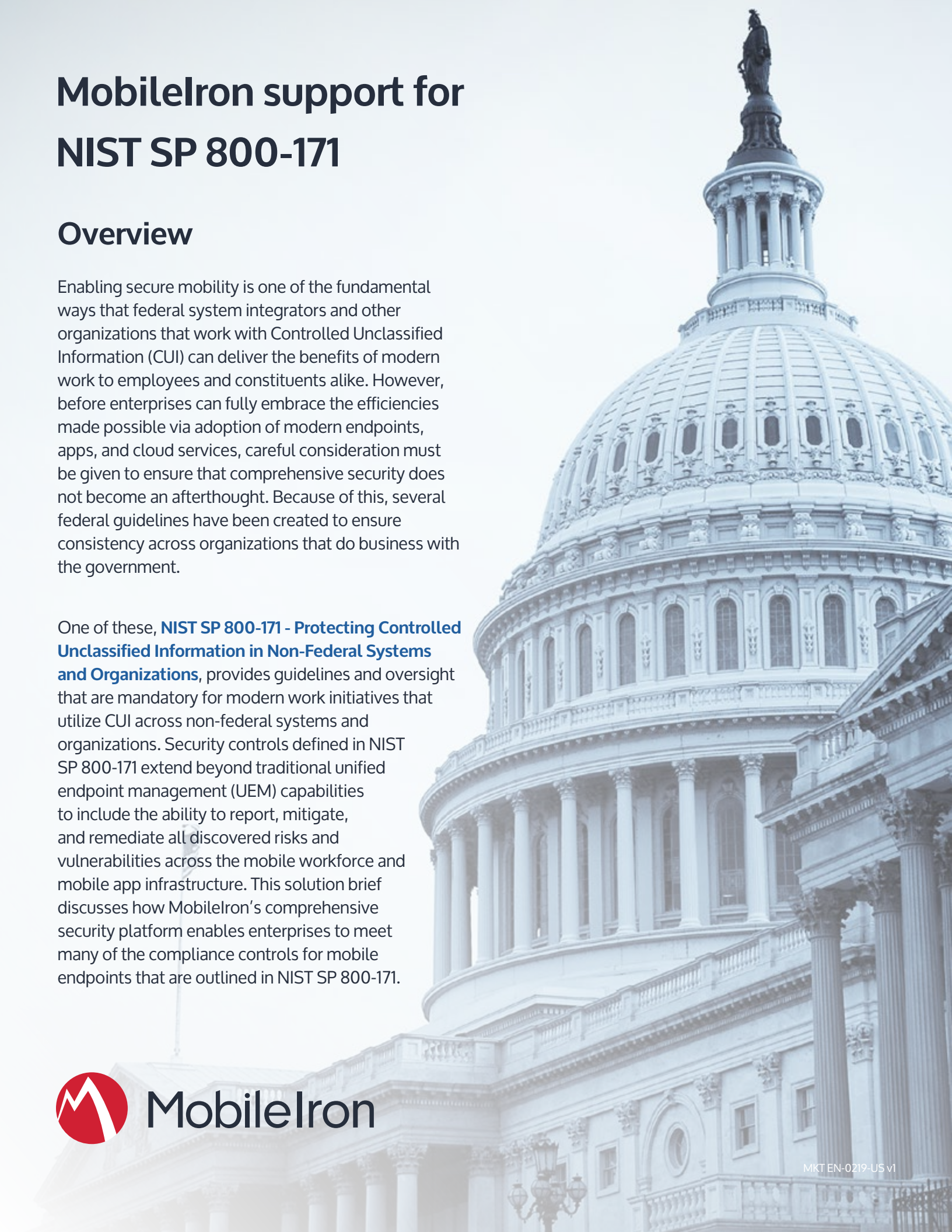
MobileIron support for NIST SP 800-171

Overview

Enabling secure mobility is one of the fundamental ways that federal system integrators and other organizations that work with Controlled Unclassified Information (CUI) can deliver the benefits of modern work to employees and constituents alike. However, before enterprises can fully embrace the efficiencies made possible via adoption of modern endpoints, apps, and cloud services, careful consideration must be given to ensure that comprehensive security does not become an afterthought. Because of this, several federal guidelines have been created to ensure consistency across organizations that do business with the government.

One of these, **NIST SP 800-171 - Protecting Controlled Unclassified Information in Non-Federal Systems and Organizations**, provides guidelines and oversight that are mandatory for modern work initiatives that utilize CUI across non-federal systems and organizations. Security controls defined in NIST SP 800-171 extend beyond traditional unified endpoint management (UEM) capabilities to include the ability to report, mitigate, and remediate all discovered risks and vulnerabilities across the mobile workforce and mobile app infrastructure. This solution brief discusses how MobileIron's comprehensive security platform enables enterprises to meet many of the compliance controls for mobile endpoints that are outlined in NIST SP 800-171.



MobileIron

MKT EN-0219-US v1

NIST SP 800-171 control families supported by MobileIron

There are 110 controls grouped into 14 control families in the NIST SP 800-171 special publication. MobileIron provides endpoint security for all of the control families highlighted in green.

