ivanti

Modernizing Army Mobility for Secure, Mission-Ready Operations in Disconnected and Contested Environments

Executive summary

The Department of the Army stands at a critical juncture in mobility management. As legacy mobility programs are approaching possible end-of-life, Army commands risk inheriting fragmented mobile infrastructures that heighten cybersecurity exposure at a time when Warfighters require native-device experiences in the most contested operational environments on earth. The gap between security mandates and cybersecurity frameworks (e.g., Executive Order (EO) 14306, Cybersecurity and Infrastructure Security Agency (CISA) Binding Operational Directive (BOD) 25-01, zero trust requirements) and operational reality could widen further.

The unified Ivanti Endpoint Mobile Manager (EPMM) + Ivanti Mobile Threat Defense + virtual mobile infrastructure solution directly addresses these challenges by delivering a secure, scalable, multi-tenant mobility ecosystem purpose-built for contested and disconnected environments. It provides automated lifecycle management, real-time threat detection and virtualized data isolation that keeps sensitive information off the endpoint entirely. This unified architecture reduces IT burden, strengthens cybersecurity posture and ensures mission continuity, even after device loss or compromise. Unlike cloud-dependent alternatives, this solution is proven across the Department of the Army and the broader Department of War (DoW), offering lower total cost of ownership (TCO), easier sustainment and a mission-ready mobile experience that enhances both operational resilience and Warfighter effectiveness.

Key Findings

Security transformation:

The unified Ivanti EPMM + Ivanti Mobile Threat Defense + virtual mobile infrastructure solution delivers continuous threat detection, autonomous remediation and data isolation that protects mission-critical information even when devices are lost, captured or compromised in theater.

Operational impact:

Army commands implementing Ivanti's proposed integrated mobility solution saves time and resources, enabling IT teams to focus on mission support rather than device troubleshooting.

Mission readiness:

Unlike cloud-dependent alternatives requiring persistent connectivity, Ivanti's solution operates fully in air-gapped, disconnected and degraded network environments. This ensures Warfighters maintain operational capability regardless of adversarial disruption.

Proven at scale:

The integrated Ivanti + virtual mobile infrastructure solution directly addresses the challenges of self-managing mobility operations across multiple devices by delivering a secure, scalable, multi-tenant mobility ecosystem purpose-built for contested and disconnected environments. It provides automated lifecycle management, real-time threat detection and virtualized data isolation that keeps sensitive information off the endpoint entirely. This unified architecture reduces IT burden, strengthens cybersecurity posture and ensures mission continuity, even after device loss or compromise.

Challenge

Mission-enabled operational user experience without compromise

Warfighters and mission staff increasingly rely on mobile devices to execute command-and-control, logistics, intelligence and sustainment operations. Department of War (DoW) users demand native Apple iOS and Android experiences that perform reliably under pressure. Any degradation in usability directly impacts mission execution. At the same time, mobile platforms must meet stringent security requirements, creating tension between usability and protection if not architected correctly.

The Department of the Army operates across disconnected, air-gapped and on-premises. Mobility solutions must function when cloud connectivity is intermittent or unavailable and must rapidly recover when systems are degraded or reconstituted. Cloud-dependent approaches that assume persistent connectivity introduce operational risk in contested environments.

U.S. government-furnished devices, as well as the Department of the Army's user-owned devices, must remain operational in the harshest conditions within the theater of war, including extreme temperatures, damaged infrastructure and degraded networks. Warfighters and forward-deployed staff require offline access, secure data isolation and rapid recovery to ensure mission continuity even after device loss, compromise or system disruption.

Mobility program uncertainty

With key mobility programs potentially approaching sunset, Army commands may become responsible for self-managing mobility operations for their devices. If this shift occurs, it could lead to fragmentation, uneven readiness, tool sprawl, increased cybersecurity exposure and the reemergence of shadow IT as Army units attempt to meet mission demands with limited resources.

