Simplified rugged device management and security

Benefits of Ivanti

- Lower TCO for rugged, line of business devices
- Simplified device lifecycle management
- Fewer helpdesk incidents with remote troubleshooting

Companies around the world rely on rugged mobile devices to help frontline workers stay productive wherever they work — in the warehouse, on the shop floor, or out in the field. The challenge: to quickly get users up and running on these devices, it is essential to efficiently deploy, manage and protect each device with all the right apps, configurations and security settings. As if that's not enough, you also need an easy way to track the devices, protect them against mobile attacks, wipe apps and data, and ultimately retire them.

Ivanti delivers the power of mobile device management (MDM) to help organizations simplify rugged device configuration, management and firmware over the air (FOTA) updates. In addition to managing all of your rugged devices, Ivanti's unified platform provides complete visibility across your entire mobile fleet, including rugged, wearable and fixed-mounted devices, use cases throughout the supply chain, and remote workers – from the warehouse to the retail floor.

Ivanti's zero trust security approach provides continuous protection against the latest mobile threats, secures access to business data in the cloud, and eliminates the hassle of passwords with zero sign-on authentication. It's why operations teams across the most demanding global supply chains rely on Ivanti for comprehensive, enterprise-grade mobility management and security.

Secure, Available, Accessible Deployments

Rugged device deployments operating with Ivanti's mobility management and security in place help ensure the mobile workforce is secure, connected, and able to work at peak productivity. And as an Android Enterprise Gold Partner, organizations trust Ivanti to help prepare their mobile fleets to meet the demands of today's and tomorrow's business – from bulk enrollment through app deployment and updates, and through remote troubleshooting. Ivanti Neurons for MDM puts zero trust security at the center of your enterprise and allows you to build upon it with capabilities such as zero sign-on, multi-factor authentication, and mobile threat defense.

Maintain Control of the Most Critical Mobile Fleets

Zero-touch enrollment

As an Android Enterprise Recommended Enterprise Mobility Management (EMM) solution, Ivanti Neurons for MDM supports Android zero-touch enrollment, which enables large-scale Android deployments across rugged device manufacturers, and Samsung Knox mobile enrollment for smart device users This simplifies device provisioning and accelerates deployment bulk without having to manually configure each device. Users simply power on and start using the device with management features, apps and configurations ready to go.

OEMConfig for corporate-liable devices

Manufacturers implement device configurations through an Android app, which can be deployed through Ivanti. This ensures admins automatically get zero-day support for new device configurations without any manual intervention required.

App lifecycle management

Admins deploy, update and retire enterprise apps through a managed enterprise app store as well as third-party app stores. Apps can be administered through the enterprise app store and distributed to different users depending on corporate policy. Through the Ivanti Neurons for MDM platform, admins can set policies that restrict which apps employees can download and prevent any apps from performing malicious actions.

Device lockdown and restrictions

Neurons for MDM empowers operations IT admins to configure rugged devices with settings, certificates, Wi-Fi, VPN, passcode requirements and more.

Protecting Mobile Productivity

Velocity platform interoperability

Designed and tested together, Neurons for MDM is the easiest way to deploy Ivanti Velocity (and Zebra All-Touch TE) app configuration, application host profiles, manage the apps and rugged devices together, and is the most efficient combination for simplified app patching. And Velocity Forms are created and deployed from same cloud platform as Neurons for MDM.

Support for manufacturer-specific tools

Ivanti Neurons for MDM fully supports tools like Zebra StageNow and LifeGuard. Tools like these simplify device configuration via XML and extending the life of rugged devices by adding years of OS security support, respectively. Neurons for MDM automates these processes, helping keep devices up-to-date and less exposed to cyber threats.

Mobile threat detection and remediation

Ivanti Mobile Threat Defense (MTD) provides immediate, ongoing threat detection and remediation for rugged devices. MTD protects against sophisticated device, app and network threats that can silently breach enterprises systems and steal business data.

Secure connectivity and access

Ivanti Access enables a secure zero sign-on experience while also blocking non-compliant devices from accessing cloud applications. Plus, IT can protect data as it leaves a device by providing secure connectivity through Ivanti Tunnel, which provides a per-app VPN and eliminates the need for a separate third-party VPN.

Device lockdown

If a device is ever lost or stolen, IT can remotely place the device in lockdown mode to prevent unauthorized users or malicious actors from accessing apps and data on the device.

Device monitoring and maintenance

Device compliance policies

Neurons for MDM helps operations teams establish and enforce a consistent security framework using an intuitive policy engine. Non-compliant devices can be quickly identified and denied access to corporate resources if needed. Granular policy settings and compliance configurations also allow IT to adapt and update security policies as business requirements and regulations such as GDPR, PCI DSS and HIPAA evolve.

Remote troubleshooting

Ivanti's Help@Work capability allows administrators to troubleshoot device issues with remote software, which helps to reduce support costs, improve device performance, and help frontline workers stay productive. Ivanti also enables remote troubleshooting – even when the rugged device is locked down in kiosk mode – with minimal user interaction required.

Device lifecycle management

Remotely wipe all the corporate apps, data and configurations from corporate-owned devices and restore factory settings for repurposing. Many operations include a BYOD model for managers, and Neurons for MDM is able to clear all corporate apps and data from those devices, while respecting personal content – especially important when a BYOD user leaves the organization. Lifecycle management of corporate and personal devices is just one way Neurons for MDM is the single mobility management solution for all the devices in your organization.

Visit Ivanti.com/mdm to learn more

Request Demo

https://www.ivanti.com/lp/demo

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