Data Resolve

mobsec™

EMPOWER YOUR ORGANIZATION WITH MOBILE WORKFORCE MANAGEMENT

www.dataresolve.com

MobSec Business

Companies worldwide deal with huge volumes of information including customer data, customer billing information and information related to the business of the company itself. Business critical data is generated at almost every organizational endpoint which continues to stay unprotected against malicious activities such as theft, unauthorized share, copy and transfer to a different location, etc.

With the continuously increasing use of smartphones and tablets to access corporate data, it becomes very important to prevent data leak through any possible channel or medium. MobSec provides an effective solution addressing the challenges of data loss prevention, device management and employee productivity monitoring

Why Mobile Workforce Management?

- To make Enterprise mobility work and to turn business opportunities, mobile access to vital resources is required. Mobile Workforce Management (MWM) is required to protect the corporate assets used on mobile devices
- The devices required to manage may be out of physical reach, but they don't have to be out of touch. With MWM, it is possible to manage everything users need to be productive and gain secure access through mobile devices
- MWM can control the insider data leakage scenarios and log such events on the basis of company specific policies
- For proactively tackling insider threats, monitoring employees digital activities like browsing (search engine, application usage, email activities) and device activities can provide insights about intention

How MobSec can help?

MobSec uses the concept of Cyber Intelligence extended to the mobile device paradigm as a unique approach towards reducing the business risks of a company through intelligent analysis of the information flowing within and outside the company and providing the following capabilities:-

Mobile Device Management

- Monitor and control device settings and features, including but not limited to:
  - Device rooting detection
  - Enforce device level encryption
  - Device online / offline
  - Location tracking
  - Last connected time
- Device configuration and applications monitoring
- Application Whitelisting/Blacklisting
- Wi-Fi profile management
- VPN profile management
- Support for offline policies and offline monitoring
- Remote wipe
- Password reset
- Enabled storage encryption
- Disable wifi
- Disable bluetooth

- Lock device
- Disable camera
- ***Disable USB***
- ***Disable GPS***
- Password protection enforcement
- Device Enrollment
- Geo Fence Policy
- ***Kiosk Mode***
- Device Monitoring Policy (Call, SMS, Web browser, Location tracking, Environment monitoring)

Mobile Application Management

- Application inventory tracking
- ***App whitelisting/blacklisting***

Data Security

- All encompassed applications (MobSec VPN, MobSec Sheet, MobSec Browser, MobSec Vault)
- Secure business apps (MobSec Editor, MobSec Gallery, MobSec Docs and MobSec Mail)

- Email Activity monitoring
- Geo-fencing and Time fencing
- Connected peripherals monitoring
- ***Extended Android APIs support***
- Profile based monitoring

Employee Productivity Monitoring

- Call Activity Monitoring (inbound and outbound)
- SMS Activity Monitoring (inbound excluded)
- Real Time Location Tracking
- Environment Monitoring (Wi-fi, Flight Mode, Bluetooth, GPS Monitoring)

