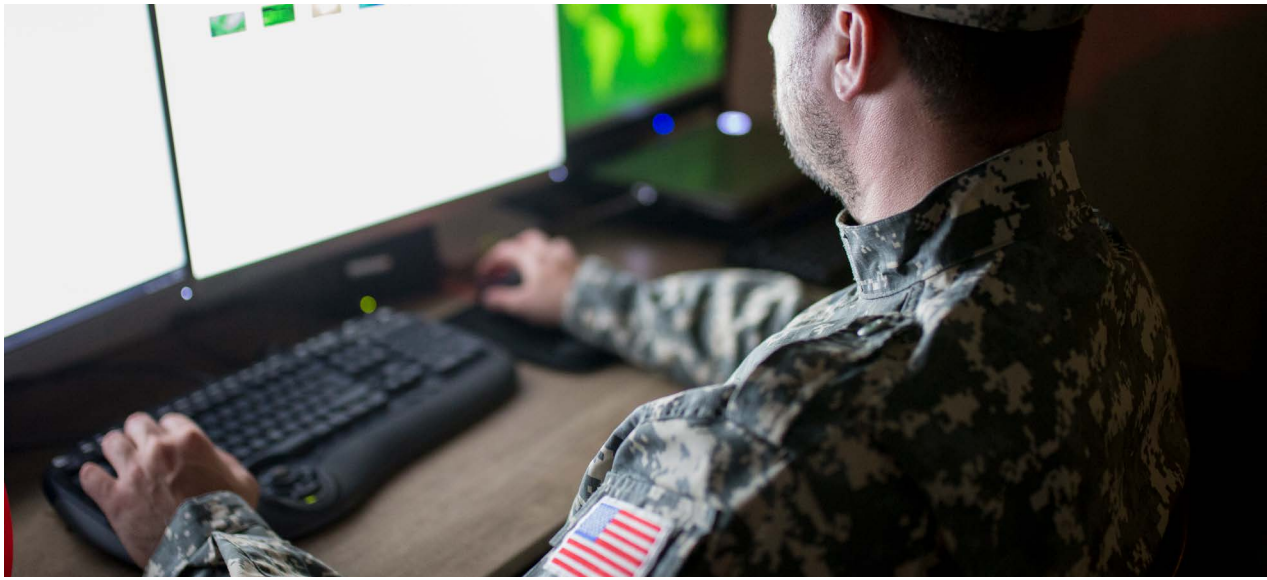
ivanti

# The Next Generation of Enterprise Mobility Management for the DoD

The Department of Defense (DoD) and its component agencies, including the Defense Information Systems Agency (DISA), operate in a complex and increasingly fiscally constrained environment. While advanced mission-critical capabilities are essential to supporting U.S. Warfighters, agency leadership, Executive Orders (EO) and other federal mandates emphasize the need to focus on cost reduction. The proliferation of mobile devices and security solutions, coupled with the lack of an overarching mobility modernization roadmap across the DoD, creates significant inefficiencies, inflates IT operational costs and complicates the comprehensive lifecycle and security management of mobile and wearable devices deployed at the tactical edge. This fragmented approach undermines DISA and other DoD agencies' ability to achieve optimal IT and end-user efficiency, and it introduces unnecessary security vulnerabilities and compliance risks.

Maintaining redundant enterprise mobility management platforms leads to inflated licensing fees, increased administrative overhead costs and inefficient allocation of IT and security resources. This duplicative spend conflicts with administration EOs and policies to consolidate procurement and optimize budgets, and it hinders DISA and the DoD's capacity to invest in strategic priorities and accelerate value through integrated and automated solutions DoD-wide. The absence of a unified mobility modernization framework across the DoD also makes deploying seamless security measures more difficult and increases the opportunity for cyberattacks by nation-states and other bad actors across classified and unclassified environments.

Without a highly efficient singular enterprise mobility management solution, the DoD faces challenges in providing frictionless user experiences to our Warfighters while proactively mitigating security risks. The complexity of managing diverse device types and use cases across varying IT environments (e.g., classified, on-premises, cloud, hybrid) with multiple technology vendors creates operational bottlenecks and increases the potential for security gaps, which impedes the DoD's ability to achieve a comprehensive enterprise end-to-end mobility management and security configuration. The result is increased costs, duplicative spending, additional cybersecurity challenges and IT resources allocating time to redundant IT operations, but it's not too late for the DoD to change that outcome.



