CASESTUDY



SECURED **MOBILE COMMUNICATION** WITH ASSOCIATED CENTRALISED **DEVICE MANAGEMENT AND SECURITY SOLUTIONS**



THE CLIENT

The Defense Sector client is the vanguard of national security entrusted with safeguarding the nation's sovereignty. Its unwavering commitment to protecting citizens and borders underscores its paramount importance.

Operating in a dynamic landscape of evolving threats, the Defense Sector requires communication systems that are not only robust but impregnable.

With security at its core, this sector seeks MASL's expertise to fortify its mobile communication devices and solutions.

As a custodian of the nation's defense, the client's partnership with MASL signifies the fusion of cutting-edge technology with strategic vigilance.

THE CHALLENGE

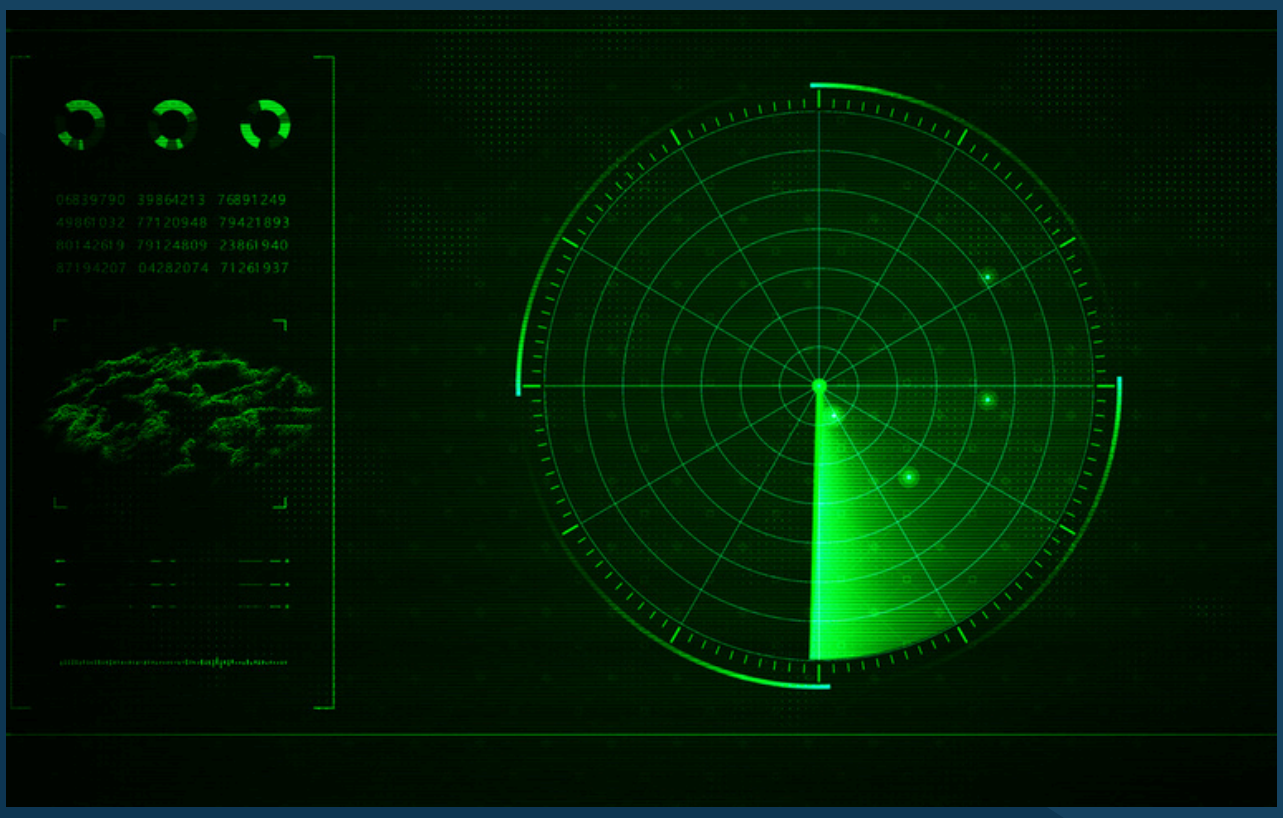
In embarking on the project objectives Millennium Automation Private Limited (MASL) confronts a spectrum of challenges head-on, each demanding innovative solutions to ensure the success of this endeavor.

