Ivanti Neurons for MDM (formerly MobileIron Cloud)

Secure access to more devices to help your workforce.

Every agency needs secure access and easy management of their data on any endpoint. For today's hybrid workforce, this includes the use of diverse endpoints such as iOS, iPadOS, macOS, Android, ChromeOS and Windows devices. For some agencies, it can also include immersive and innovative devices such as HoloLens, Oculus, Zebra and more.

Managing privacy and compliance, minimizing risk and supporting a mobile workforce necessitates separating and protecting government apps from personal apps within staff devices. As public sector service delivery continues to evolve, agencies need the freedom to let their staff work with the best endpoint device for the job anytime and anywhere. To achieve this, a secure, unified endpoint management solution is needed, offering easy enrollment, remote troubleshooting and timely software updates. This solution should also ensure a superior experience for all users, including agency staff, contractors, teachers and administrators in schools.

Secure and manage your devices everywhere with Ivanti Neurons for MDM

You can manage any endpoint and its apps with a unified solution from Ivanti Neurons for Modern Device Management (MDM) (formerly MobileIron Cloud). Ivanti Neurons for MDM enables secure access to data and apps on any device across your agency, ensuring that only authorized users, devices, apps and services can access agency resources.

Ivanti Neurons for MDM puts enterprise-wide mobile security at the forefront and allows you to build upon it with technologies to eliminate passwords with zero sign-on (ZSO), ensure user authentication with multi-factor authentication (MFA) and detect and mitigate endpoint security threats with mobile threat defense (MTD).

How Ivanti Neurons for MDM helps agencies support secure work access from any device

Ensure privacy and compliance in protecting sensitive data

Secure government data on any endpoint and separate government and personal data on various endpoints. Ensure two-factor authentication from common access cards (CAC) and personal identity verification (PIV) is applied across all devices performing government work.

Facilitate multi-device, multi-OS, multi-app management from a single console

Ivanti Neurons MDM allows agencies to manage a mixed device environment with iPhones, iPads, Macs, Android devices, Windows laptops, Chromebooks and PCs, Zebra, Oculus, etc. Unified management of these devices with different OSs and apps is a top priority.

Ensure access from anywhere on personal and provided devices

Support your agency's hybrid workforce by ensuring the devices they use to do their work, whether personal or provided by your agency, are secure and connected.

Provide a superior end-user choice and onboard with ease

When user choice and end user experience matter, Ivanti Neurons for MDM provides the simplest onboarding and superior on-device experience, which improves user productivity.

Rationalize IT resources needed for endpoint management

Leverage powerful tools that simplify the administrative management of staff devices, including automated onboarding, helpdesk tools, Trust Engine and passwordless authentication. Keep your workforce on mission without distractions or long waits for support.

Security standards and certifications*

- FedRAMP Moderate Authority
- CSA STAR
- SOC 2 Type II

**Additional information on certifications can be found at: ivanti.com/resources/security-compliance*

Comprehensive security

Ivanti Neurons for MDM provides the visibility and IT controls needed to secure, manage and monitor any government or personal-owned mobile device or desktop that accesses your data. It allows organizations to secure a vast range of bring-your-own (BYO) devices that can be used to further your mission while managing the entire lifecycle of the endpoint, including:

- Automated onboarding
- Policy configuration and enforcement
- Application distribution and management
- Management and security monitoring
- Decommissioning and retirement

Ivanti Neurons for MDM is built on a proven, secure, scalable architecture with flexible deployment options that put the user experience first while complying with stringent government security standards.

Ivanti Sentry acts as an email and content in-line gateway that manages, encrypts and secures traffic between the mobile device and back-end systems. Ivanti Tunnel is a multi-OS app VPN solution that allows organizations to authorize specific mobile apps to access government resources behind the firewall without requiring any user interaction.

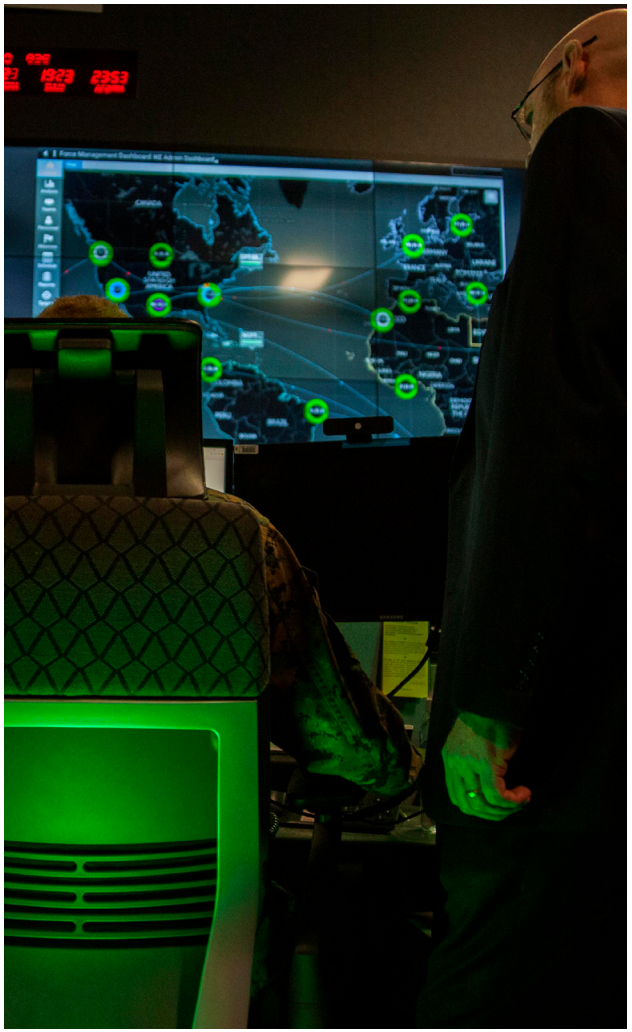
Manage and scale your agency confidently and securely

