



Data **Resolve**

**m**  **b sec** <sup>TM</sup>

**EMPOWER YOUR ORGANIZATION WITH**  
MOBILE WORKFORCE MANAGEMENT

[www.dataresolve.com](http://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

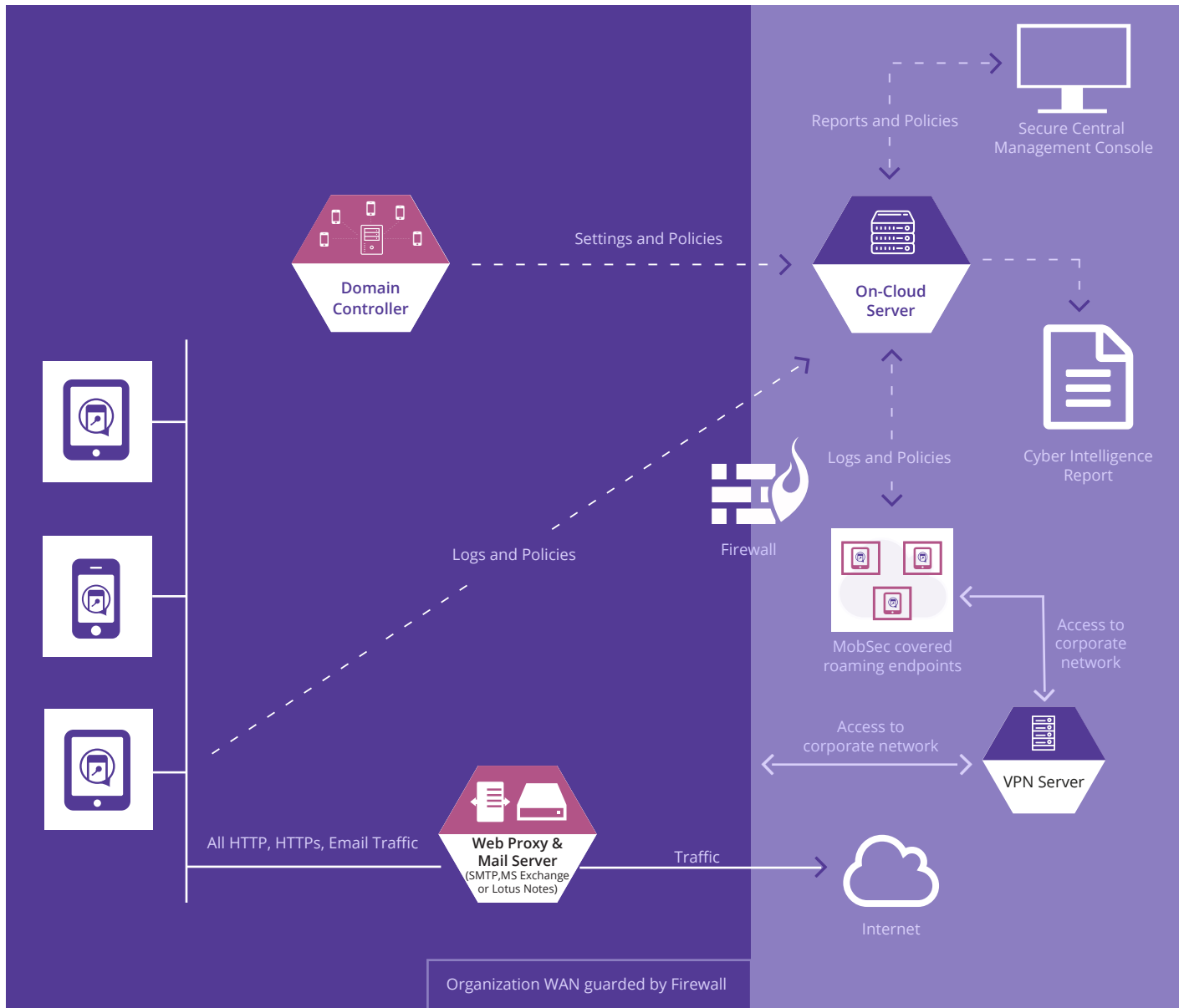
- 📞 Comprehensive incident reporting and analytics sections to provide the customer an overview of various activities occurring on the covered mobile endpoints
- 📞 Easy export of reports for offline viewing in PDF format

*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.