## Ivanti expertise

Ivanti provides defense agencies with solutions that modernize enterprise mobility management and reduce operational costs and wasteful spend, while proactively reducing security risk, improving IT and end-user efficiency, and productivity. Ivanti has a comprehensive technology stack that federal CIOs and CISOs can leverage — giving IT and security teams feature-rich software solutions that scale up or down based on their organizations' needs to enable, secure and manage employees' efficiency.

Ivanti's proven track record has helped many federal agencies lower software and vendor costs, optimize IT budgets and accelerate value through consolidation, integration and automation. This enables IT and security teams to reduce risk, focus on strategic priorities and realize efficiencies by avoiding redundant solutions. Ivanti provides versatile mobile device management (including Apple iOS and Android) and critical security capabilities that protect traditional, mission-critical mobile and wearable devices that connect at the edge.

### Savings and security

- Reduced running costs by 80%.
- Securely managed 180k devices and 400+ apps.
- Saved over $300k per decommissioned on-premises site.
- Reduced provisioning time by over 60%

## The solutions

To meet current and future mission needs, DISA and other defense agencies require a scalable, secure and proven enterprise mobility management solution with a frictionless user experience. Ivanti has served as DISA's trusted mobility modernization partner for more than 12 years through a number of programs like DMUC and EPMS, delivering enterprise mobility management and services to joint Warfighters, agency leadership and mission partners. Ivanti is the only vendor to meet the full spectrum of DISA's enterprise use cases and critical integrations, making it uniquely positioned to support DISA's next generation of enterprise mobility management solution across classified and unclassified environments.

Ivanti Neurons for MDM gives the DoD the power to secure any device, of any kind, anywhere. As an endpoint-agnostic solution, DoD agencies can manage iPhones, iPads, Macs, Android devices, rugged mobile devices, PCs, Chromebooks, Oculus and more — in a single, unified platform.

In addition to enterprise mobility management, Ivanti helps elevate protection against "mishing" (i.e. phishing delivered via text message) and zero-day threats with mobile security that integrates into the enterprise mobility management platform. Deploying mobile security with Ivanti is easy for agency IT and security teams, but also transparent to the end user — deploying to managed devices without requiring end-user involvement with the installation. This silent deployment makes it possible to attain 100% implementation, thus mitigating compliance risk.

## Why Ivanti?

Our solutions provide seamless deployment, advanced cybersecurity and an optimized end-user experience for all DoD-managed mobile and cloud assets. Ivanti is uniquely situated to enable DISA and other defense agencies to consolidate under a single enterprise mobility management vendor to meet all DoD mission requirements for the unclassified and classified environments, allowing DISA and DoD agencies to save on redundant resources and costs for programs like DMUC and DMCC.

- **Ivanti is the only provider with a proven track record of executing the complex, large-scale and diverse federal requirements unique to DISA and other DoD agencies. No other vendor delivers:**
  - Custom user profiles matching users with the right access and policies.
  - Dynamic profiles to improve privacy and user experiences based on time and location.
  - Offline security to protect sensitive data in disconnected government environments.
  - Mobile security that deploys without any end-user interaction, putting 100% compliance within reach.
- **Comprehensive end-to-end lifecycle management and security configuration for all device types and use cases:**
  - VIPs.
  - Knowledge workers.
  - Frontline workers.
  - Tactical, kiosk, supply chain, etc.
- **Deployment flexibility through on-premises, classified networks, hybrid or cloud options (SaaS Cloud and FSI Multi-Service Provider offerings), including the following certifications:**
  - NIAP.
  - FedRAMP Moderate.
  - FedRAMP High/DoD IL5 (in process).

## Ivanti's commitment to security

Like most other companies that develop network security and edge products, Ivanti's solutions have been targeted and exploited by sophisticated threat actors. While these products are not the ultimate target, they are increasingly the route that well-resourced nation-state bad actors are focusing their efforts on for espionage campaigns against extremely high-value organizations.

An important point: we all continue to reap value from important security industry partnerships. By collaborating closely with the DoD, other federal agencies and security industry partners, we are stronger and more secure together. We thank our collaborators and look forward to redoubling our efforts in the future.