Organizational and user control: Ivanti Neurons for MDM allows agencies to implement individualized mobility and security strategies to meet their needs at their own pace. Ivanti also ensures the privacy of users' personal data while protecting sensitive government data—giving users and administrators alike control over their information.

Freedom of choice: Ivanti Neurons for MDM is OS and device-agnostic. IT administrators can choose a cloud or on-premises deployment based on their budget, and workers can use their favorite endpoints for work.

Experience-driven adoption: Ivanti Neurons for MDM helps IT drive adoption by supporting a native user experience across productivity apps at work. This simplifies compliance while mitigating security threats and shadow IT. With higher staff adoption rates, IT can accelerate productivity and growth across the agency.

Decrease interruptions in work time: Our security platform prevents interruptions without being intrusive to the user. Invisible and automated security ensures compliance while allowing your agency to forge ahead.



Key Features and Capabilities

Feature	Capabilities
Device management and security	
Security and management	Secure and manage endpoints running iOS, macOS, iPadOS, Android, ChromeOS and Windows operating systems. Available on-premises and as a cloud service.
Mobile application management (MAM)	Secure government apps with Ivanti AppStation on contractor and staff devices without requiring device management.
Easy onboarding	Leverage services such as Apple Business Manager (ABM), Google Zero-Touch Enrollment and Windows AutoPilot to provide users with automated device enrollment.
Secure email gateway	Ivanti Sentry is an in-line gateway that manages, encrypts and secures traffic. between the mobile endpoint and back-end architecture.
App distribution and configuration	Apps@Work, an enterprise app storefront, facilitates the secure distribution of mobile apps. In addition, capabilities such as iOS Managed Apps and Android Enterprise allow for easy configuration of app-level settings and security policies.
Secure productivity	
Secure email and personal information management (PIM) app	Ivanti Email+ is a cross-platform, secure PIM application for iOS and Android. Security controls include encryption fit for the government, certificate-based authentication, S/MIME, application-level encryption and passcode enforcement.
Secure web browsing	Web@Work enables secure web browsing by protecting data in motion and data at rest. Custom bookmarks and secure tunneling ensure users have quick and safe access to information.

Feature	Capabilities
Secure content collaboration	Docs@Work allows users to access, create, edit, markup and share content securely from repositories such as SharePoint, Box, Google Drive and more.
Mobile app containerization	Deploy the AppConnect SDK or app wrapper to provide an additional layer of security for your in-house mobile apps, or choose from our ecosystem of AppConnect integrated apps.
Derived Credentials	Support two-factor authentication using common access cards (CAC) and personal identity verification (PIV).
Secure connectivity	
Per-App VPN	Ivanti Tunnel is a multi-OS VPN solution that allows agencies to authorize specific mobile apps to access government resources behind. the firewall without requiring any user interaction.
Scale IT operations	
Helpdesk tools	Help@Work lets IT remotely view and control a user's screen, with the user's permission, to help troubleshoot and solve issues efficiently.
Reporting	Gain in-depth visibility and control across all managed devices via custom reports and automated remediation actions.
Conditional access	
Trust Engine	Combine various signals such as user, device, app, network, geographic region and more to provide adaptive access control.
Passwordless user authentication	Passwordless multi-factor authentication using the device as identity for a single cloud or on-premises application.

Summary

Ivanti Neurons for MDM makes it possible for any organization — federal, state, local or educational — to secure a diverse range of endpoint devices. It empowers your workforce to get more done with the devices that work best for their roles, and it helps them stay on track with no-distraction updates and controls. Keep your mission moving forward by empowering your staff and IT teams to do their best work with the best device for the job.

About Ivanti

Ivanti elevates and secures Everywhere Work so that people and organizations can thrive. We make technology work for people, not the other way around. Today's employees use a wide range of corporate and personal devices to access IT applications and data over multiple networks to stay productive, wherever and however they work. Ivanti is one of the only technology companies that finds, manages and protects each IT asset and endpoint in an organization. Over 40,000 customers, including 88 of the Fortune 100, have chosen Ivanti to help them deliver an excellent digital employee experience and improve IT and security team productivity and efficiency. At Ivanti, we strive to create an environment where all perspectives are heard, respected and valued and are committed to a more sustainable future for our customers, partners, employees and the planet. For more information, visit www.ivanti.com and follow @GoIvanti.

ivanti

For more information, or to contact Ivanti, please visit ivanti.com.