Cyber Intelligence

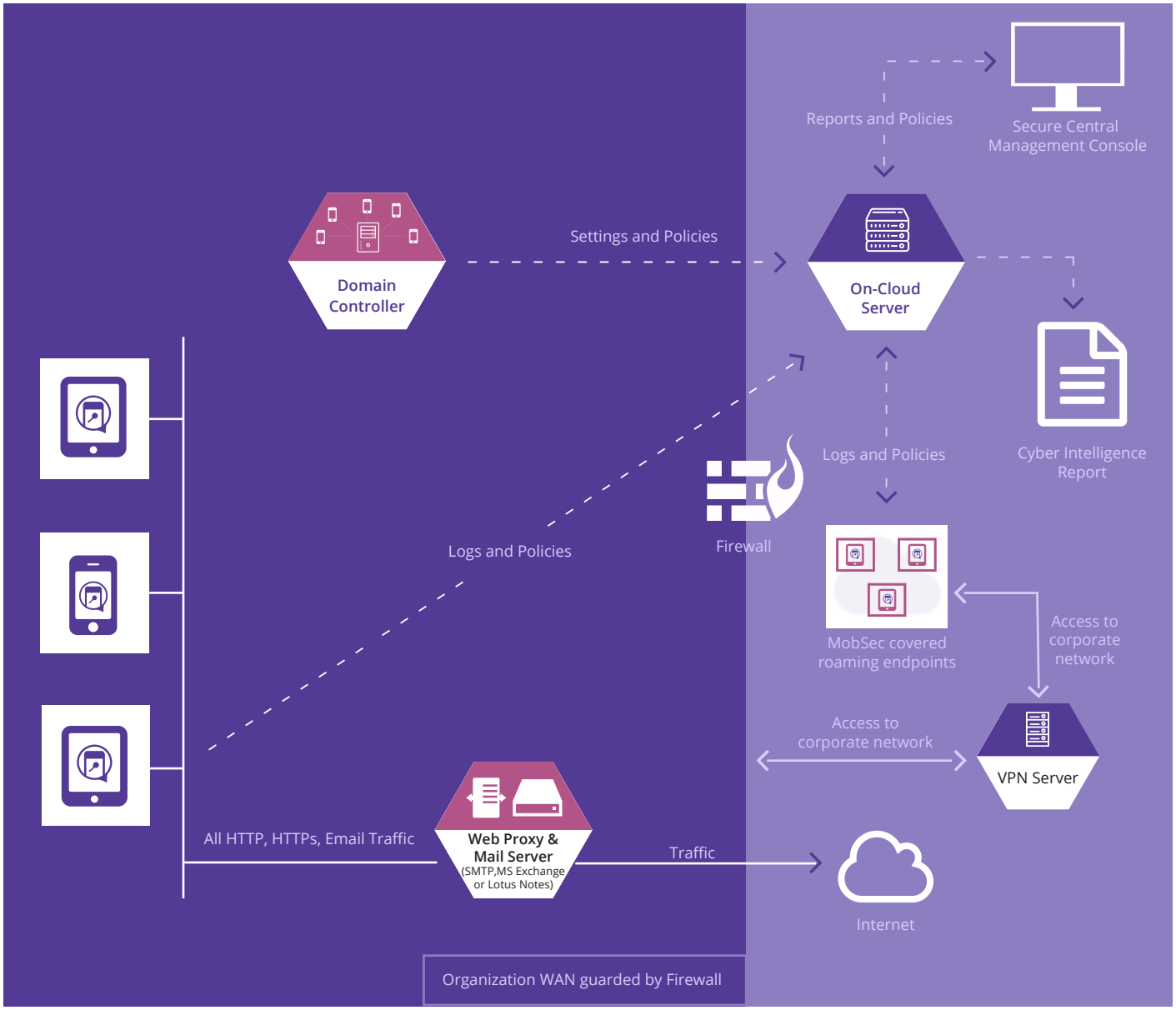
- Comprehensive incident reporting and analytics sections to provide the customer an overview of various activities occurring on the covered mobile endpoints
- Easy export of reports for offline viewing in PDF format

*Capabilities marked with * are supported only for Samsung Knox based devices*

MobSec Business-Deployment Model

On-Cloud

The MobSec on-cloud server is recommended for small businesses having either a network at one single location or offices spread across multiple cities.