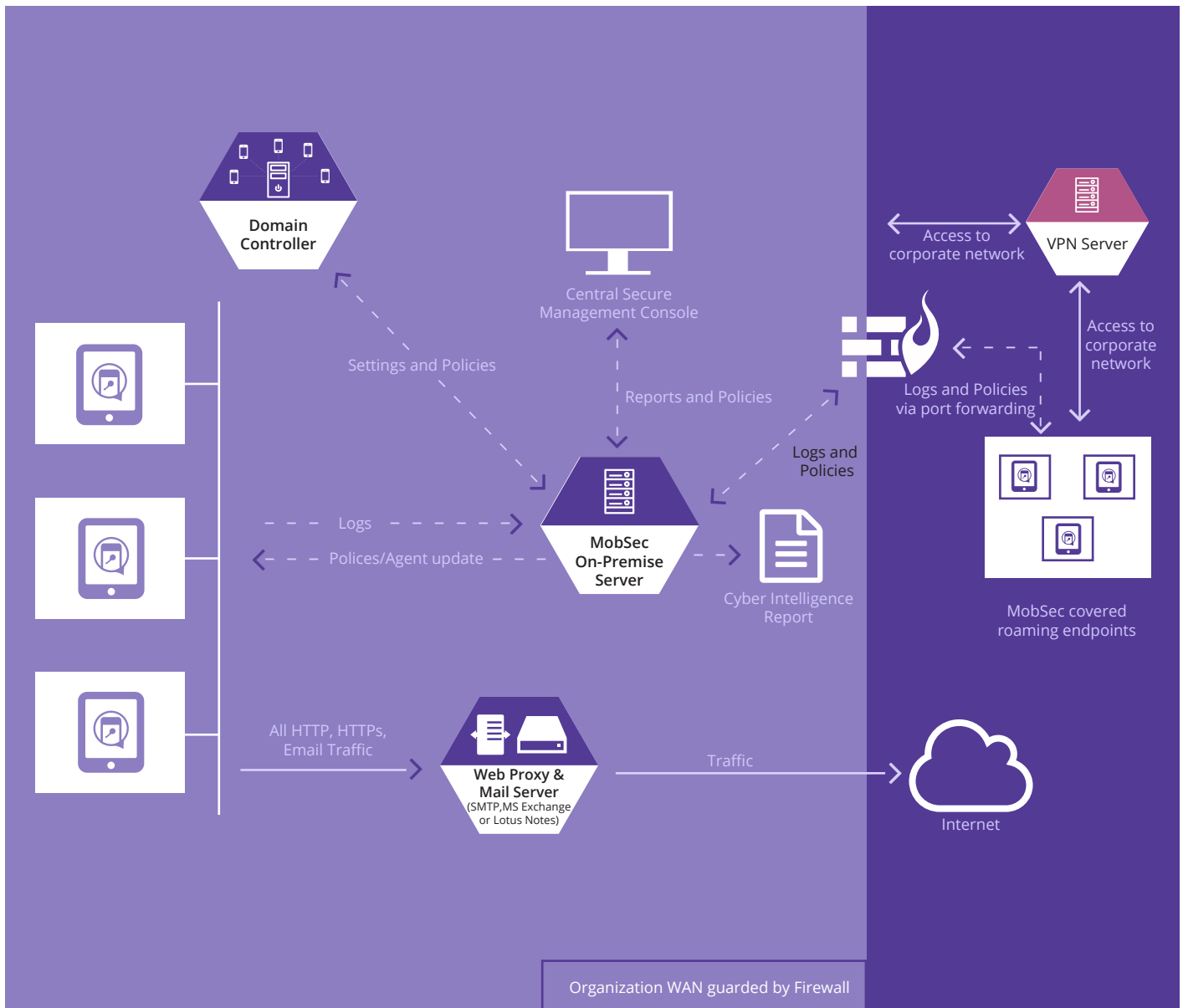


### mobsec On-Cloud Server

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 communicate 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](mailto: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.