Enhanced Security:

- The Defense Sector's communication demands are uniquely sensitive. MASL is tasked with designing a comprehensive security ecosystem that shields communication from advanced cyber threats, ensuring data integrity and confidentiality across all levels.

Diverse Device Management:

- Coordinating a fleet of high-end and low-end mobile devices requires a dynamic approach.
- MASL must implement a Mobile Device Management (MDM) solution that caters to the diverse functionality of these devices while maintaining centralized control.



Complex Integration:

- The amalgamation of various hardware and software components is intricate. MASL faces the challenge of seamlessly integrating Mobile Device Management, Data Security Solutions, Antivirus Solutions, and more, ensuring a unified and cohesive communication ecosystem.



Real-time Updates:

- Over-the-air (OTA) solution deployment poses a challenge in ensuring uninterrupted and secure patch updates for the Android Operating System and SIM configurations while maintaining redundancy to minimize disruption.



End-to-End Encryption:

- The Defense Sector demands top-notch encryption to secure communication. MASL must establish end-to-end encryption measures encompassing data in transit and data at rest, spanning a wide range of file formats and applications.

Long-Term Maintenance:

- As a partner entrusted with the defense sector's communication infrastructure, MASL must provide reliable and continuous operation and maintenance services for five years, including patch updates, software upgrades, and application redevelopment.

THE SEARCH

The organization soon realized they needed a Best-in-Breed Solution. A vendor who specializes in IT Infrastructure and Technology. In the search process for the right vendor, they finalized MASL primarily because they found us the best IT infrastructure company with proficiency for esteemed clients in various Industry Verticals.





SCOPE OF WORK

- Integration of perpetual device management solutions into smartphones at OEM factories.
- Deployment of MDM in DO Mode at buyer's premises, seamless integration with LDAP and IAF certificate authorities.
- Advanced device setup, security features, and centralized configuration management.
- Deployment of a Centralized Antivirus Solution with 150,000 node licenses for real-time device protection.

- Web-based dashboard for real-time monitoring, compliance control, and incident response.
- VPN implementation with SSL and IPsec, compatible with Android 11.0 and above.
- Integration with third-party encryption libraries, RADIUS/DIAMETER protocols, and secure file sharing.
- Data protection measures, including AES 256-bit encryption for data at rest and end-to-end encryption for files.





THE SOLUTION

By addressing these challenges, MASL demonstrates its prowess in orchestrating a complex symphony of technology and security, proving its commitment to delivering a resilient and secure cellular communication solution for the Defense Sector.

MASL's innovative approach to addressing the challenges of a secure communication platform through Android phones led to the implementation of robust solutions in Mobile Device Management (MDM), Data Security, and Antivirus protection.

Custom Binary (C-Binary):