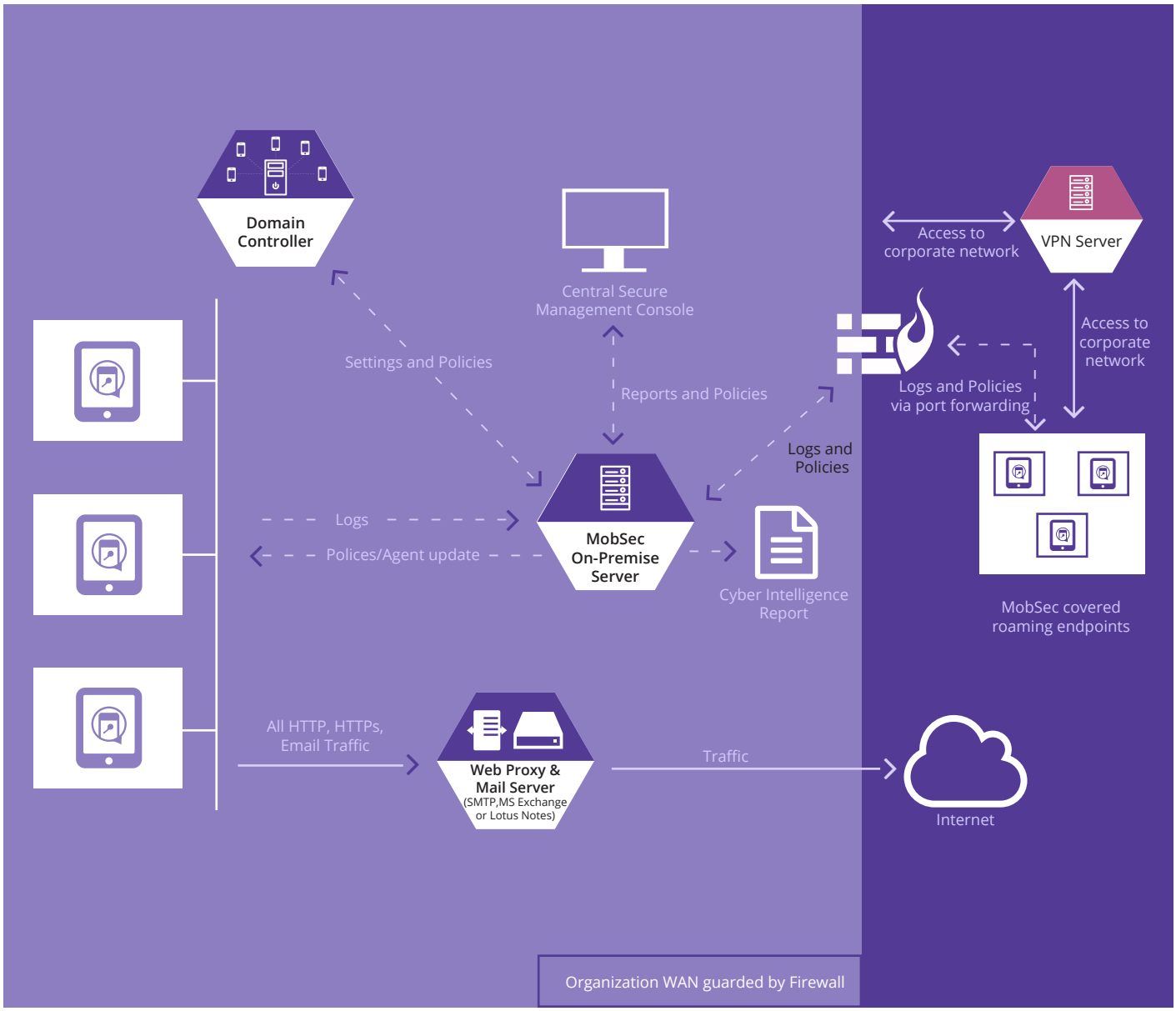


mobsec™ **On-Cloud Server**

The server resides on our secure data centres which gives the organization an advantage of not hosting their own server within the network and just install the agents on the devices that needs be protected

On-Premise

The MobSec on-premise server can be either a dedicated server within the organization's office premises or an online server hosted and managed by the vendor.



Corporate VPN/Internal Network mobsec On-Premise Server

The above diagram shows how MobSec can be deployed in a typical business network with offices located at multiple locations with a set of users travelling outside.

System Requirements

MobSec Server Requirements

The configuration of the MobSec Business server depends on the number of systems you need to protect. For example, an organization with up to 300 systems to be protected can be supported by a dedicated server with:

Platform Supported

- Windows Server 2008
- Windows Server 2012

Linux (64 bit) flavors of the following distributions:

- RHEL – 7.x or above
- CentOS – 7.x or above
- Ubuntu – 14.x or above

RAM- 8 GB Hard Disk Space- 900 GB or above CPU- Intel Xeon 3.3.ghz 4 Core

MobSec Agent Requirements

RAM- 256 MB

Storage Space- 256 MB free

CPU- 512 MHz and above

Operating System- Android 4.4 or above

Key Benefits

- Overall addition of protection layer to your organization's critical mobile devices
- Employee Productivity and Behaviour Analysis
- MobSec generates relevant audit logs which you can use to ensure security compliance in your IT security practices
- When outside network offline monitoring protection of MobSec is activated. Upon mobile device connecting back the logs are visible and MobSec agent to communicates with the MobSec Server and enforce already set policies
- Implementation of various security controls on such mobile devices even when they are in offline mode
- Daily email summary report about sensitive mobile security events (incidents) occurring across the covered mobile endpoints

CONTACT US FOR A FREE TRIAL

VISIT OUR MOBSEC PAGE

https://dataresolve.com/mobsec/

TO SPEAK WITH OUR CYBER SECURITY CONSULTANT

Call +91 92666 03983
Email ask@dataresolve.com

OUR WORLDWIDE PRESENCE

India (Noida, Mumbai, Bangalore)
UAE (Dubai)

DATA RESOLVE TECHNOLOGIES HEAD OFFICE

G-30, Third Floor, Sector-3,
Noida, Uttar Pradesh-201301, INDIA
Phone: +91-9266603983

ABOUT DATA RESOLVE TECHNOLOGIES

Data Resolve Technologies is an IIT Kharagpur incubated startup, focused towards building futuristic products for Insider Threat Management and Employee Monitoring for mid-sized and large enterprises. We enable CIOs/ CISOs and business managers to monitor and predict employee behaviour and report any anomalous intentions detected, helping them build a secure ecosystem and increasing employee productivity.