**Data Resolve**

Cyber Security & Intelligence  
for Enterprises

**INDEFEND BUSINESS**

# Secure Printer Gateway

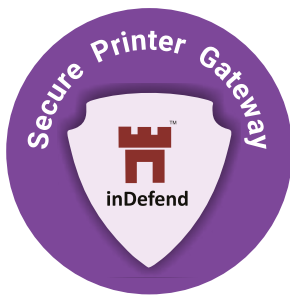
**An Intelligent Approach for Extended Security**

## Why Securing of Print Activities is important?

Regulation of print activities is becoming an increasingly important issue for businesses today. Because of growing cyber threats and increased legislations around privacy and data security, companies and organizations need to focus on strategies for securing their printing functions.

The main goal behind securing of print activities is to prevent leakage of data via print channels so that end user cannot walk away with confidential data without approval. Regulated access to printing of documents within the corporate environment can help prevent document theft or snooping in the form of hard copies and stop unauthorized access and misuse of critical documents.

## Secure Printer Gateway (SPG) Approach



To achieve this goal, Data Resolve offers the capability to monitor and control print requests with sensitive content, via a gateway based approach. To achieve this, organizations need to deploy the inDefend - Secure Printer Gateway (SPG) within their organization network.

inDefend – Secure Printer Gateway acts as a security layer between the end user and the actual printer servers and filters all incoming requests before they are actually printed.

inDefend - SPG analyses all outgoing print requests, applies security policies as defined on the inDefend Server and transmits the generated logs along with shadow copy of the submitted documents to the printer

## Used cases addressed via inDefend-SPG



Monitoring of all print requests submitted to the secure printer gateway along with details of the file being printed



Shadow logging of documents submitted for printing



Content analysis of all print requests submitted to the secure printer gateway

## Secure Printer Gateway (SPG) Approach

The below diagram illustrates a typical network topology depicting how inDefend SPG would be deployed.