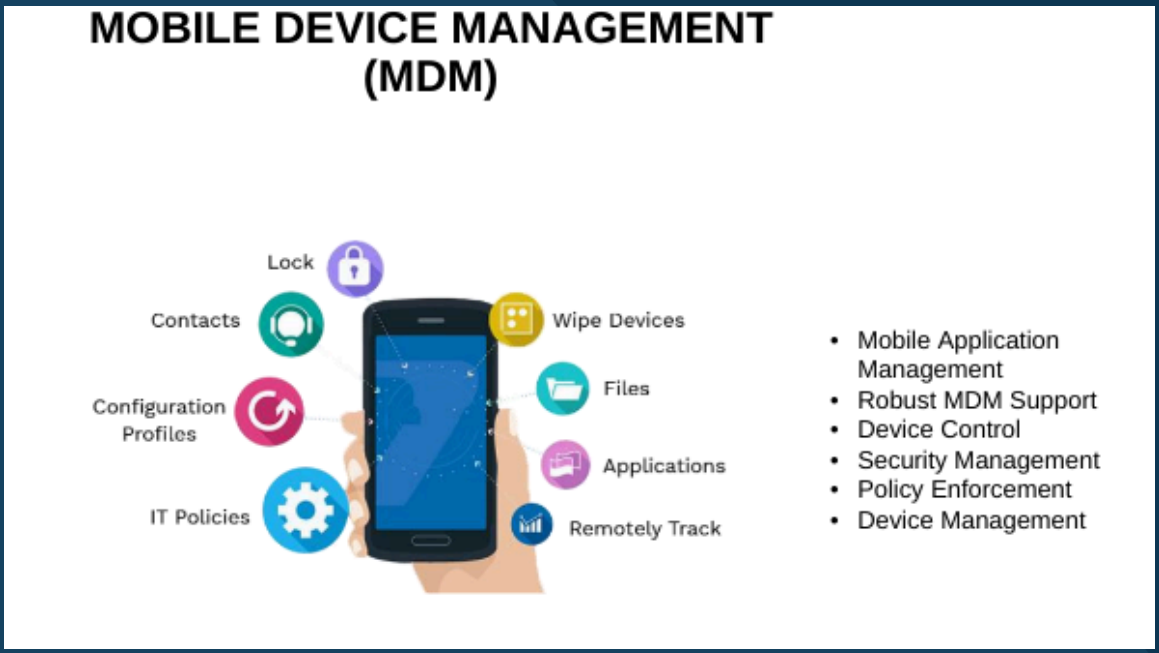
- Custom Binary (C-Binary) is a specific firmware that is a customized binary that includes specialized customer's requirements such as Network Settings, Additional features, Boot logo and wallpaper, Kiosk mode settings, and Customized app preload.



Mobile Device Management (MDM):

- MASL collaborated with handset OEMs to ensure that smartphones came bundled with a perpetual device management solution. This solution was deployed at the OEM factory premises.

- MDM clients were enrolled and deployed in device owner mode (DO Mode) at the buyer's premises before joining the AFCEL network.



- The MDM solution seamlessly integrated with existing LDAP and IAF certificate authorities, supporting the grouping of devices based on organizational hierarchy and various admin levels. It facilitated the movement of devices between user groups without enrollment.

- MASL's MDM solution enabled extensive device setup and security features such as advanced passcode restrictions, partial and complete wipes, compliance enforcement, access to security logs, turning off debugging, and more.

- The solution allowed centralized configuration management, network settings control, system audio settings, and specific permission requests for various apps and services.

- Advanced features included capabilities like enforcing GPS, remotely rebooting devices, managing system settings, and integrating with VPN solutions.

- Customized policies could be scripted and applied to devices for specific actions, ensuring tailored security and management.

Data Security Solution (DSS):

- VPN solutions were implemented with support for Secure Socket Layer (SSL) and Internet Protocol Security (IPsec), compatible with Android 11.0 and above.
- AES 256-bit encryption and RSA 4096 authentication were used for secure VPN connections.
- Integration with third-party encryption libraries and RADIUS/DIAMETER protocols provided additional security layers.
- Data at rest was safeguarded with AES 256-bit encryption, multiple volume creation, and secure file sharing.
- End-to-end encryption for files, e-signature image storage, and passcode protection ensured comprehensive data security.