## Investing in product security and embracing Secure by Design frameworks

Ivanti's response to any incident is to learn from it, invest in improving our products and ultimately make it harder for sophisticated bad actors to abuse our products. Below are some examples of recent actions taken to reinforce product integrity.

| | |
|---|---|
| **Specialized security resources** | The Ivanti Security team comprises highly skilled security specialists who support Ivanti's overall security and a dedicated Product Security team focused on the security of our solutions. The size of this team has increased more than 8X over the past few years, along with meaningful elevation in threat expertise. |
| **Leading third-party partnerships and tooling** | Ivanti has expanded engagements with leading security and threat intelligence experts. We use industry-leading static and dynamic code analysis tooling during the development process to validate the security of our solutions and ensure Ivanti developers adhere to secure coding practices. |
| **Secure by Design alignment** | Development processes include robust security protocols throughout the product lifecycle, including rigorous threat modeling, vulnerability assessment and security measures specifically designed to improve our solutions' resilience against current and emerging threats. Additional details can be found on our website. |
| **Product security optimization** | We have invested significant resources in our Ivanti Neurons cloud platform to alleviate the burden of security for our customers, including automated security updates, MFA enabled out of the box and a unified role-based access control (RBAC) system. |
| **Organizational enhancements** | The Network Security Group, which is responsible for developing Ivanti Connect Secure, has evolved in focus, size and product leadership. The team has expanded internal engineering resources and engaged specialized external support as needed to achieve security expectations. |
| **Prioritizing product security enhancements for Ivanti Connect Secure (ICS)** | We have prioritized product security enhancements for ICS. Additional security enhancements in our Network Security products include Secure Boot with TPM key management, Non-Root Privilege Access Control, a modernized web service and WAF component. |
| **Enhancements to the Integrity Checker Tool (ICT)** | ICT is an effective tool for identifying threat actor efforts and is a prime example of Ivanti's commitment to proactive security for our solutions. This tool has aided in our forensic efforts, including during vulnerability instances, alerting our customers to threat actor activity on the same day it occurred. This allowed for a swift response and development of a fix for the issue. |

## Earning trust through guidance and communication

Continued investment in vulnerability identification is yielding significant results for federal agencies. Ivanti continues to enhance internal scanning, manual exploitation and testing capabilities. Increased communications — through an enhanced responsible disclosure process and more effective information sharing with the security ecosystem — have led Ivanti to become a CVE Numbering Authority. This is evidence of Ivanti's commitment to transparency and delivering beyond industry standards.

A more secure ecosystem includes thoughtfully guiding migrations from legacy, end-of life products to modern solutions that offer advanced features that boost productivity and strengthen security. While not every situation is ripe for migration to the cloud-based Ivanti platform, best practice guidance continues to be available, so on-premises implementations may continue with minimized risk until such time that cloud migration aligns with strategic initiatives.

Inbound feedback is equally important as outbound communications and guidance. Ivanti offers a variety of forums for sharing input throughout the solution lifecycle. It is essential to hear about evolving needs and emerging use cases so that the value received from Ivanti products continues to grow into the future. And it is equally important to recognize that security is one of the first concerns keeping federal IT teams up at night. Being available to recognize and address those concerns continues to be a core commitment for Ivanti. We're your trusted partner for efficient enterprise mobility management and a productive, secure mobile ecosystem.

## Conclusion

The DoD is at the nexus of modernizing its mobility IT infrastructure, driven by the need to support our Warfighters and adhering to the administration's EOs and mandates to reduce costs and mitigate duplicative spending. The reliance on fragmented enterprise mobility management and security solutions increases costs, creates inefficiencies and opens the DoD up to security vulnerabilities. Ivanti's proven expertise, developed over a decade of serving DISA and other DoD agencies, offers a singular, scalable and secure enterprise mobility management solution that addresses these challenges and enhances operation efficiency and mitigates risk across classified and unclassified environments.

By choosing Ivanti, the DoD can achieve unparalleled efficiency and security and consolidate redundant systems under a single, trusted technology vendor. We are committed to Secure by Design, continuous product security enhancements, Zero Trust architecture and transparent communications. Our mobility modernization solutions deliver seamless deployment, advanced cybersecurity and optimized end-user experience for all DoD-managed mobile and wearable devices. Ivanti stands ready as the mission partner uniquely positioned to meet the full spectrum of the DoD's mobility requirements and to provide the DoD with a more productive, secure and modern mobility management future.

## About Ivanti

Ivanti is an enterprise software company that provides a comprehensive IT and security cloud-based platform. Ivanti provides software solutions that scale with our customers' needs to help enable IT and Security to improve operational efficiency while reducing costs and proactively reducing security risk. The Ivanti Neurons platform is cloud-native and is designed as a foundation of unified and reusable services and tools for consistent visibility, scalability and secure solution delivery. Over 34,000 customers, including 85 of the Fortune 100, have chosen Ivanti to meet challenges head-on with its end-to-end solutions. At Ivanti, we strive to create an environment where all perspectives are heard, respected and valued and we are committed to a more sustainable future for our customers, partners, employees and the planet. For more information, visit ivanti.com and follow @GoIvanti.



ivanti

To learn more about Ivanti Neurons for MDM for the DoD, please read this whitepaper and datasheet.