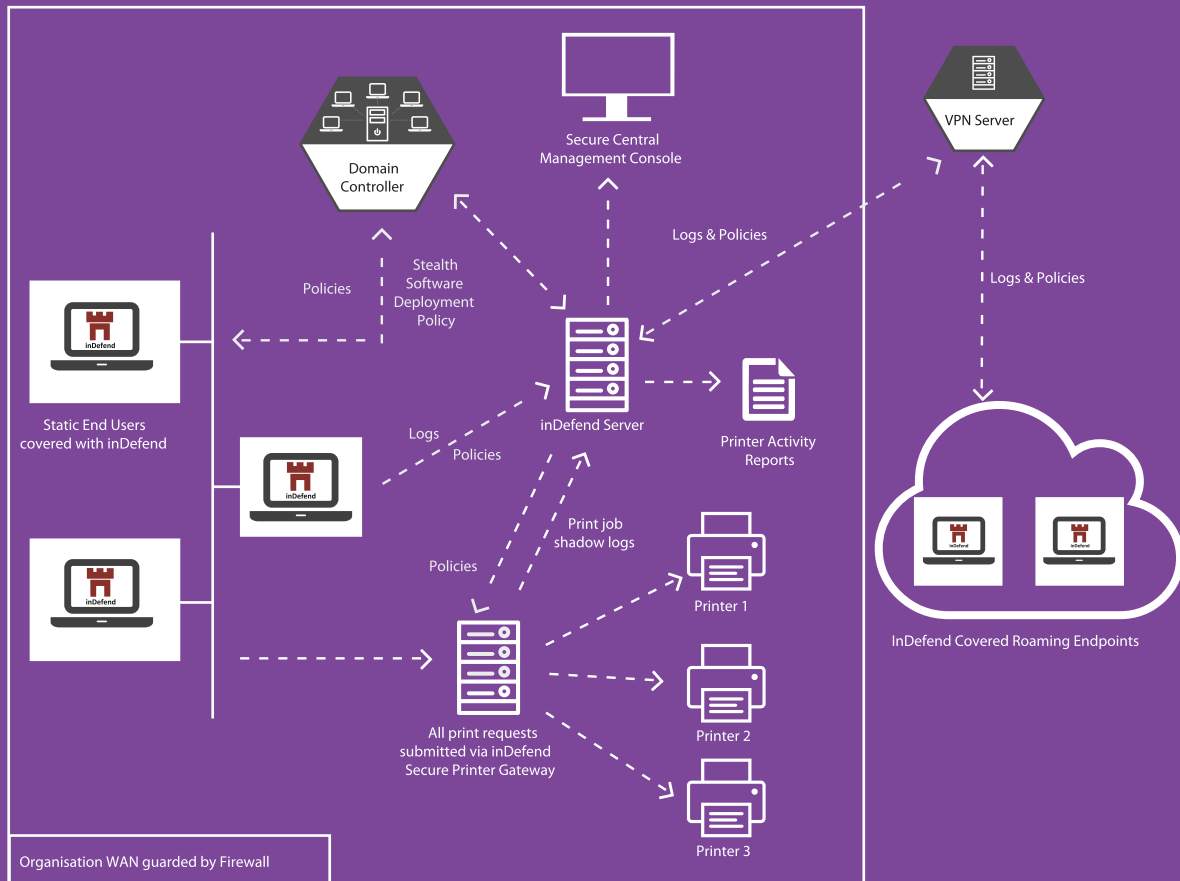


Figure 1: SPG Architecture

## System Requirements

### Hardware & Software Requirements

64-bit operating systems of the following flavors of Linux are supported viz:

- ❖ Ubuntu (14.04 LTS and above)
- ❖ CentOS 7.x
- ❖ RHEL 7.x
- ❖ Fedora 19 and above

**RAM-** 2 GB free (minimum)

**Storage -** 10 GB free (minimum)

## Architecture Support

- ◊ In-premise Only
- ◊ Compatible with both in-premise and in-cloud versions of inDefend Business server

## Key Benefits

- ◊ Added layer of security around print activities
- ◊ Reduction in data leakage attempts occurring via prints
- ◊ Establishment of clear audit trail and forensic reports around print activities done with malicious intent
- ◊ Real-time alerts sent to the administrator related to occurrence of such activities



**Data Resolve**

\*Terms and conditions are applicable on the features as mentioned in this document. For any clarification, please connect with team Data Resolve

### CONNECT WITH US

2/F, Elegance Tower, Jasola District Centre,  
Mathura Road, New Delhi - 110025, INDIA  
sales@dataresolve.com | +91-9266603983

[www.dataresolve.com](http://www.dataresolve.com)

### CLOUD PARTNERS



\* All logos used are copyrights of the respective owners



**Data Resolve**

Cyber Security & Intelligence  
for Enterprises

## **INDEFEND BUSINESS**

# Combat the Wave of **Insider Threats**

[www.dataresolve.com](http://www.dataresolve.com)

# inDefend Business

Data in any organisation is integral and key asset to the business it functions. Organisations need to evolve from a tactical perspective to a more strategic, holistic approach with their data security. Insider data theft has become one of the key enterprise security issues across the globe which experts are tackling nowadays. Implementation of current methods of security controls at the perimeter and endpoint level continue to prove insufficient against insider threats as traditional rule based methods cannot be directly applied on them. Keeping in mind the complexity of these threats, Data Resolve has come up with an insider threat management suite which proactively analyses the employee's behaviour patterns along with setting up controls in order to prevent data leakage.

## How inDefend can help?

inDefend Business is an application that helps you achieve full control over all the organisation computers by minimizing possibility of data theft across the enterprise network while maintaining relevant data access through device and network access control, simultaneously blocking all kinds of unauthorized removable media devices, websites, and applications like chat and VoIP that can lead to data loss.