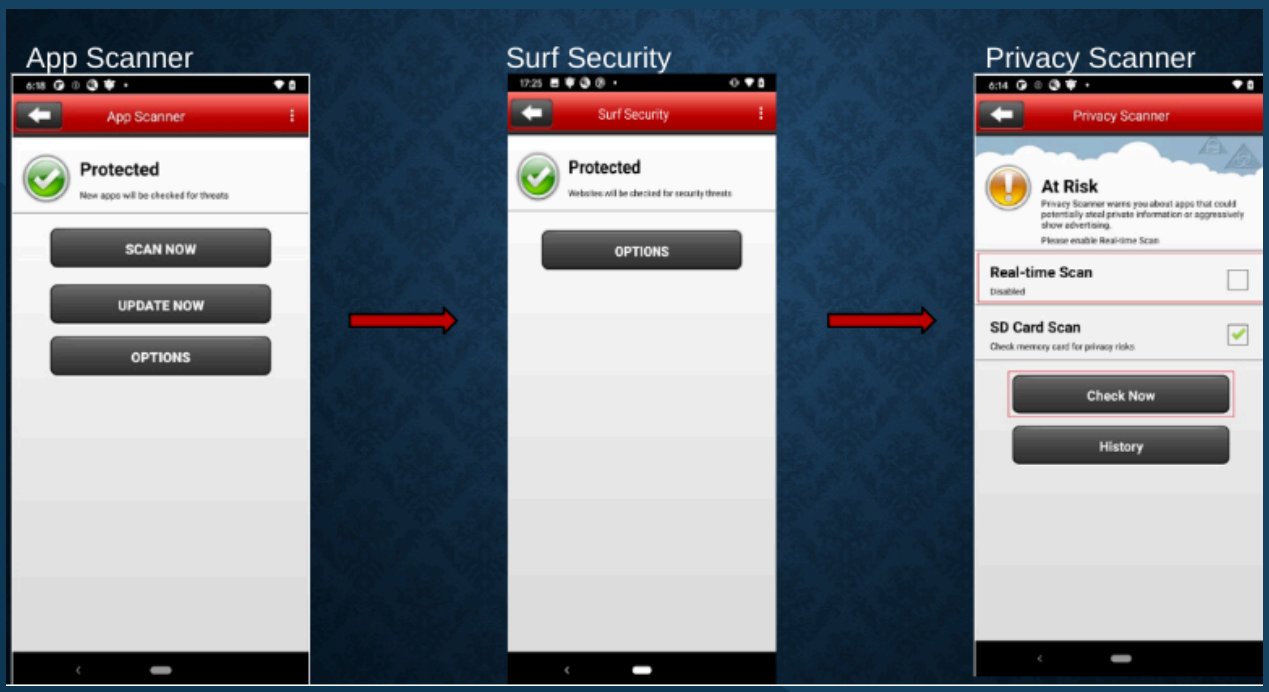
TrendMicro Antivirus (AV) Solution:

