Ivanti EPMM Fortified: Securing and Managing iOS Devices in Government Classified Networks

Ivanti Endpoint Manager Mobile (EPMM) Fortified is the only enterprise mobility modernization solution proven to meet the rigorous demands of highly restricted and classified environments following National Information Assurance Partnership (NIAP) and National Security Agency's (NSA) Commercial Solutions for Classified (CSfC) baselines. Purpose-built for U.S. federal agencies, North Atlantic Treaty Organization (NATO) countries and U.S. allies, Ivanti EPMM Fortified delivers end-to-end lifecycle management and hardened security for government-furnished iOS mobile devices operating within red/classified and other secure networks.

With full support for iOS, Ivanti EPMM Fortified streamlines provisioning, enforces enterprise policies, enables operating system (OS) and application updates, and secures data at rest with secure app containerization — all while ensuring seamless mobile app lifecycles. Integration with the Apple App Store enables rapid delivery and management of mission-critical apps like iTAK and ForeFlight.

Ivanti EPMM Fortified also protects sensitive data with advanced data loss prevention (DLP) through secure app containerization, email client controls and application-level policy enforcement.

Ivanti EPMM Fortified goes beyond traditional mobile device management — it enables secure, classified mobility for mission-critical operations.

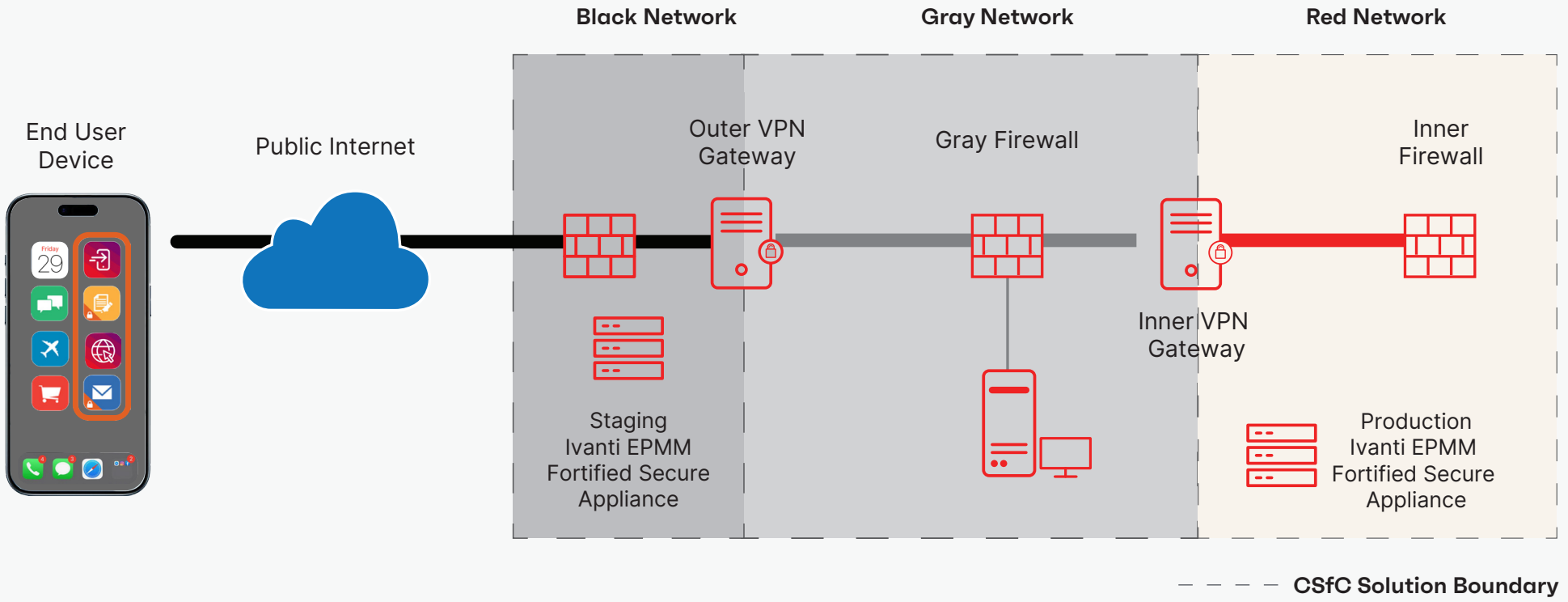
iOS devices have been approved by NATO to handle classified information up to the restricted level. This certification means that iOS devices can access NATO-restricted data without requiring any specialized security software or custom hardware modifications. The approval is based on iOS' built-in security features, which include hardened encryption, biometric authentication and protections, including memory integrity enforcement.