## Our 3 Step Insider Threat Approach





# inDefend Capabilities



## Centralized Console

inDefend provides easy to use single centralized administration console for all the administration and management purposes.

- ✦ Advanced Reporting and Analytics Framework for all kinds of device and network activities
- ✦ Silent monitoring of all activities (stealth mode)
- ✦ Central installation and upgrades on end user computers
- ✦ Flexibility to monitor and control offline computers



## Analytics

inDefend provides easy to use single centralized administration console for all the administration and management purposes.

- ✦ Advanced Reporting and Analytics Framework for all kinds of device and network activities
- ✦ Silent monitoring of all activities (stealth mode)
- ✦ Central installation and upgrades on end user computers
- ✦ Flexibility to monitor and control offline computers



## Data Leakage Prevention

inDefend's strong data leakage detection and prevention engine helps keep the business critical information secure by:

- ✦ Monitoring, alerting and blocking capability for Emails, File Uploads and Attachments
- ✦ Monitoring and blocking capabilities for Unproductive or Rogue Applications
- ✦ Blocking of USB Storage, MTP and Local/Network Printers
- ✦ Content based alerting mechanism for Emails, File Uploads and Attachments
- ✦ Enforced Encryption on USB drives to keep the data accessible yet secure
- ✦ Prevention of malware spread across organisation network via blocking of malicious web browsing activity



## Employee Monitoring

inDefend proactively analyzes and facilitates the employers to detect and analyze various sensitive activities performed by end users by monitoring outgoing channels through:

- ✦ Detailed logging of Browser and Application Activities
- ✦ Detailed logging of all the Application Usage
- ✦ Detailed logging of all the Searches done
- ✦ Detailed logging of all the USB Devices used
- ✦ Internet browser behaviour analysis which gives Time based reports on the basis of Websites and articles/videos being viewed
- ✦ Application Activity monitoring which gives time based reports on the basis of Applications being used
- ✦ Analysis of activities to report time spent on unauthorized or unproductive applications



## Employee Forensics

Employees who steal data or perform any malicious activity leave a trail of digital evidence that proves valuable during investigation. Employee Forensics helps in, in-depth analysis and detection of the malicious activities performed by employees via various channels, with inbuilt tools for performing extreme monitoring facilitating:

- ✦ Shadow logging for complete Email body and attachment
- ✦ Shadow logging for all the Browser based file uploads
- ✦ Screen Shot monitoring for Activity Monitoring
- ✦ Logs of all the Emails, File Uploads, Application Usage, Website visits, Searches made, USB & CD/DVD data transfers, USB usage and Chat activities performed
- ✦ Analytics modules help generate forensic reports with evidence across suspicious users with the help of Analytics
- ✦ Log in and log out activity monitoring

**Security can be achieved with INTELLIGENCE**



## On-Premise

In this model, the server is hosted within the organizational network and dashboard is accessible from within the company WAN.

In this model, end points are connected to the inDefend server via the server's internal IP address. Connectivity of remote end points with the inDefend server can be managed with the public IP address based port forwarding.