- Access Control
- Awareness & Training
- Identification & Authentication
- Incident Response
- Personnel Security
- Physical & Environmental Protection
- Audit & Accountability
- Configuration Management
- Maintenance
- Media Protection
- Risk Assessment
- Security Assessment
- System & Communications Protection
- System & Information Integrity

Additional security standards and compliance certifications

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

Learn more about MobileIron's security standards and certifications here:
https://www.mobileiron.com/en/certifications-and-uptime

How MobileIron provides support for NIST SP 800-171

See what's on the network

- MobileIron provides the level of control necessary to ensure that only authorized, compliant endpoints can access resources and CUI made available on government networks.
- By leveraging the MobileIron trusted workspace, admins can define and enforce granular compliance policies, manage and distribute only those apps that have been fully vetted and approved and enable access control and multifactor authentication (MFA).
- MobileIron can detect and remediate known and zero-day threats on mobile devices, even without Internet connectivity, to reduce data loss without disrupting user productivity.

Know who is on the network

- MobileIron extends the same level of security provided by personal identity verification (PIV) cards to mobile devices to identify and authenticate users to federal networks and applications. MobileIron also provides an inline gateway that manages, encrypts, and secures traffic between mobile devices and back-end government systems.
- Secure, conditional access control for cloud services such as Microsoft Office 365, G Suite, Box, Dropbox and others is provided.
- Threat defense is automatically deployed to all devices for 100% user adoption and immediate compliance without users needing to download or activate the app, and they cannot remove it. Admins can continuously analyze the integrity of managed devices to ensure vulnerabilities at the device, network, and app level. If a threat is detected, the solution can mitigate it locally on the mobile device.

Understand what is happening on the network

- MobileIron's comprehensive security platform offers enterprises in-depth, multilayered protection against the latest known and unknown mobile threats, risks, and vulnerabilities. The MobileIron UEM trusted workspace (secure container) on mobile devices secures and encrypts all data at rest and in transit, and leverages FIPS 140-2 validated crypto libraries. Users can securely leverage email (S/MIME) and MobileIron's productivity suites like Docs@Work and Web@Work. Admins can remotely configure, deploy, and update compliance policies as well as manage the lifecycle and security of mobile applications with no user intervention required. MobileIron's integrated mobile threat defense and continuous diagnostics and mitigation (CDM) capabilities also work with Samsung Knox and the latest Android Enterprise administrative policy and privacy controls.

- MobileIron provides granular, per-app VPN session security to connect each managed application to the federal network along with various configurations and support for traditional VPNs and the Trusted Internet Connections (TIC). This ensures all federal content and data is continuously encrypted and protected against attacks and ensures mitigation from zero-day attacks. One-touch enrollment and our ability to support enterprise-class PIV-D derived credentials for SSO and MFA provides the best possible user experience with the strongest cybersecurity. Enforced analytics and adaptive risk-based policies account for the type of endpoint, app, network, user, location, and more.

- Mobile threat defense can be automatically deployed on corporate or employee owned mobile devices through MobileIron's unique UEM platform. Our integrated pane of glass with a Splunk forwarder built into our administrative console provides real-time analytics and intelligence that detects all threats and attacks on mobile endpoints. Admins quickly gain visibility into device, operating system, network, and mobile application risks and vulnerability scores. Machine learning algorithms and behavior-based methodologies detect mobile threats, and actionable intelligence provided by the apps analytics engine quickly mitigates and remediates all mobile threats, risks, and vulnerabilities. Admins can limit exposure to possible exploitations by stopping and remediating attacks before they infiltrate the device. Our automated tiered compliance actions provide alerts about risky behaviors, proactively shut down attacks on the device, isolate compromised devices from the network, and remove malicious apps and their content.

