Data Resolve

Cyber Security & Intelligence
for Enterprises

INDEFEND BUSINESS

Combat the Wave of **Insider Threats**

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

Monitor
Employee Behaviour & Productivity

Proactively Monitors Employee Behaviour and Productivity patterns and sends alarms for the sensitive incidents.

Protect
Data Leak Channels

Secures the data leakages and thefts via all the outgoing channels

Control
Sensitive Activities

Restricts the data access as per the rules defined.

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

Integrated Solution Architecture

Data Resolve's inDefend Business supports hybrid hosting models On-Cloud

In this model, the server is hosted on cloud so no additional hardware procurement is needed and all the machines directly communicate with the server via any internet connectivity. And its dashboard can be accessed 24*7 across the globe.

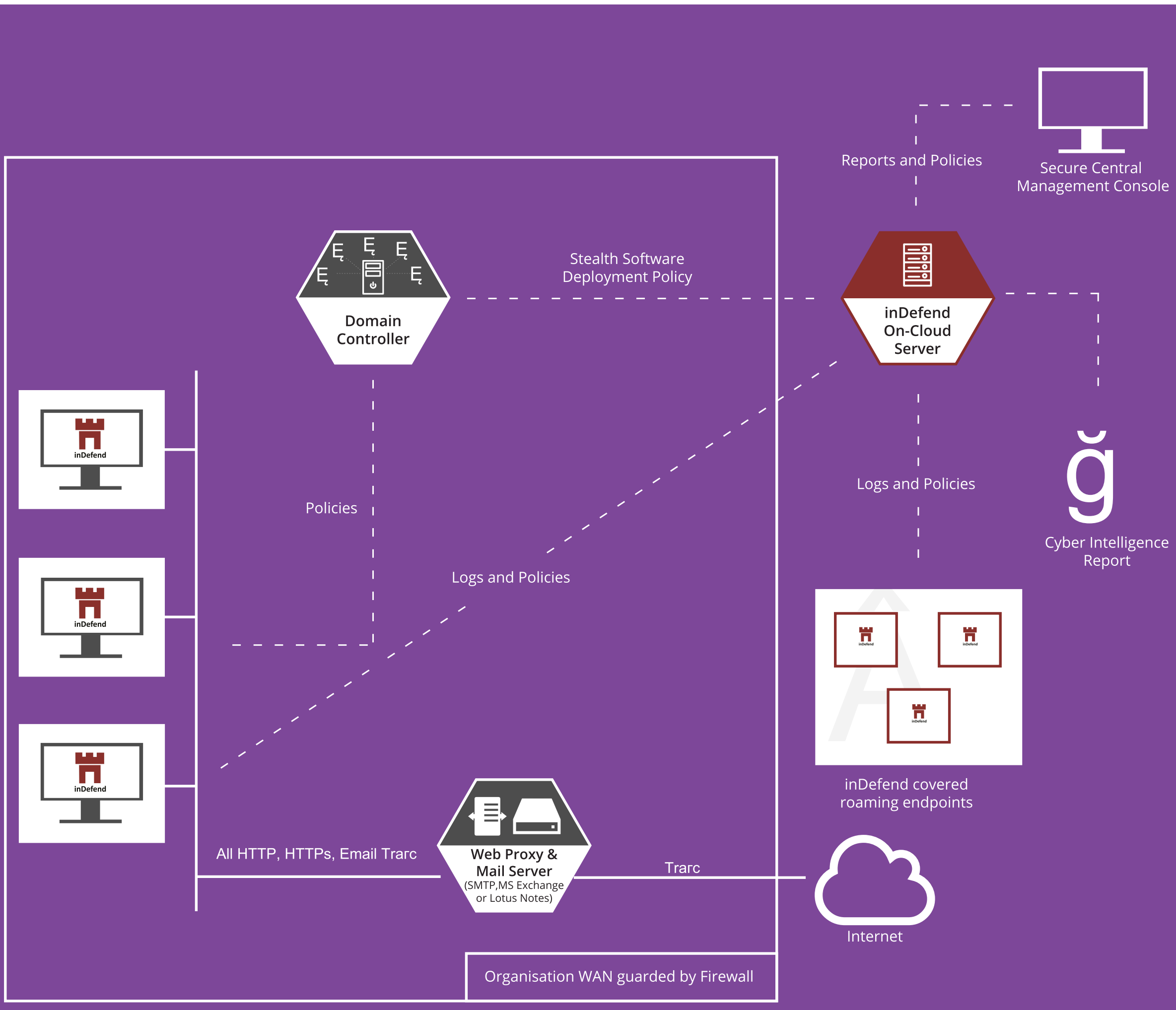
Reports and Policies
Secure Central Management Console
Stealth Software Deployment Policy
Domain Controller
inDefend On-Cloud Server
inDefend
Policies
Logs and Policies
Logs and Policies
Cyber Intelligence Report
inDefend covered roaming endpoints
All HTTP, HTTPs, Email Trarc
Web Proxy & Mail Server (SMTP,MS Exchange or Lotus Notes)
Trarc
Internet
Organisation WAN guarded by Firewall

