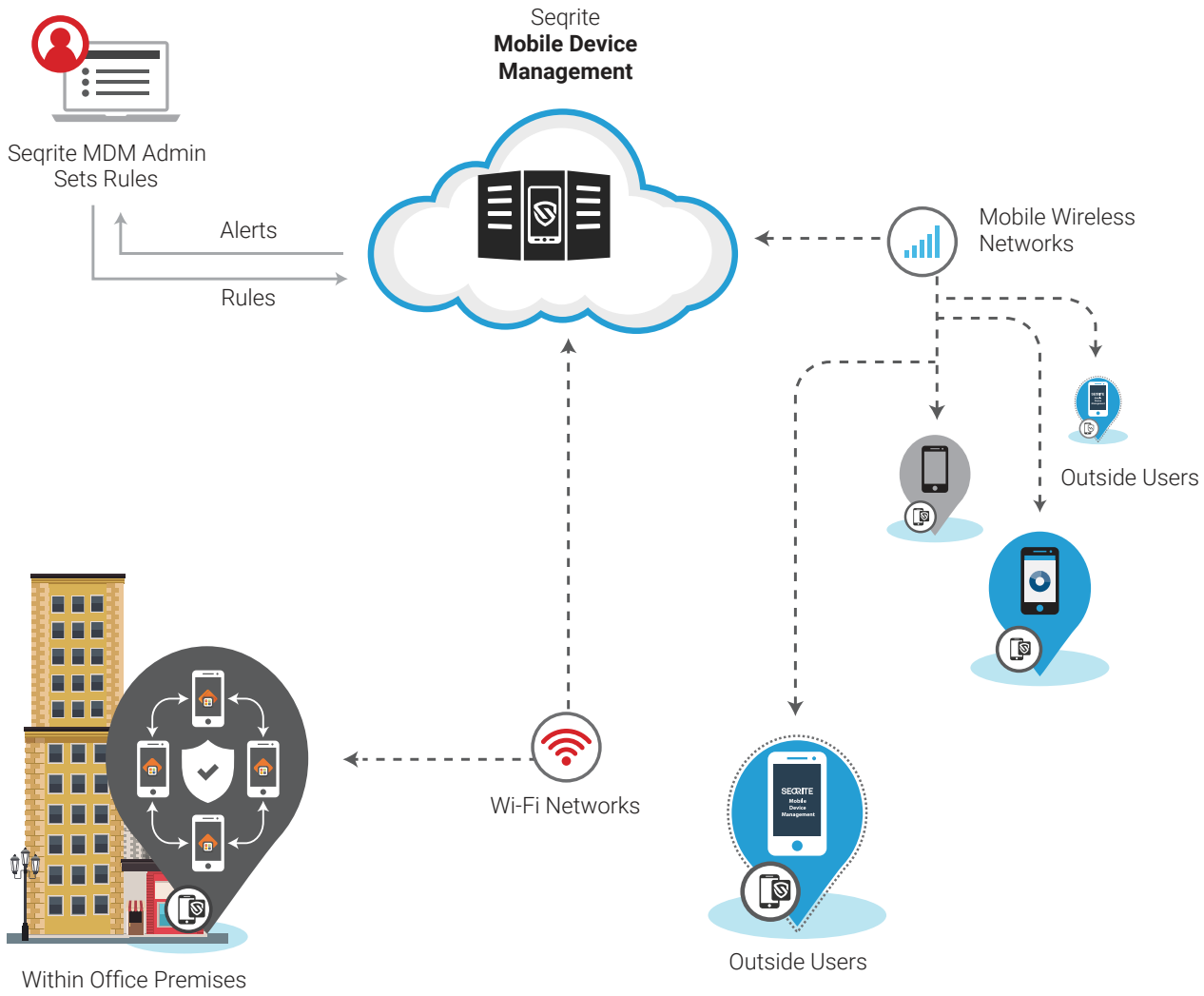
GoDeep.AI
AI Enabled Deep Predictive Malware Hunting Technology

SEQRITE

Seqrite
Mobile Device Management

Seqrite Mobile Device Management is a simple yet powerful tool to manage all your mobile devices running on Android and iOS. It allows the network manager to control the installed apps on official devices, monitor the internet usage patterns, track the device location, apply policies per location and time, and provide support through remote device control and file transfer. Our solution allows the organization to remain in total control of what's happening with its data, even beyond its network.



Supports deployment on-cloud and on-premises

Zero Day support for Android & iOS.

Real-time alerts on policy violations

Single Console Management For All Devices

- **Zero Touch Enrolment**
  Enrol devices in seconds with Zero Touch Enrolment.
- **Group Level Administrator**
  Create Group Level Admins with rights to manage members of spcific groups.
- **Role Based Administrator**
  Define role based admins providing them with customized privileges.
- **Device Grouping**
  Group devices based on departments, business functions or any other criteria. Apply policies and restrictions based on groups.
- **Location Tracking**
  Track devices in real-time; view historical location data.

