MDM +
advanced mobility

PRODUCT BROCHURE

#becrypt

MDM+ - *THE FIRST MDM PLATFORM COMPATIBLE WITH DEEP PACKET INSPECTION AND SECURE MDM SERVER HOSTING.*

MOBILE DEVICE MANAGEMENT (MDM) SERVER - *AN ORGANISATION'S UNRECOGNISED CROWN JEWELS.*

As the sophistication, capacity and business reliance on smart devices has increased, so has the significance of potential compromise of either the mobile device management platform or smart devices themselves. Imagine an adversary geo-locating your executives, and being able to unlock their device, extract data or change device settings!

Organisations, particularly those subject to the more sophisticated cyber-attacks, face this unfortunate risk today as a result of the constraints that popular smart device ecosystems impose. High-value MDM Servers tend not to reside in the well-protected segments of organisations' networks, due to the nature of required connectivity to the global smartphone infrastructure.

Developing MDM standards

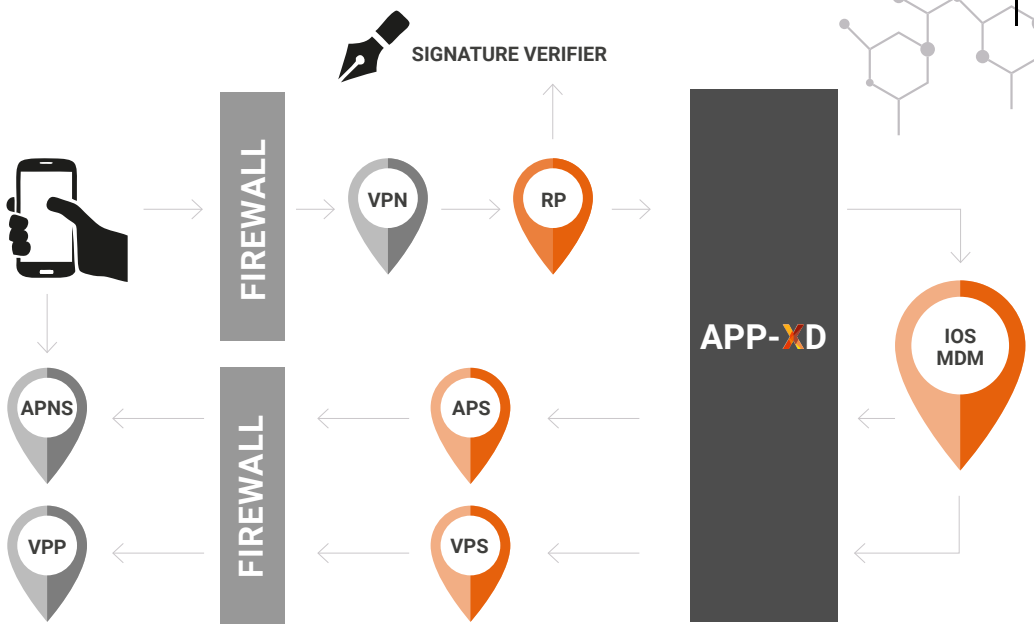
Unwilling to accept this risk, the UK National Cyber Security Centre (NCSC) and international partners have supported the development of standards that allow MDM Servers to be hosted in secure well-protected network segments, sufficiently isolated from internet-related threats. The architecture enables network packet inspection of MDM traffic. Packet inspection has become an important tool for security conscious organisations - providing cyber network defence teams visibility of attacks and data egress. However, common MDM platforms are incompatible with network inspection tools, given the imposed protocol and architectural constraints, rendering organisations more susceptible to both attack and undetectable data egress.

Becrypt – Your Trusted Advisor

Becrypt has worked closely with NCSC to support the enhanced security characteristics of the Advanced Mobile Solutions programme, resulting in the first MDM platform compatible with Deep Packet Inspection and secure MDM server hosting. Becrypt's MDM+ solution has been deployed to protect government and corporate networks, allowing active defence against sophisticated and persistent adversaries. MDM+ offers enterprise scale intuitive management of devices such as Apple iPhones, while remaining transparent to the users.

Through NCSC collaboration, Becrypt has implemented an architecture compatible with standard network defence tools, such as Web Application Firewalls. Based on a novel split-architecture approach, MDM+ allows the management server to be hosted within a secure network, appropriately segmented from a DMZ within a 'walled-garden' network architecture. The split architecture allows proxy server components to deliver scrutinisable network traffic for packet inspection within the DMZ or robust protocol validation via a Cross Domain Solution.

ACRONYM	DESCRIPTION
APNS	Apple Push Notification Service - used by MDM and other server applications to contact devices
APS	APNS Proxy service, this acts as a TLS initiator and authenticator to the APNS
MDM	Mobile Device Management
RP	Reverse Proxy (and TLS terminator) - used to ensure all externally originated data is unencrypted and capable of inspection.
VPN	Virtual Private Network terminator
VPP	Apple Volume Purchase Program - controls the assignment of previously purchased applications to devices
VPS	VPP Proxy Service - simplifies the communication between MDM and VPP across the WAF
APP-XD	APP-XD is Becrypt's API centric High Assurance Cross Domain Solution



The best of both worlds

MDM+ is available as a Cloud Hosted solution, or on premise. MDM+ is part of Becrypt's High Assurance product offerings including Paradox, the security-focused operating system for accessing cloud and online applications.

Security

From a security perspective, MDM+ is the only MDM platform that allows MDM server hosting on the network 'high-side'.

It enables deep packet inspection of network traffic and is compatible with Web Application Firewalls and Cross Domain solutions.

MDM+ delivers comprehensive centralised management of device policies, certificates and security events.

Functionality

MDM+ supports native smartphone experience meaning that users are unaware of additional security.

A functional equivalence to common MDM platforms through native platform MDM API.

Available as Cloud-hosted service or on premise.

It has a Flexible Docker-based split proxy architecture.

#becrypt

WHY BECRYPT?

With a heritage of creating National Cyber Security Centre-certified products, Becrypt is a trusted provider of endpoint cybersecurity software solutions. Becrypt helps the most security conscious organisations to protect their customer, employee and intellectual property data. It has an established client base which includes governments (central and defence), wider public sector, critical national infrastructure organisations and SMEs.

As one of the early pioneers in device encryption software to today being first to market with a unique desktop operating system, Becrypt continues to bring innovation to endpoint cyber security technology. A recognised cyber security supplier to the UK government, Becrypt's software also meets other internationally accredited security standards. Through its extensive domain and technical expertise, Becrypt helps organisations optimise the use of new technologies and its MDM platform delivers the security required for the modern age.

GET IN TOUCH

If you would like to find out more about MDM+, please contact us on:

0845 838 2080

View us on: becrypt.com

Follow us on: @Becrypt

Support us on: Becrypt

Address: Becrypt Ltd, Albion House, 55 New Oxford Street, London WC1A 1BS, United Kingdom