Figure 1.0: On-Cloud Network Topology For inDefend

Private Cloud By Customer

In this model, inDefend server can be hosted on any suitable cloud based server provided by the customer. And all the endpoints directly communicate within the inDefend server via any internet connectivity. And its dashboard can be accessed 24*7 across the globe.

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.

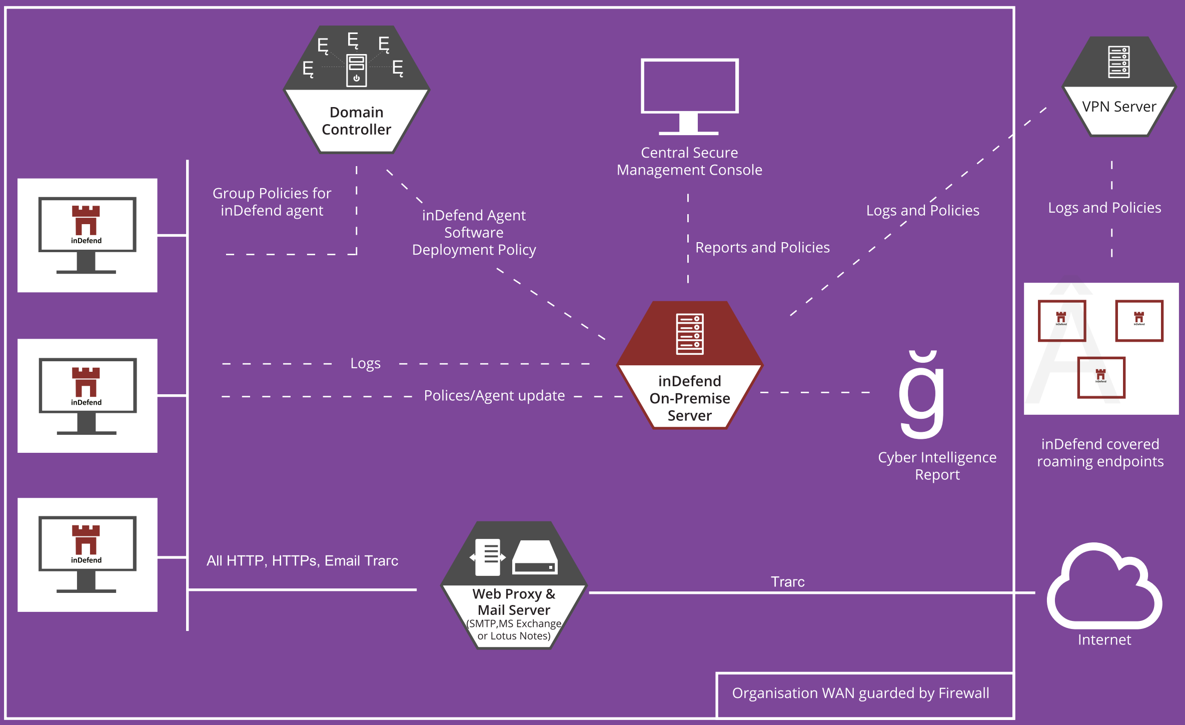
Domain Controller
Central Secure Management Console
VPN Server
Group Policies for inDefend agent
inDefend Agent Software Deployment Policy
Reports and Policies
Logs and Policies
Logs and Policies
inDefend
inDefend
inDefend
Logs
Polices/Agent update
inDefend On-Premise Server
Cyber Intelligence Report
inDefend covered roaming endpoints
All HTTP, HTTPs, Email Trarc
Web Proxy & Mail Server (SMTP,MS Exchange or Lotus Notes)
Trarc
Internet
Organisation WAN guarded by Firewall

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:	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	Hard Disk Space	CPU
8 GB	900 GB or above	Intel Xeon 3.3.ghz 4 core

End Point System Requirements

Windows (32 bit and 64 bit)	**Mac OS X**	**Linux** (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

RAM	Hard Disk Space	CPU
2 GB or above	1 GB or above	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

CLOUD PARTNERS

amazon web services | Partner Network

BUILT ON SOFTLAYER an IBM Company

* *All logos used are copyrights of the respective owners*