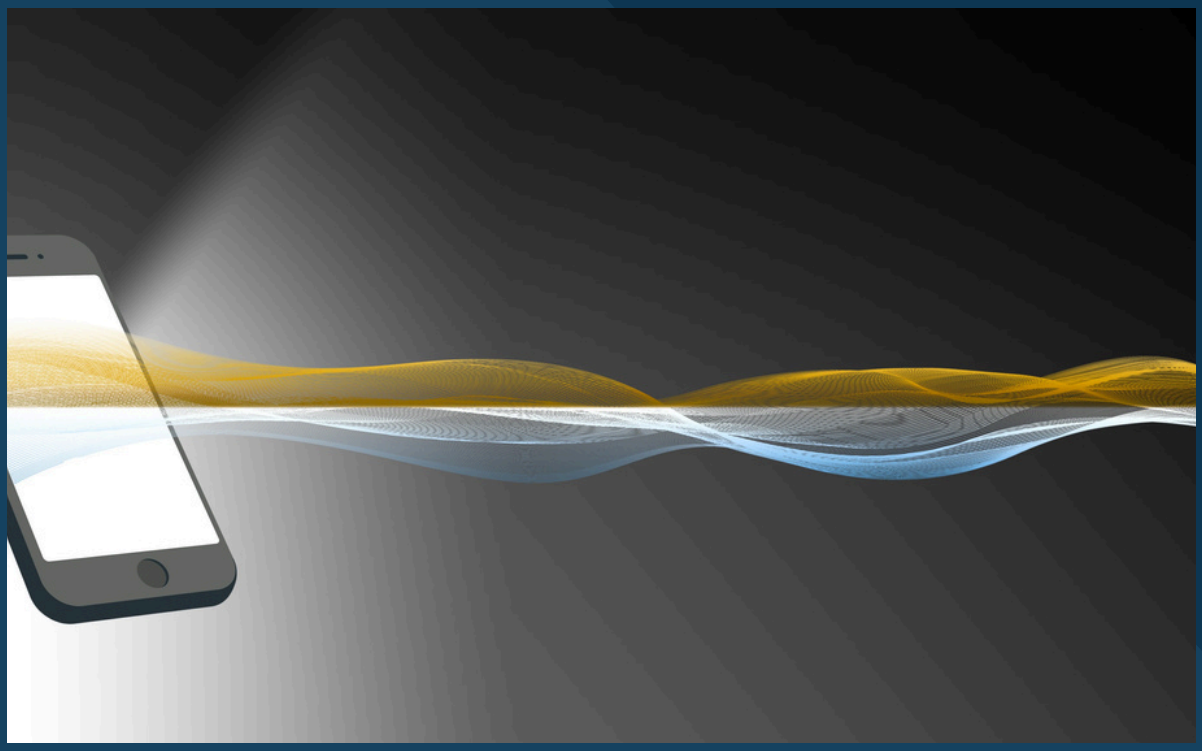
- MASL deployed a Centralized Antivirus Solution with 150,000 node licenses to protect mobile devices.

- The solution was meticulously installed, configured, and maintained on all handsets connected to the network, ensuring real-time protection.

- The AV solution covered features such as malware detection, web reputation services, network attack detection, and data encryption.

- Centralized management provided a web-based dashboard for real-time monitoring, compliance control, and incident response.





