Ivanti Neurons for MDM
Device Management for Operations and IT (formerly MobileIron Cloud)

Secure and Manage Rugged Devices, Smartphones and More

Business operations have no time for downtime, and stoppages caused by cyberattacks are among your growing concerns. You need visibility to all the operational tech in your line of business: rugged mobile computers, tablets, wearables, and the software on each, so you can manage and protect it all alongside the laptops and smartphones corporate IT oversees. The shift to Android Enterprise is designed to help organizations with standards for performance, though not all enterprise mobility management products are compliant. You need to increase cybersecurity protection, swiftly access the benefits of Android Enterprise, and do it all while ensuring uptime for the workers in your supply chain operations.

Android Enterprise Recommended

With more than 75% of mobile endpoints running the Android OS, you need one platform to manage them all. Not all enterprise mobility management products are the same. You need to know your operational tech is managed in line with leading standards for optimized device performance and user experience. Ivanti Neurons for MDM is an Android Enterprise Recommended solution. You benefit from a solution that has been validated by the leading mobile operating system vendor, with requirements that are equally relevant for securing and managing your devices running iOS or Windows.

Complete Visibility

Siloed endpoint management is no longer viable for many organizations. Operational and Corporate IT have a shared interest to enable work at the point of activity. Ivanti Neurons for MDM provides visibility across all the devices in your ecosystem, helping you get accurate accounting of what hardware is out there, the apps and OS version operating on each, and the confidence that they are secure. It's a single pane of glass for managing any device, any OS, anywhere in your organization. And the solution is built on our Ivanti Neurons platform rated a leader in Unified Endpoint Management[1].

Operational Security

Threat actors are targeting the supply chain, and you need to know your operational tech is protected to minimize risk. Adding Mobile Threat Defense from our MobileIron heritage to Ivanti Neurons for MDM gives you real-time threat intelligence to help you detect malicious apps and prevent known and zero-day threats. Reinforcing prevention tactics, including vulnerability assessments, are essential to keeping cybercriminals from entering your ecosystem. With improved visibility, you're able to assess software exposures across application and OSes, so you know what patches are necessary to protect productivity.

Use Cases

- **Manage your Rugged Mobile Fleet:** Support and service all your devices, mobile apps, and operating systems they run – Android, iOS, and Windows, to ensure peak performance.

- **Software Risk Management:** Know whether all your devices have the latest app version installed, or if that OS update has been deployed.

- **Simplified Enrollment:** Easily stage devices through Android Enterprise Zero-Touch Enrollment, via QR code scanning, or near-field communication (NFC).

- **Role-based Access:** Rugged devices are often shared among workers. Give each access to the appropriate software tools to accomplish their tasks.

Maximize Uptime

Every minute of delay can put your customer satisfaction, and even your peak season at risk. You don't have time for downtime, and your business depends on maximized worker productivity. Be sure your rugged mobile devices, wearables and other operational tech is in top shape. Ivanti Neurons for MDM provides the insights you need to keep your devices ready for today's business.

App and OS Management

Inconsistency in application updates leads to chaos and downtime. The same is true for operating system updates. Ensure a common user experience while standardizing on baseline application and OS version control. Configure Ivanti Velocity-based apps, including license server configuration and application variables to maintain peak interaction with enterprise systems. You're able to see the application performance and version information for each device in your fleet and be certain everyone has the same software versions and OS updates installed. This helps ensure performance, and reduces the risk of software incompatibilities that lead to support nightmares.

Key Benefits

- **Android Enterprise:**
  Confidence that your MDM solution aligns to the rigorous performance and usability standards, essential for rugged mobile computers in mission critical operations.

- **Continuous Security Monitoring:**
  Mobile Threat Detection is always scanning to detect and remediate known and zero-day threats, whether a device is active or docked.

- **Ready for Work:**
  See and confirm operating system and application software updates to be sure mobile devices are ready for the start of each shift.

- **Supports All Your Devices:**
  Bring Operations and IT together by securing and managing rugged mobile devices, smartphones, tablets and more in one platform.

android enterprise recommended

Don't compromise on productivity in your operations.

Learn more and get a free demo of Ivanti Neurons for MDM.

Request a Trial

ivanti

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

Kreski

Zapraszamy do kontaktu!
Więcej informacji: www.kreski.pl

1.   Gartner Magic Quadrant for UEM, 2023