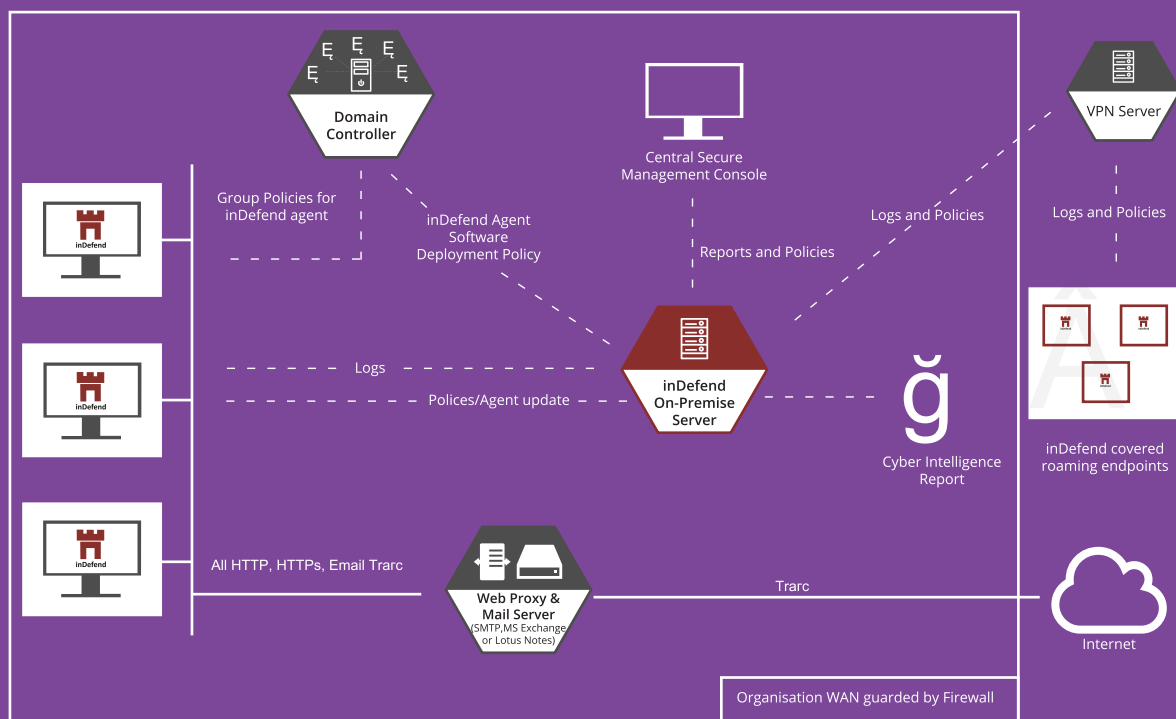


Figure 1.1: On-Premise Network Topology For inDefend

## Virtual Machine (VM) By Customer

In this model, inDefend server shall be installed on any suitable virtual machine provided by the customer. The VM shall reside within the organisation where the end points are connected to the inDefend server via the server's internal IP address. Connectivity of remote end points with the inDefend server can be managed with the public IP address based port forwarding.




# System Requirements

## inDefend Server Requirements

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

Platform Supported:	<ul style="list-style-type: none"> <li>Windows Server 2008</li> <li>Windows Server 2012</li> </ul>	
Linux (64 bit) flavors of the following distributions:	<ul style="list-style-type: none"> <li>RHEL – 7.x or above</li> <li>CentOS – 7.x or above</li> <li>Ubuntu – 14.x or above</li> </ul>	
<b>RAM</b> 8 GB	<b>Hard Disk Space</b> 900 GB or above	<b>CPU</b> Intel Xeon 3.3.ghz 4 core

## End Point System Requirements

<b>Windows</b> (32 bit and 64 bit) 	<b>Mac OS X</b> 	<b>Linux</b> (32 bit and 64 bit) flavors of following 
Windows Server 2008, Windows Server 2012, Windows 7, Windows 8, Windows 8.1, Windows Vista, Windows 10	Mountain Lion, Mavericks and Yosemite, El Capitan	Ubuntu -12.x or above, Fedora -16 or above, Debian - 7.0 or above, Boss - 5.0, CentOS - 6.x or above, RHEL - 6.x or above, Kali Linux - 1.0.8 or above
<b>RAM</b> 2 GB or above	<b>Hard Disk Space</b> 1 GB or above	<b>CPU</b> Intel Core i3 or above

\* All logos used are copyrights of the respective owners

# Key Benefits

- ◊ Secures the business critical data from insider threats for local and remote Users
- ◊ Integrated dashboard with advanced analytics
- ◊ Flexibility to deploy the solution On Cloud or in your own Premises
- ◊ Real-time SMS alerts and summary email reports for sensitive activities
- ◊ Advanced in-built device control capabilities with enforced encryption to keep the data secure in case device is stolen or lost



