Managing and Securing DoD's Global Device Fleet with Ivanti Neurons MDM and MTD

Across the Department of Defense (DoD), teams need the ability to operate anywhere and in any condition. With DoD personnel traveling the globe and rotating roles, they frequently need new or updated devices. Issuing, securing and decommissioning devices can be a burden on IT resources. Device security cannot be compromised at any point–each endpoint must remain secure.

Ivanti Neurons for Mobile Device Management (MDM) and Ivanti Mobile Threat Defense (MTD) help warfighters, civilian defense employees and embedded contractors use any device their role requires, while ensuring those devices are always accounted for and equipped with the strongest threat protections.

Manage devices everywhere: Ivanti Neurons for MDM

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.

- **Classified + tactical network management:** Discover, secure and manage devices on air-gapped, highly restricted and closed networks through a centralized platform that streamlines operations and enhances security posture.
- **Support for tactical modern devices on the edge:** Comprehensive tactical device support, including secure VPN access, TAK mapping, encrypted communications, certificate management with PIV-D/Purebred integration and secure network connectivity for classified operations.
- **Advanced security controls:** Implement security measures, including policy enforcement, strict access controls and disconnected network patch management, to protect sensitive data across all devices.
- **FedRAMP authorization:** Ivanti Neurons for MDM is FedRAMP Moderate, helping your agency ensure compliance with federal standards.
- **Multifactor authentication enforcement:** Ensure two-factor authentication from common access cards (CAC) and personal identity verification (PIV) is applied across all devices performing government work.

Ivanti Mobile Threat Defense

- Ivanti Neurons for MTD adds layers of security to each device. It runs continuously even when the device is offline, detecting and remediating security issues as they happen. This data provides visibility into threats across all devices, helping IT teams combat threats and make more timely, informed and actionable decisions to better protect the DoD's IT network from adversaries and bad actors.

- **Machine learning (ML) powered threat detection:** Harness ML to identify and mitigate mobile security threats before they affect operations.
- **Continuous protection protocol:** Maintain robust security measures during network disruptions, ensuring your field personnel remain protected even when they're offline.
- **Comprehensive security architecture:** Leverage real-time malware detection, network threat monitoring and sophisticated application security controls and behavior monitoring.
- **Configure devices for compliance:** Set device configurations to automatically enforce FISMA, NIST and DoD-specific security requirements across all mobile devices while maintaining detailed compliance documentation.

MDM and MTD: Combining to combat evolving threats

When combined, Ivanti Neurons for MTD and Ivanti MDM deliver a comprehensive mobile security solution that streamlines operations while maximizing protection. Comprehensive fleet management layers with robust security that works on all devices, regardless of connectivity status, to help protect those who protect us.

Use cases

- **Device deployment and onboarding:** MDM allows organizations to achieve (near) 100% adoption of the solution. Device setup and configuration are quick and efficient, and MTD works alongside it to ensure each device meets required security standards from day one. Deployment happens without any end-user interaction, so there are no "accept" or "allow" buttons that need to be clicked.
- **Classified and air-gapped network device management:** MDM offers support for air-gapped, highly restricted and closed networks. MTD monitors devices across those networks to pinpoint and mitigate threats before they compromise the network at large.
- **Lost device protection:** MDM provides endpoint discovery and remote data wiping capabilities for lost or stolen devices, while MTD actively protects against unauthorized data access and theft attempts.
- **Application management:** MDM's integrated AppStore lets security teams manage sensitive apps like ATAK or iTAK with full control over application distribution and permissions. MTD safeguards devices by monitoring applications for potential security risks and suspicious behavior.
- **Zero Trust adherence:** Conditional access controls in MDM let DoD cybersecurity teams fine-tune access control inputs with device, app, network, geographic region and more. In case of improper access, MTD adds more layers of protection with threat detection and remediation.

Ivanti's comprehensive solutions are designed to meet these challenges at scale, combining robust device management with advanced threat detection to protect the nation's largest workforce.

By implementing Ivanti Neurons for MDM and Ivanti MTD together, the DoD can:

- Efficiently manage and secure millions of devices across global locations.
- Maintain strict security standards while enabling operational flexibility.
- Protect sensitive data with FedRAMP-authorized, military-grade security.
- Streamline IT operations through automated device management and threat response.

ivanti

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.

For more information about Ivanti's innovative federal IT solutions, or to contact us, please visit www.ivanti.com/industries/government