfaction must not overshadow the requirement to maintain government-grade security to protect against data loss. Federal agencies also have to ensure compliance with regulations such as continuous diagnostics and mitigation (CDM) established by the Department of Homeland Security (DHS). While maintaining CDM compliance can be challenging, MobileIron's comprehensive security platform makes it easier than ever before.



Key capabilities

- Provision a trusted workspace
- Protect government data and user privacy
- Block untrusted endpoints and apps
- Detect and mitigate threats on-device

Benefits

- Proven, government-grade security architecture
- Smart and simple to use
- Easy and insightful
- 100% user adoption
- Superior support

Federal security standards and certifications

- CSA STAR
- CSfC
- DISA STIG
- EU-US Privacy Shield
- FedRAMP Authority to Operate
- FIPS 140-2 Affirmation
- NIAP Common Criteria Certification

About MobileIron

MobileIron provides the secure foundation for modern work to companies of all sizes around the world. For more information, please visit www.mobileiron.com

Mapping MobileIron capabilities to CDM phases

Phase 1
What is on the network?

Use MobileIron unified endpoint management (UEM) to define and push security policies and configurations such as email, Wi-Fi, and VPN. Flag non-compliant devices as compromised and log detected violations.

Track and manage OS and app versions, security patch information, encryption status, device location, and more for mobile devices. This information is exportable to external dashboards.

Determine which mobile applications, networks, and users are connecting to the federal network and cloud services. This information is exportable to external dashboards.

Protect against device, network, and app vulnerabilities. Determine the security posture of the network to which a device is connecting. If non-compliant, the device can self-mitigate by blocking enterprise apps and VPN access, disabling Wi-Fi, etc. This information is exportable to external dashboards.

Phase 2
Who is on the network?

A secure gateway determines who is connecting to a federal network or cloud services. It provides conditional access to services based on device security posture, app security, and user access control.

Use SSO capabilities such as CBA, SAML, or derived credentials authentication to ensure only trusted users are connecting to the network.

Automatically deploy threat defense on 100% of users' mobile devices to ensure immediate adoption and compliance. Continuously analyze the integrity of devices that connect to the network. Ensure devices and connections have not been compromised. Mitigate detected threats locally on the device.

Extend security provided by personal identity verification (PIV) cards to mobile devices. This enables use of mobile devices for purposes of SSO and identification and authentication of users to federal networks, applications, and cloud services.

Phase 3
What is happening on the network?

Data protection is provided via managed applications, DLP controls, and containerization.

Data at rest is encrypted via a FIPS 140-2 validated secure mobile app container.

Data in transit is encrypted via a FIPS 140-2 validated secure tunnel for mobile devices and apps connecting to the federal network.

Continuously diagnose device, network, and application attacks on mobile devices connecting to the federal network, and mitigate threats on devices via compliance rules. Mobile threat detection and mitigation is built into the UEM client for easy, 100% user adoption and immediate compliance.

All device, network, and application attacks, risks, and vulnerabilities detected on mobile endpoints are stored and made visible through the intuitive console. This makes it easier to view, mitigate, and remediate security incidents. This information is exportable to external dashboards.

Phase 4
How is data protected?

Federal data is protected by the continuous identification of mobile cybersecurity risks and vulnerabilities. Admins can prioritize risks based on potential impacts and remediate the risks immediately on the device. LIkewise, the CDM analytical dashboard now provides immediate situational awareness of all known and potentially unknown zero-day attacks. It also automatically mitigates vulnerabilities and reduces the risk of lost productivity because admins can remotely bring the device back into compliance, with no manual intervention necessary.

Generate detailed and short summary reports from the threat defense console.

Remotely wipe data at rest from retired or compromised devices while ensuring all mobile devices have the latest OS and security versions and updated mobile applications settings.

Disable access to federal email, VPN, and Wi-Fi when mobile security risks are detected. Provide the end user with automated mitigation actions and remediation guidance.

Revoke access to non-compliant mobile devices. Immediately report any continued risks or attacks to the device, federal assets, or data, whether it resides in the cloud or back-end federal enterprise infrastructure data centers.

Enforce a graduated set of compliance actions on the device with automated actions and end-user notifications delivered over a period of time.