Technical Product Overview

Becrypt **MDM+**

High Assurance Secure Mobile Solutions

Becrypt MDM+ is the first Mobile Device Management (MDM) platform compatible with deep packet inspection and secure MDM server hosting.

Built with UK Government

HM Government

becrypt

Becrypt **MDM+**

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.

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 MDM+ has been deployed to protect government and corporate networks, allowing active defence against sophisticated and persistent adversaries. Becrypt MDM+ offers enterprise scale intuitive management of devices such as Apple iPhones, iPads and Google Android devices, 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, or APP-XD - the next generation API based high assurance cross domain gateway. Based on a novel split-architecture approach, Becrypt 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.

The best of both worlds

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

Security

From a security perspective, Becrypt 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.

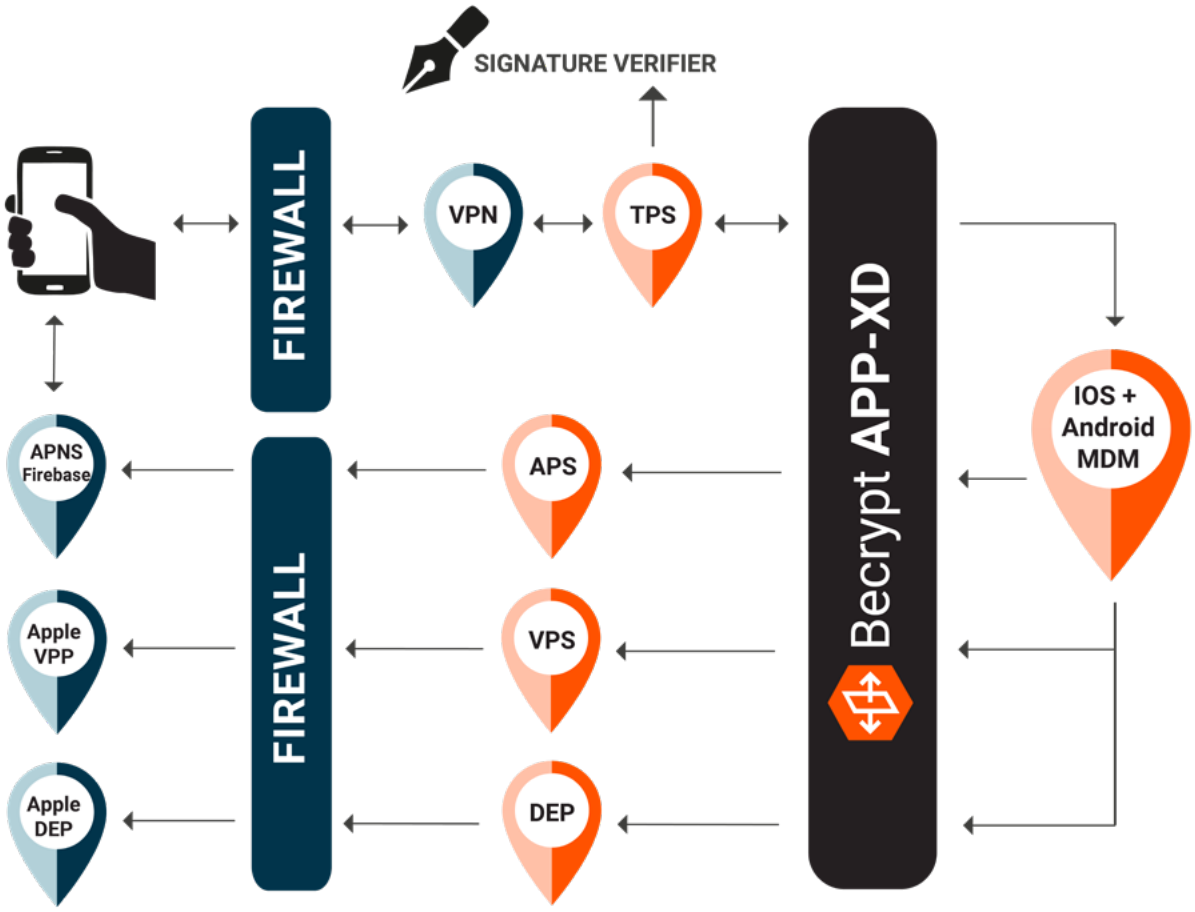
Functionality

Becrypt 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.



Acronym	Description
APNS	Apple Push Notification Service - used by MDM and other server applications to contact devices
APS	Push Notification Proxy service, this acts as a TLS initiator and authenticator to the APNS and/or Firebase Cloud Messaging services
MDM	Mobile Device Management
TPS	Translation Proxy Service is a Reverse Proxy (and TLS terminator) - used to ensure all externally originated data is unencrypted and translated ready for inspection.
VPN	Virtual Private Network terminator – an optional component in this architecture
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 APP-XD Gateway or WAF
DEP	Apple Device Enrolment Programme – simplifies the process for organisations to deploy and manage Apple Devices
DPS	DEP Proxy Service – brokers the connection between the MDM and Apple business manager
APP-XD	Becrypt APP-XD is Becrypt's API centric High Assurance Cross Domain Solution

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 the Becrypt MDM+ platform delivers the security required for the modern age.

Find out more about Becrypt

Call us: 0845 838 2080
Email us: info@becrypt.com

View us on: becrypt.com
Follow us on: @Becrypt
Support us on: Becrypt
Follow us on: Becrypt_Ltd

becrypt