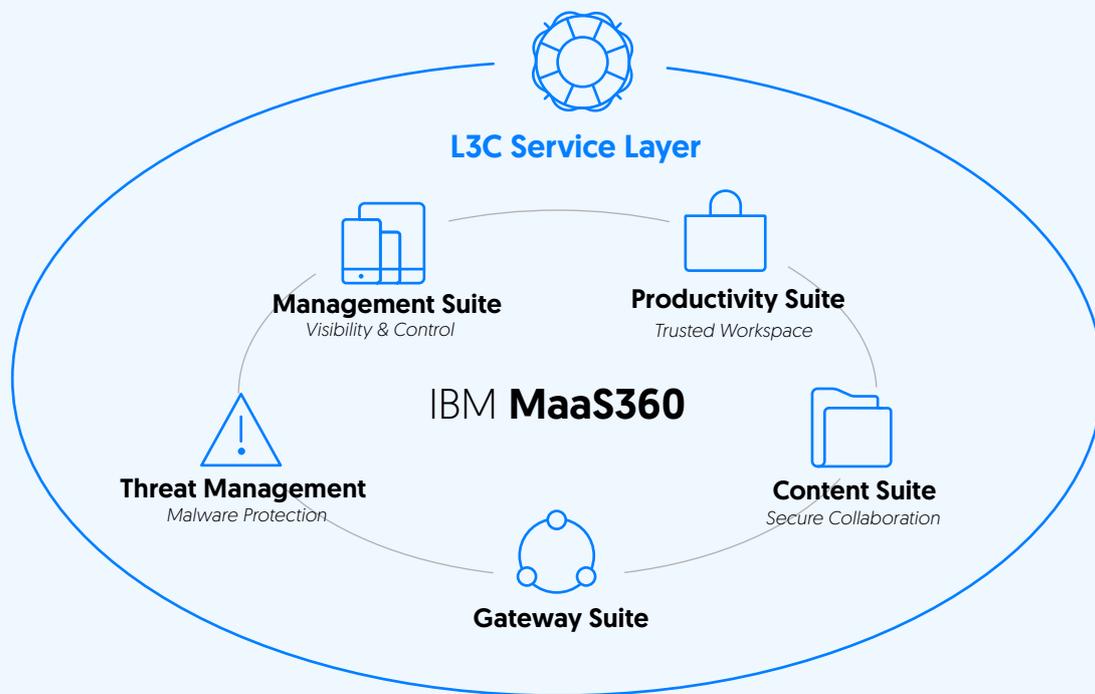# L3C Enterprise Mobility Management

Empower your workforce while securely managing your devices, apps and content.

L3C Enterprise Mobility Management utilises IBM's MaaS360 solution to provide a secure and comprehensive EMM platform to quickly and seamlessly deploy devices, deliver applications and enable secure content collaboration on BYOD or corporate owned devices allowing:

- ✓ Enhanced security and compliance
- ✓ Better employee productivity
- ✓ Reduced cost of supporting mobile apps

L3C Service Layer

Management Suite
Visibility & Control

Productivity Suite
Trusted Workspace

IBM **MaaS360**

Threat Management
Malware Protection

Content Suite
Secure Collaboration

Gateway Suite

Deploy and manage devices and apps

IBM MaaS360 Management Suite integrates mobile device management (MDM) and mobile application management (MAM) giving IT centralized policy control and the ability to deploy an enterprise app catalog giving users easy access to work information. With support for multiple operating systems, including iOS, OS X, Android and Windows, MaaS360 provides the flexibility to choose the right devices, models and platforms for business. MaaS360 also provides a seamless way to securely connect with existing enterprise infrastructure, including Microsoft Exchange, Office 365, Lotus Traveler, Gmail, Active Directory/LDAP and Certificate Authorities. Integration with other leading enterprise infrastructure solutions are provided through a robust set of APIs.

Enable secure productivity

IBM MaaS360 Productivity Suite combines an easy to use set of work tools with complete containment for email, attachments, apps and web content. By separating work and personal data, the trusted workplace reduces security risks and prevents data leakage. Users can safely navigate the web via the IBM MaaS360 Secure Mobile Browser, which allows IT to provide access to intranet sites and restrict specific URLs or categories deemed inappropriate for work. This module is also available as a standalone solution without enrolling devices in MDM.

Secure access to mobile content

Users need a quick, easy and safe way to access, modify and sync files. IBM MaaS360 Content Suite provides a protected container for distributing, viewing, creating, editing and sharing documents on mobile devices. It includes access to distributed content and cloud repositories such as Microsoft Share-Point, Box, OneDrive and Google Drive. Content can be pushed to authenticated devices or made accessible to users via a corporate document catalog. Managed documents in the Content Suite can be contained to prevent the loss of sensitive data.