Most Army commands lack the IT manpower required to manually configure, sustain and troubleshoot large-scale mobile environments without automation, multi-tenancy and white-glove operational support. A modern mobility management solution must provide centralized orchestration, automated provisioning and proactive monitoring to reduce administrative overhead. This would enable the Army commands to focus on mission execution in the theater of war rather than focusing on device issues and troubleshooting.

Multi-tenancy and command autonomy

True multi-tenancy is essential for aligning mobility management with the Army's hierarchical structure, where responsibilities and authorities are distributed across echelons. A robust solution must allow enterprise-level administrators to enforce global standards while simultaneously empowering subordinate commands to tailor configurations to their unique operational environments.

This balance ensures that cybersecurity and compliance mandates are uniformly met, while local units retain the flexibility to adapt to mission-specific requirements. Multi-tenancy also supports auditability and accountability, enabling clear visibility into who made changes, when and why, which are critical for both operational integrity and compliance with federal oversight.

Policy, governance and cybersecurity mandates

Mobility management solutions mustn't only follow current mandates but also anticipate evolving requirements in the federal cybersecurity landscape. EO14306 and CISA BOD 25-01 emphasize the importance of continuous monitoring, rapid incident response and zero trust principles, all of which must be embedded into the Army's mobile ecosystem. A compliant solution should integrate automated policy enforcement, real-time threat detection and secure data handling practices to minimize risk exposure.

Moreover, alignment with DoW mobility directives ensures that Army units remain interoperable with joint and coalition partners, strengthening mission assurance. Failure to adopt such forward-leaning governance frameworks risks operational disruption, reputational damage and increased vulnerability to adversarial exploitation.

Solution

The Department of the Army requires a comprehensive mobility management solution that isn't only secure and compliant but also adaptable to the realities of contested, disconnected and resource-constrained environments. The integration of proven technologies, such as Ivanti Endpoint Mobile Manager (EPMM), Ivanti Mobile Threat Defense and a virtual mobile infrastructure solution into unified architecture reduces IT burden, enforces cybersecurity mandates and sustains mission readiness.

By combining automated lifecycle management, continuous threat detection and virtualized data isolation, this solution directly addresses the fragmentation, tool sprawl and compliance challenges facing Army commands, if key mobility programs are sunset. It delivers a scalable, multi-tenant capability that empowers units to self-manage mobility operations while maintaining centralized governance and alignment with federal mandates.

Ivanti Endpoint Mobile Manager

Ivanti EPMM provides a battle-tested, Army-proven mobile device management platform designed for secure, scalable and multi-tenant operations. Ivanti EPMM supports native iOS and Android experiences while enforcing granular security controls, policy compliance and automated lifecycle management. Its flexible deployment options, including on-premises and disconnected environments, align with the Department of the Army's operational realities and governance requirements.

Ivanti Mobile Threat Defense

Ivanti Mobile Threat Defense delivers continuous, real-time threat detection and response for mobile devices, networks and applications. Ivanti Mobile Threat Defense identifies malware, zero-day exploits, phishing attacks and device compromises, all without degrading user experience. Integrated directly with Ivanti EPMM, Ivanti Mobile Threat Defense enables automated remediation and policy enforcement, reducing risk while minimizing administrative burden.

Virtual mobility infrastructure technology

Virtual mobile infrastructure solutions provide a virtualized mobile workspace that keeps sensitive data off the endpoint device entirely. Applications and data reside securely in controlled environments while users access them through a native mobile experience. This architecture dramatically reduces data spillage risk, enables rapid recovery and supports use cases where devices may be lost, captured or operated in high-threat environments.

Integrated solution advantage

Together, Ivanti EPMM, Ivanti Mobile Threat Defense and a virtual mobile infrastructure solution form an end-to-end mobility management solution that directly mitigates the Army's most pressing challenges. The integrated architecture delivers secure, native mobile experiences while operating effectively in disconnected, air-gapped or on-premises. Automation, policy-driven enforcement and multi-tenant design reduce IT manpower requirements and enable commands to self-manage mobility programs without sacrificing governance or readiness.