Deploy modern tactical devices at the edge

Ivanti EPMM Fortified delivers comprehensive mobile device management capabilities designed for secure, efficient tactical operations. Ivanti EPMM Fortified deploys and configures secure VPNs, further enabling access to red/classified networks directly from mobile endpoints. Ivanti EPMM Fortified provides comprehensive content management for hosting, managing and transferring data and classified documents on mobile endpoints.

Ivanti EPMM Fortified seamlessly deploys and integrates with encrypted voice and text solutions, ensuring secure communication channels for sensitive operations. Ivanti EPMM Fortified extends Common Access Card (CAC) certificates to mobile devices via Personal Identity Verification–Derived (PIV-D) and Purebred integration. It ensures resilient connectivity by supporting any iOS mobile devices running on secure 5G networks.

CSfC Solution Infrastructure Components



Holistic security with Ivanti AppConnect Fortified for dual data at rest

Ivanti AppConnect Fortified is a hardened mobile application container that provides an additional layer of encryption for iOS devices, delivering Federal Information Processing Standards (FIPS) 140-3 validated cryptography and NSA-approved data-at-rest protection. This ensures app data is protected, enables centrally managed Data Loss Prevention (DLP) and configures hardened authentication to the secure container.

Ivanti Fortified offers a holistic solution including Ivanti AppConnect and Ivanti EPMM — empowering the U.S. government and its allied nations to configure, manage, update and enable their mission critical apps on iOS-based mobile devices.

Ivanti EPMM Fortified benefits

Ivanti EPMM Fortified delivers unparalleled benefits for federal agencies operating iOS mobile devices in red/classified networks. Ivanti's solution empowers federal agencies to securely manage and deploy iOS mobile devices with enhanced efficiency and compliance.

With Ivanti EPMM Fortified you can:

- Deploy iOS mobile devices to warfighters, full-time employees or embedded contractors in any federal agency with a need for classified tactical or enterprise use cases.
- Equip frontline workers with mission critical apps and access to classified environments from any mobile device
- Achieve rapid authority to operate (ATO) and approval to deploy with Mobile Access Capability Package (MACP) approval.
- Easily provision, manage and secure devices in accordance with Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG), Department of War and National Institute of Standards and Technology (NIST) guidance.

Additional capabilities:

- Saves time with STIGs and accreditation processes with Ivanti's hardened virtual appliance.
- Streamlines patch management and supports disconnected network OS and application updates.
- Deploys and integrates with encrypted voice and text solutions.
- Protects devices and data against device, network, application and phishing attacks via integration with Mobile Threat Defense.
- Meets NSA CSfC, NIAP MDM PPv4 and Department of Defense Information Network Approved Product List (DoDIN APL) certification requirements.

ivanti

For more information on how Ivanti enable federal missions, visit ivanti.com/industries/federal-government

Mobile access capabilities package

The Mobile Device Management (MDM) server provides administration of mobile device policies and reporting on mobile device behavior. The MDM server is responsible for managing device enrollment, configuring devices, sending policies to the MDM agents, collecting reports on device status and sending commands to the agents. The above architecture provides a mobile endpoint access to secret or classified-level data on the red network from the tactical edge.

Secure your mission-critical mobility

Ivanti EPMM Fortified is the enterprise mobility modernization solution for iOS mobile devices, enabling federal agencies to securely deploy and manage iOS devices across highly restricted and unclassified environments. Its comprehensive features streamline operations, ensure stringent compliance with critical security standards such as STIGs, and facilitate rapid ATOs. By empowering warfighters and federal workers with secure access to red/classified networks from iOS devices, Ivanti EPMM Fortified enhances operational efficiency and mission readiness. Transform your mobile strategy with Ivanti EPMM Fortified and confidently secure your most sensitive communications and data.