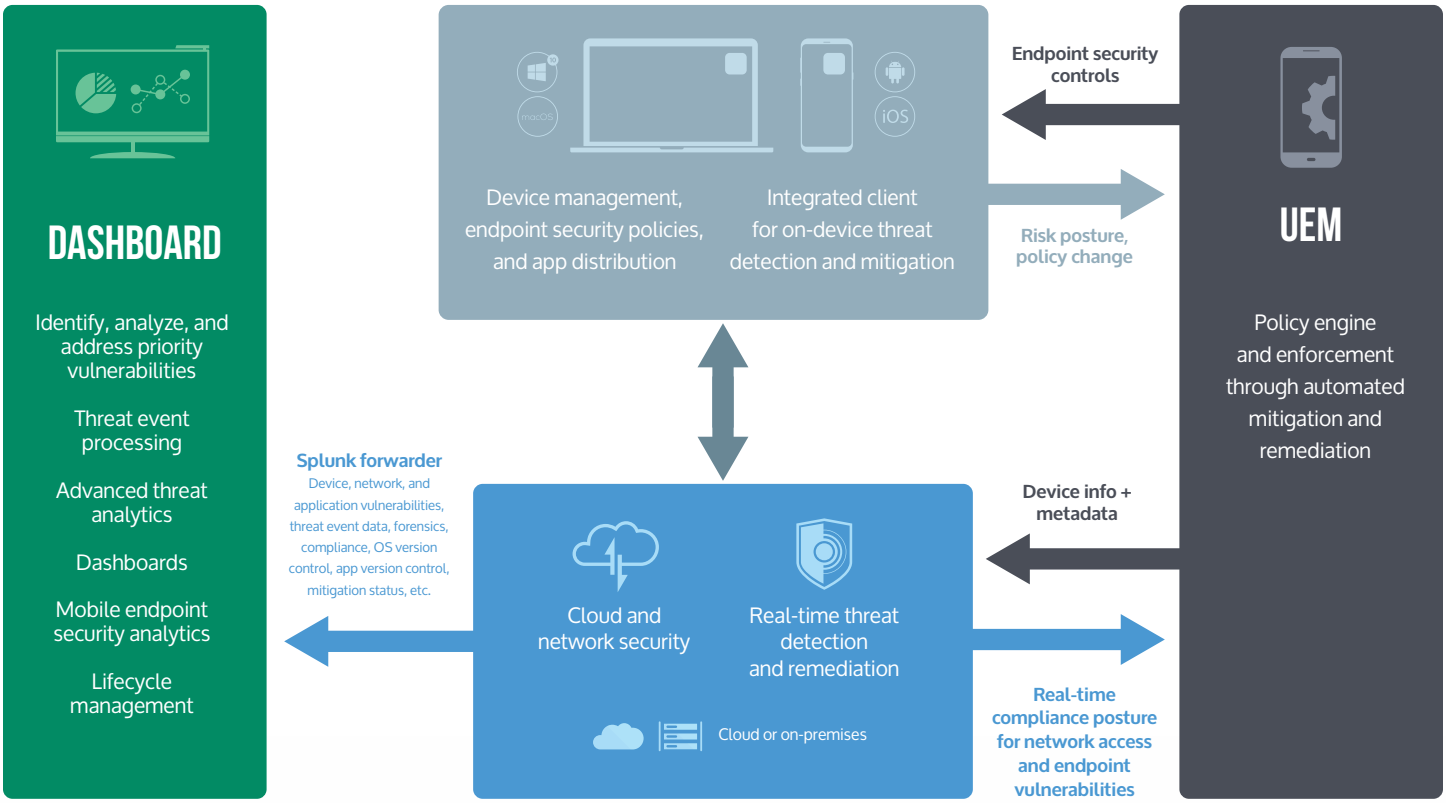
Protect data across multiple endpoints

- MobileIron provides continuous visibility into what is happening on endpoints and mobile apps that connect to corporate and federal network and cloud services. Administrators can configure and apply consistent data security policies and enforce tiered remediation and mitigation actions across all endpoints. Secure access to enterprise email, calendars, and contacts is ensured while also preserving the native user experience.

- If BYOD initiatives are in place, MobileIron ensures that user privacy is maintained while enforcing federal compliance policies and control over federal resources and data accessed on personal devices. Encryption protects sensitive government data at rest on endpoints and in motion across any network or cloud service. Secure, instant access to enterprise resources and the prevention of unauthorized file sharing also protects against data loss.

- MobileIron protects CUI by continuously identifying mobile cybersecurity risks. Admins can prioritize these risks based on potential impacts, and mitigate the risks immediately on the device. The solution can then disable access to email, VPN, and Wi-Fi, or even remove data at rest from the device while preventing access to corporate and federal network and cloud services. In addition, a graduated set of local compliance actions can be taken over a period of time to increase user compliance while keeping productivity constant.

MobileIron Reference Architecture



Dashboards and reporting

Intuitive dashboards and custom reports provide deep visibility into device compliance, user access control, app security, and privacy risks. In addition, web APIs, Splunk forwarders and a reporting database export data into a centralized security information and event management (SIEM) system.

App security and privacy risk summary reports provide insight into app risk scoring, app behaviors, and context so admins can take necessary actions.

About MobileIron

MobileIron's government-grade, comprehensive security platform enables federal agencies to establish the highly-adaptive perimeter of zero-trust required to ensure the widest and deepest levels of security necessary. This can protect agencies against data loss caused by vulnerabilities introduced at the device, network, or application level. Selected as the platform of choice by the most security-conscious organizations in the world, MobileIron continues to maintain a leadership position in numerous industry reports published by Gartner, IDC, Forrester, and others. MobileIron has received more than 80 modern UEM patents, we have a broad ecosystem of over 350+ third party technology integrations, successfully completed numerous security certifications and standards, and is the only UEM vendor to achieve the Service Capability & Performance (SCP) Customer Support Certification.

MobileIron is a modern cloud and endpoint security platform providing unified endpoint management (UEM), cloud security, and mobile threat defense.

www.mobileiron.com
401 East Middlefield Road, Mountain View, CA 94043
globalsales@mobileiron.com
Tel: +1.877.819.3451
Fax :+1.650.919.8006

MobileIron