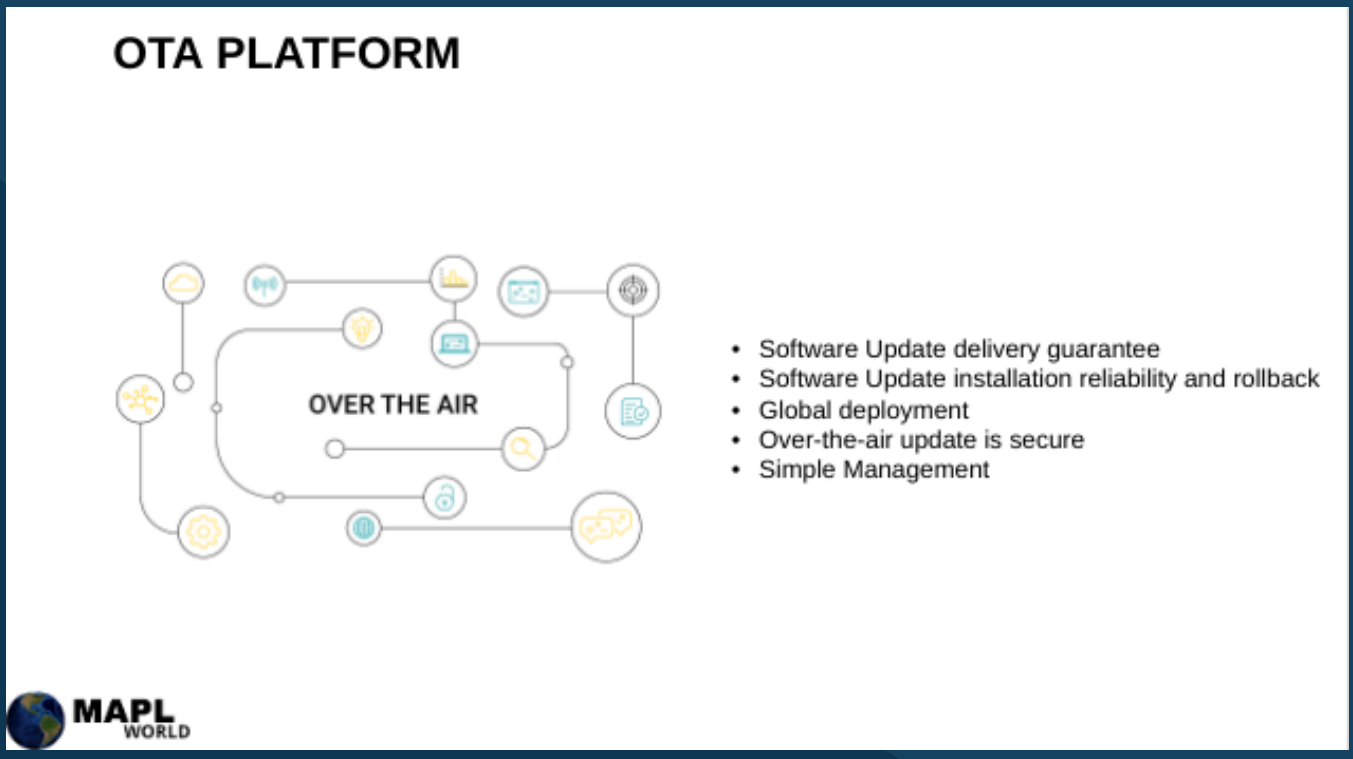
- The AV solution actively scanned installed applications and files, supporting real-time scanning during installation.
- Machine learning algorithms aided in identifying unknown and zero-day threats.
- Centralized management extended to policy violation logs, event logs, and compliance criteria enforcement.
- The solution supported integration with the MDM system, enhancing overall security and device management.

OTA Solution:

MASL's OTA Solution stands as a pinnacle of reliability and security. It guarantees the prompt and secure delivery of software updates to devices regardless of their geographic dispersion.

The solution provides administrators the flexibility to remotely control and update the Operating System version on mobile devices without end-user interaction and ensure the latest security patches are immediately deployed to every device. Also, over-the-air solutions shall enable administrators to configure and update the SIM modules included in the mobile equipment.

This solution not only ensures that updates are efficiently deployed but also prioritizes the reliability of the installation process. In the event of any complications, a robust rollback mechanism ensures uninterrupted device operation.



THE OUTCOMES



Data Protection:

- The Data Security Solution (DSS) ensured robust data protection in transit and at rest. Encryption mechanisms and secure file-sharing features safeguarded sensitive information from unauthorized access and breaches.

Proactive Threat Prevention:

- The TrendMicro Antivirus solution was crucial in proactive threat prevention. It scanned applications, files, and network traffic in real-time, detecting and blocking malware, malicious applications, and potential security breaches. Machine learning algorithms enhanced threat detection capabilities.

Compliance Enforcement:

- Administrators enforced security policies, including passcode policies and network settings, ensuring devices adhered to organizational security standards.

Enhanced Device Usability:

- MASL's solutions balanced security and usability, offering customization options for user experiences, branding, and lock screen messages.

Incident Response and Reporting:

- The solutions provided incident response tools, including diagnostic tools in MDM and a centralized dashboard for analysis, reporting, and alerts.

Real-time Monitoring:

- The centralized management dashboard enabled real-time monitoring of device health, compliance, and security events for prompt responses to incidents.

Cost and Resource Optimization:

- The Defense Sector optimized costs and resources with centralized management, reducing manual interventions and enhancing operational efficiency.







"Transform your business with our proven solutions and elevate to new heights".

GET IN TOUCH !

+91 93112 40651

www.maslworld.com

info@maslworld.com

E 48/9,Okhla Phase-II
New Delhi 110020