Seamless access to behind-the-firewall resources

Mobile connectivity to resources such as Share-Point, Windows File Share, intranet sites and app databases is crucial for organizations seeking to maintain organizational connectivity—but information security remains a top priority. IBM MaaS360 Gateway Suite makes it possible to access these resources from smartphones and tablets without requiring a VPN session, simplifying user connectivity to corporate resources while keeping the data safely contained.

Defend against advanced mobile threats

The proliferation of smartphones and tablets in the workplace has had a consequential impact on the number of mobile malware attacks and incidents. Powered by IBM Trusteer®, IBM MaaS360 Mobile Threat Management provides IT with a means to detect advanced mobile threats before they have a chance to impact data security. The solution helps organizations safely and securely support BYOD and corporate devices through proactive monitoring and automated remediation capabilities—with functionality made available directly from the EMM console.

Implementation assistance and support

L3C can assist with implementation and provides ongoing support with a service desk for your authorised support staff.

Total enterprise mobility

- ✔ Support for all major platforms including iOS, Android, Windows and OS X
- ✔ OTA device configuration
- ✔ Automated compliance and rules enforcement engine
- ✔ Selective/full wipes of compromised devices
- ✔ Integrate with existing enterprise systems

A secure approach to BYOD

- ✔ Enforce security policies
- ✔ Detect jailbroken/rooted devices
- ✔ Restrict taking screenshots, copying, pasting and sharing to prevent data leaks
- ✔ Uphold app secutiry through authentication enforcement, blacklisting and whitelisting
- ✔ Block website access based on content categories or domain name

On-the-go productivity

- ✔ Deliver apps and track installation across users, groups or devies
- ✔ Use the enterprise App Catalog for third-party and in-house apps
- ✔ Store, view and share content from container
- ✔ Securely view, edit and share documents via content repositories
- ✔ Enable secure mobile access to corporate data and intranet sites without using the device's VPN

Delivered from IBM Cloud

By utilising IBM's Maas360 as part of L3C's EMM solution we deliver the service from IBM Cloud. Additionally, L3C can help integrate into your on premise infrastructure as well as providing additional hybrid cloud services through L3C cloud.

IBM MaaS360 is mature, proven and secure and complies with AICPA SOC-2 TypeII, FISMA, FedRAMP and FIPS 140-2 regulations. While L3C are certified for ISO27001:2013 (Information Security Management), ISO2000-1:2011 (IT Service Management) and ISO9001:2015 (Quality Management System), giving you an ideal combination to have a fast and cost effective way to meet new business challenges.

Maintaining End User Privacy

L3C EMM with IBM MaaS360 does not compromise end user privacy. Our solution CANNOT view:

- Emails, calendars, contacts
- User passwords or credentials for any app
- Data on any app on the device, app logs
- Stored pictures, Facebook and other social media
- Network traffic and browsing behaviour such as web pages visited
- Documents and eBooks

Additional, the location of the device can only be seen by your company administrators with explicit permission of the end user.

Therefore, we do not read or have access to any end user data such as emails, documents and app data. Emails do not flow through MaaS360 but continue to flow directly from your email server to your devices.

L3C EMM with IBM MaaS360

Doesn't impact the end-user experience

Is the ideal balance between flexibility and security for the mobile workforce

Protects email and other corporate data on mobile devices without negatively impacting your staff

A complete solution – available in predefined packages

While some elements are available 'a la carte' the most efficient way to deploy is by utilising pre-defined packages all wrapped with L3C service and support.

Solution	Management Suite	Productivity Suite	Gateway Suite	Content Suite	Threat Management
Mobile Device Management Smartphones, tablets and laptops	✓				
Mobile Application Management	✓				
Container App		✓			
Mobile Expense Management	✓				
Secure Mobile Mail		✓			
Secure Mobile Chat		✓			
Secure Mobile Browser		✓			
Gateway for Browser			✓		
Mobile Content Management				✓	
Gateway for Documents			✓		
Mobile Application Security		✓			
Gateway for Apps			✓		
Mobile Identity Management				✓	
Mobile Document Editor				✓	
Mobile Document Sync				✓	
Mobile Threat Management					✓

Let us discuss how L3C EMM can empower your people, reduce the cost of supporting mobile applications while enhancing your security compliance.

info@l3c.cloud
0203 542 0870 (Jerry Crossfield)