App Management, Launcher and Kiosk Mode

- **App Distribution**
  Push apps (Custom apps or apps from Playstore) and updates from console to the devices.
- **App Management**
  Blacklist or whitelist apps or categories of apps.
- **App Repository**
  Publish custom apps to Enterprise Appstore. Allow users to download apps on-demand through enterprise appstore.
- **Launcher**
  Establish control over the use of apps on devices and enable configuring selected apps which are authorized for use within organization.
- **Kiosk Mode**
  Lockdown the device to single-app or multi-app kiosk mode to optimise device productivity.

Deployment & Management for Company Owned Devices

- **Dedicated Devices**
  Locked down devices for specific tasks or functions managed in kiosk/ launcher mode with only selected apps and features – reducing misuse and maximizing operational efficiency.
- **Fully Managed Devices**
  Manage all apps, settings, and usage, ensuring complete security, compliance, and a consistent user experience with full administrative control.
- **Fully Managed Devices with Work Profile**
  Hybrid model, allowing personal use while keeping work data isolated in a secure Android Work Profile - Manage only the work container, ensuring data separation, user privacy, and corporate compliance.

Fencing and Data Monitoring

- **Virtual Fencing**
  Define digital boundaries and apply restrictions on devices on the basis of Geographical location, Wi-Fi, Time. Ability to create multiple fence groups and apply policies.
- **Network Data Monitoring**
  Monitor data usage over Mobile, Wi-Fi networks. Get detailed analytics at user & device level.

Comprehensive Mobile Security And Anti-Theft

Advanced security differentiators in Seqrite MDM set it apart as a security-first MDM solution:

- **Artificial Intelligence based Anti-Virus**
  Best-in-class, built-in antivirus engine that keeps the devices safe from cyber threats.
- **Incoming Call Blacklisting/Whitelisting**
  Restricts incoming calls to only approved series or contacts, reducing distractions and preventing unauthorized communication.
- **Intruder Detection**
  Captures a photo via the front camera upon repeated failed unlock attempts, alerting users to potential unauthorized access.
- **Camera/Mic Usage Alerts**
  Monitors and notifies when the camera or microphone is accessed by any app, ensuring privacy and threat detection.
- **YouTube Monitoring**
  Restricts usage of YouTube to control non-work-related content consumption during work hours.
- **Data Breach Alerts**
  Integrates with public breach databases to alert if any enterprise email IDs have been exposed in known breaches.
- **App Lock for Sensitive Apps**
  Adds an extra layer of protection by locking selected apps behind additional authentication, safeguarding sensitive data.
- **Anti-theft**
  Remotely locate, lock, and wipe data on lost or stolen devices. Block or completely lock the device on SIM change.
- **Web Security**
  Comprehensive browsing, phishing, and web protection. Blacklist/whitelist the URLs or use category/keyword-based blocking
- **Scheduled Scan**
  Remotely schedule a scan at any time and monitor the status of enrolled devices for security risks and infections.

Reporting & Summary

- **Customized Reporting**
  Standard and custom interactive reports giving graphical summaries. Get admin activity andaction logs.
- **Scheduled Reports**
  Easily schedule automatic export of reports on a periodic basis.
- **Business-Ready Reporting templates**
  Leverage rapid readymade reporting templates to procure instant graphical summaries on-the-go.

Remote Trouble Shooting & Data Transfer

- **Remote Device Control**
  Remotely troubleshoot issues to reduce device downtime and maximize productivity.
- **Remote Data Transfer**
  Instantly transfer a variety of file types to multiple users/groups.

Feature Comparison between Standard & Advance Variant

Features	Standard	Advance
GoDeep.AI	✓	✓
Device Management	✓	✓
Application Management	✓	✓
Security Management	✓	✓
Real Time Malware Protection	✓	✓
Network Data Monitoring	✓	✓
Launcher Mode	✓	✓
Device Lockdown	✓	✓
Call & SMS Monitoring	✗	✓
Virtual Fencing (Geo, Wi-Fi, Time based)	✗	✓
Remote Device Control	✗	✓
Reporting	Basic	Custom
Historical Logs	1 month	3 months
Seqrite BYOD	Sold Separately	

Android Enterprise Silver partner

Android Enterprise Silver Partner

Seqrite MDM is now an Android Enterprise Silver Partner, recognized for product excellence, security, and performance.

SCHEDULE A DEMO!

www.seqrite.com/mobile-device-management-mdm/

SEQRITE | Quick Heal Technologies Limited
Phone: 1800-212-7377 | info@seqrite.com | www.seqrite.com | /seqrite