This combined solution supports offline operations, rapid device recovery and mission continuity, even in contested or degraded environments. Virtual mobile infrastructure solutions minimize the impact of device loss, while Ivanti's unified management and threat defense ensure compliance with EO 14306, BOD 25-01, zero trust objectives and the Department of the Army's governance mandates — without introducing additional tool sprawl.

Differentiation from Microsoft Intune

While Microsoft Intune is often perceived as "included" with Microsoft's E3/E5 licensing, the operational reality reveals hidden costs. Intune requires significant manpower for planning, configuration and sustainment, resulting in higher ticket volumes, increased troubleshooting and greater lifecycle overhead. Its limited support for disconnected or air-gapped environments forces DoW agencies to build costly workarounds that negatively impact readiness and introduce unneeded cybersecurity risks.

In addition, reimage and re-enrollment cycles with Intune are longer, slowing recovery and impacting mission effectiveness. Additional tools are often required to meet Security Technical Implementation Guide (STIG) enforcement, mobile threat defense and offline capability requirements. This drives up cost and complexity. What appears "at no additional cost" at the licensing level quickly becomes expensive in manpower, risk and mission impact.

In contrast, the Ivanti + virtual mobile infrastructure solution is purpose-built for tactical and operational environments with easier enrollment, lower total cost of ownership through cost avoidance and a unified capability set proven across the Département of the Army and the broader DoW. This delivers a lower-TCO, mission-proven solution that reduces both IT burden and operational friction.

Conclusion

The Department of the Army stands at a pivotal moment in its mobility management journey. With the possibility of key mobility programs ending, and the increasing reliance on mobile platforms for mission-critical operations, the Army deserves a solution that's both resilient in contested environments and uncompromising in its security posture. The Ivanti + virtual mobile infrastructure solution architecture delivers a unified, multi-tenant mobility management capability that empowers the Department of the Army to self-manage their devices while remaining aligned with enterprise governance and zero trust mandates.

Integrating Ivanti Endpoint Mobile Manager, Ivanti Mobile Threat Defense and a virtual mobile infrastructure solution, ensures secure, native mobile experiences across iOS and Android while operating seamlessly in disconnected, air-gapped, cloud and degraded environments. It reduces IT burden through automation, enforces compliance with evolving federal cybersecurity directives and safeguards mission continuity even in the harshest operational conditions. Unlike solely cloud-dependent alternatives, this approach is purpose-built for the Army's tactical realities, offering lower TCO, faster recovery and reduced complexity.

Ivanti + virtual mobile infrastructure solution provides the Department of the Army with a future-ready mobility management solution that strengthens operational resilience, hardens cybersecurity posture and preserves the mission-enabled user experience without compromise. The Ivanti + Virtual mobile infrastructure solution equips Warfighters and mission staff with the tools they need to execute confidently, securely and effectively, ensuring that mobility remains a catalyst for mission success rather than a vulnerability in the theater of war.

To learn more about Ivanti's mission-ready mobility solutions for the Department of the Army and other DoW agencies, please visit www.ivanti.com/industries/federal-government

About Ivanti

Ivanti is a global enterprise IT and security software company dedicated to unlocking human potential by managing, automating and protecting data and systems to empower continuous innovation. With adaptable software solutions tailored to customer needs, Ivanti empowers IT and security teams to enhance operational efficiency, cut costs and proactively mitigate security risks. At the heart of Ivanti's offerings is the AI-powered Ivanti Neurons platform, which transforms the way IT and security teams operate. By delivering unified, reusable services and tools, the platform helps ensure consistent visibility, scalability, and secure solution implementation, enabling teams to work smarter, not harder. Ivanti follows "Secure by Design" principles to provide software solutions that scale with our customers' needs to help enable IT and Security to improve operational efficiency while reducing costs and proactively reducing risk. Ivanti fosters an inclusive environment where diverse perspectives are honored and valued, reflecting a commitment to a sustainable future for customers, partners, employees and the planet. For more information, visit ivanti.com and follow @GoIvanti.

ivanti

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