Ivanti Enables Secure BYOAD for the Department of Defense

The Dept of Defense has released a memo that now allows for the use of non-government mobile devices to access the DoD network. This memorandum and attachment establish minimum requirements for the use of non-government owned mobile devices (i.e., personally, or corporately owned), hereinafter "Approved Mobile Device" (AMD), to store, process, transmit, or display up to DoD Controlled Unclassified Information (CUI)."

Modern mobile devices and apps have transformed how military service members communicate, collaborate, and maximize productivity. While many service members use government-owned devices, they also want to use their personal smartphones and tablets to stay connected wherever they work.

Ivanti provides government-grade security that enables military organizations to protect enterprise military apps and data on personally owned devices.

Leveraging native iOS and Android capabilities, our Unified Endpoint Management (UEM) and Mobile Application Management (MAM) solution enables service members to quickly authenticate to work apps on their devices while still protecting their private apps and data. This helps service members access essential military apps, such as email and tactical planning, without worrying about the security of their private data.

Ivanti provides an end-to-end, zero trust architecture

Ivanti can support military BYOAD programs through various management methods, from the native operating system, containerization, or segmentation, which separates work apps from personal apps on the device. This allows military organizations to safely deploy critical apps and data, such as DoD information, to service members on their personal

devices and gives the admin the ability to easily wipe the work off the device in an automated fashion.

Ivanti's unique "CAC-less" authentication process works by installing derived credentials via Purebred integration or leveraging cert generation. These credentials can only be accessed by apps in the FIPS 140-2 approved workspace. As a result, service members can easily access work apps without a physical gadget connecting their CAC, which makes authentication fast and easy for busy military service members on the go.

> "Mobile technology is impacting every aspect of the enterprise, and a scalable mobile management solution is critical. We are proud to provide Ivanti's industry-leading enterprise mobility platform to support DISA's mission."
>
> **Steve Keefe,** President and CEO, Patriot Technologies

The Ivanti platform has received Security Technical Implementation Guide (STIG) approval from the Defense Information Systems Agency (DISA), is on the DISA APL, and is NIAP Common Criteria approved. These certifications allow U.S. Department of Defense (DoD) agencies to deploy Ivanti on both Android and iOS devices within DoD networks.

Security standards and certifications

- Common Criteria Certification
- NIAP MDM PP V4
- CSfC
- DISA STIG
- EU-US Privacy Shield
- FedRAMP Authority to Operate (ATO)

Benefits of choosing Ivanti for BYOAD security

Ivanti Containerization

Prevent unauthorized or malicious apps from accessing DoD apps and data on multi-OS devices with mobile app workspace separation.

Leverage Apple iOS managed workspace or Android Enterprise Work Profile separation.

Ivanti Email+

Enable fast, easy and secure authentication to military email with S/MIME, calendar, tasks, document sharing and signing, plus other productivity apps within a FIPS 140-2 approved container.

Ivanti Tunnel

Manage, encrypt and secure traffic between the mobile device and back- end enterprise and cloud systems.

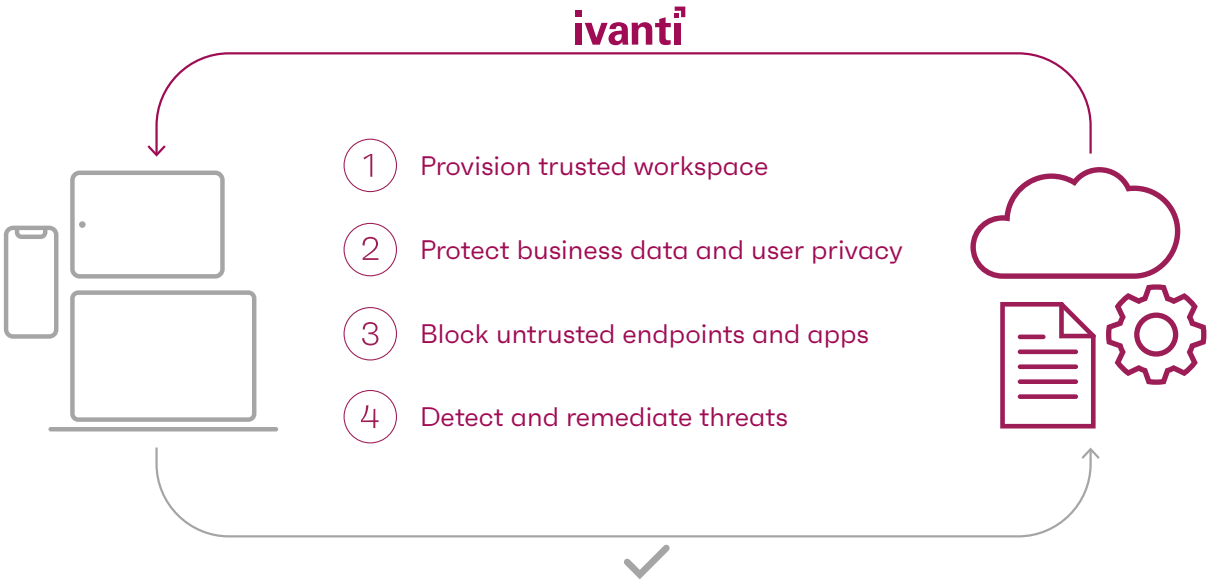
Ivanti Threat Defense

Defend against mobile phishing, device, network, and app threats with immediate, automatic protection that resides on the device itself — no user action is required to install or update a security app.

Ivanti Access

Leverage device and app posture, user identity, location, and more to ensure only trusted devices, apps and users can access apps and cloud services such as Microsoft Office 365, G Suite, Box, Deltek and others.

Benefits of choosing Ivanti for BYOAD security - *Continued*



- Separate personal apps from work apps in a secure workspace supported by the operating system.
- Integration with DoD IL5 M365 for data loss prevention (DLP) and device compliance.
- Enable fast and easy authentication with single sign-on (SSO) and multi-factor authentication (MFA).
- Protect data at rest in the secure workspace.
- Protect data in transit to the cloud or data center with the Ivanti conditional access policy enforcement point.
- Stop mobile threats including phishing with immediate, on-device protection and remediation.
- Ensure only trusted devices, apps and users can access work apps.
- Provide an enterprise app store and suite of productivity apps, to include email, web and document editing and sharing.

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com

Copyright © 2021, Ivanti. All rights reserved. IVI-2615 8/21 SR