KNOX is Samsung’s secure mobile platform designed specifically to enhance security of the Open Source Android Project, yet retain full compatibility with Android and the Google ecosystem.

**Top Reasons Cited by CIOs for Poor Android Acceptance in Enterprise**
- Lack of Security
- Limited Manageability

**Samsung KNOX addresses CIO concerns**
- Secure Mobile Platform
- Manageability and Enterprise Enablers
- Secure App Framework/Defense Grade Security

*Gartner, Strategies to Solve Challenges of BYOD in Enterprise, 2013

**Samsung KNOX Enables Robust Enterprise Manageability**
- Remote Management
- Data Leakage Prevention
- Controls and Limits
- Monitoring
- Secure Access to Enterprise Resources
- Real-time Mobile User Support
- Enterprise Integration

**KNOX Solutions Protect and Manage Mobile Data to Secure Your Enterprise**
Samsung KNOX 2.0 Provides the Security and Manageability Enterprise IT Administrators Need

Android Platform Security
• Secure Boot/Trusted Boot – Provides boot time integrity
• TrustZone-based Integrity Measurement Architecture (TIMA) – Real time OS kernel integrity verification
• Security Enhancements for Android (SE for Android) – Implements fine grained access controls to isolate system services and 3rd party apps, while rendering rooting useless
• SmartCard Support

Powerful and Flexible Device Management
• Simple cloud-base setup and maintenance
• Manage users, apps and devices from anywhere
• Integrates with Active Directory and Microsoft Exchange ActiveSync
• Active Directory-based device management
• Dual Persona – Secure separation of enterprise and personal environments
• Ideal for both BYOD and COPE scenarios
• Per App VPN – Separates enterprise resources
• Cloud-based SSO – One set of credentials to access multiple cloud-based apps
• Supports a wide-range of devices including iOS and Android from one console
• KNOX MDM Community supports over 500 IT policies
• SDK with over 1300 MDM APIs for Developers

Defense Grade Security
• FIPS 140-2 Level 1 Certification for Protection of Data-In-Transit (DIT)
• FIPS 140-2 Level 1 Certification for Data-At-Rest (DAR)
• Approved by the US Defense Information Systems Agency (DISA) for use on Department of Defense (DoD) networks*
• CommonCriteria Certification

AOSP vs. Samsung KNOX Workspace:
KNOX: Multi-layered Security from Hardware to Software

Samsung KNOX Meets Enterprise IT Security Needs

<table>
<thead>
<tr>
<th>Enterprise Need</th>
<th>KNOX MDM Policy Groups**</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Management</td>
<td></td>
</tr>
<tr>
<td>Applications Management</td>
<td>Email Accounts</td>
</tr>
<tr>
<td>Password</td>
<td>Certificate Management</td>
</tr>
<tr>
<td>Dual Persona</td>
<td>Container Firewall</td>
</tr>
<tr>
<td>Camera Restriction</td>
<td>Integrity Management</td>
</tr>
<tr>
<td>Container Management</td>
<td>Applications/</td>
</tr>
<tr>
<td>Controls and Limits</td>
<td>Container Permissions</td>
</tr>
<tr>
<td>Monitoring</td>
<td>Integrity Monitoring</td>
</tr>
<tr>
<td>FIPS IPSec VPN</td>
<td>Per-app VPN</td>
</tr>
<tr>
<td>Application</td>
<td>Exchange Account</td>
</tr>
<tr>
<td>Real-time Mobile User Support</td>
<td>Remote Control</td>
</tr>
<tr>
<td>Enterprise Integration</td>
<td>Cloud-based SSO</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Excluding certain features.

**Availability of Samsung KNOX features may vary by MDM partner.