## Data Resolve

\*Terms and conditions are applicable on the features as mentioned in this document. For any clarification, please connect with team Data Resolve

### CONNECT WITH US

2/F, Elegance Tower, Jasola District Centre,  
Mathura Road, New Delhi - 110025, INDIA  
sales@dataresolve.com | +91-9266603983

[www.dataresolve.com](http://www.dataresolve.com)

### CLOUD PARTNERS



\* All logos used are copyrights of the respective owners



**Data Resolve**

Cyber Security & Intelligence  
for Enterprises

**INDEFEND BUSINESS**

# Secure Email Gateway

**An Intelligent Approach for Extended Security**

[www.dataresolve.com](http://www.dataresolve.com)

## Why Securing Outbound mails is important?

In today's digitally connected world, email (Electronic mail) continues to be the top medium for communication by organizations. With heavy usage and reliance on email as a medium of corporate data communication and exchange, the presence of security threats continues to be a major concern. Hence, it is important for organizations to protect their important and critical data against leakage or confidentiality breaches happening through corporate email.

On a daily basis, a large number of mails are sent by the organization's employees from their official mail accounts. With increased acceptance of enterprise mobility, end users are now able to access corporate email via personally owned mobile devices as well. Organizations need to safeguard themselves against any employee that may have an intention to leak data outside office hours, from any other personal device.

## Secure Email Gateway (SEG) Approach

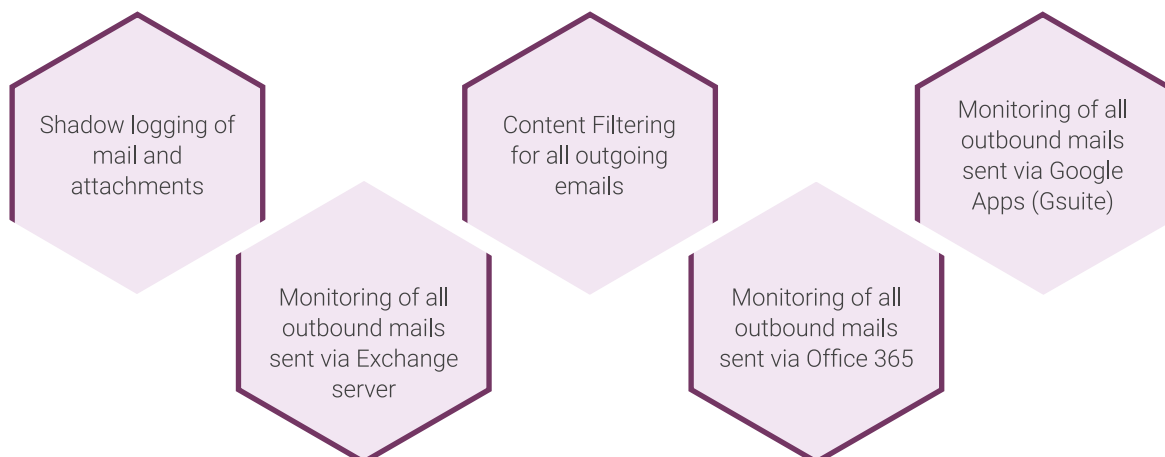


Secure Email Gateway (SEG) provides a protection layer on sensitive content going via corporate email channel to any third party, via agentless approach.

Data Resolve offers the capability to monitor and block outgoing emails with sensitive content via a gateway based approach, christened as inDefend Secure Email Gateway (SEG).

inDefend-SEG analyses all outgoing email content, applies security policies as defined on the inDefend Server and transmits the generated logs along with shadow copy of the email content, to the inDefend Server.

## Secure Email Gateway (SEG) Approach







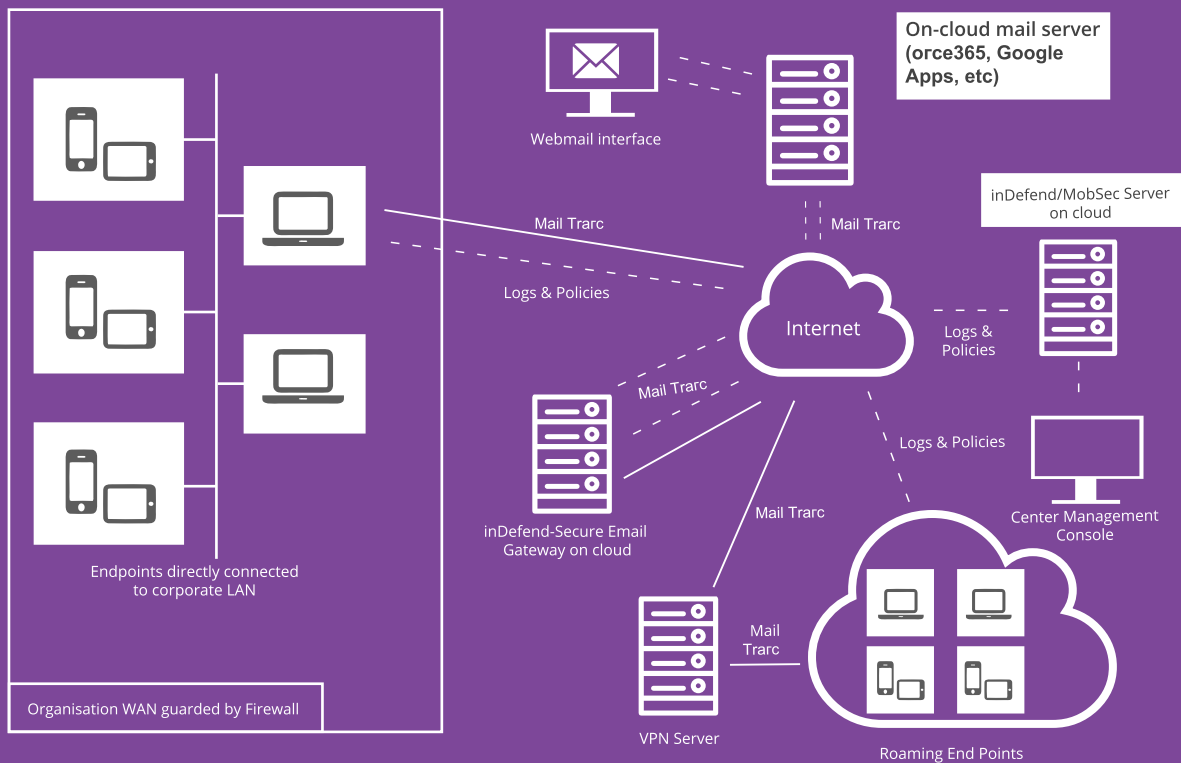


Figure 1.1: Typical network topology diagram for email analysis in inline (MTA) mode for cloud-based mail servers for roaming end points

## System Requirements

### Hardware & Software Requirements

64-bit operating systems of the following flavors of Linux are supported viz:

- ✦ Ubuntu (14.04 LTS and above)
- ✦ RHEL 7.x
- ✦ CentOS 7.x
- ✦ Fedora 19 and above

**RAM-** 8 GB free (minimum)

**Storage -** 50 GB free (minimum)

## System Requirements

- Deployment supported either on customer's private cloud, or Data Resolve's managed cloud
- Compatible with both on-premise and on-cloud deployments of inDefend server

## Key Benefits

- Visibility for all outgoing corporate e-mails, even from alien devices
- Helps to know details of the sender in the organization in case of data leakage scenario
- In-depth analysis of outgoing corporate emails with information about sender, recipient and mail content



\*Terms and conditions are applicable on the features as mentioned in this document. For any clarification, please connect with team Data Resolve

### CONNECT WITH US

2/F, Elegance Tower, Jasola District Centre,  
Mathura Road, New Delhi - 110025, INDIA  
sales@dataresolve.com | +91-9266603983

[www.dataresolve.com](http://www.dataresolve.com)

### CLOUD PARTNERS



\* All logos used are copyrights of the respective owners