



Data Resolve

Cyber Security & Intelligence
for Enterprises

INDEFEND BUSINESS

Secure Printer Gateway

An Intelligent Approach for Extended Security

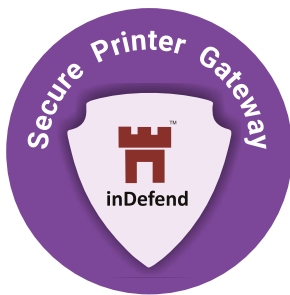
www.dataresolve.com

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.

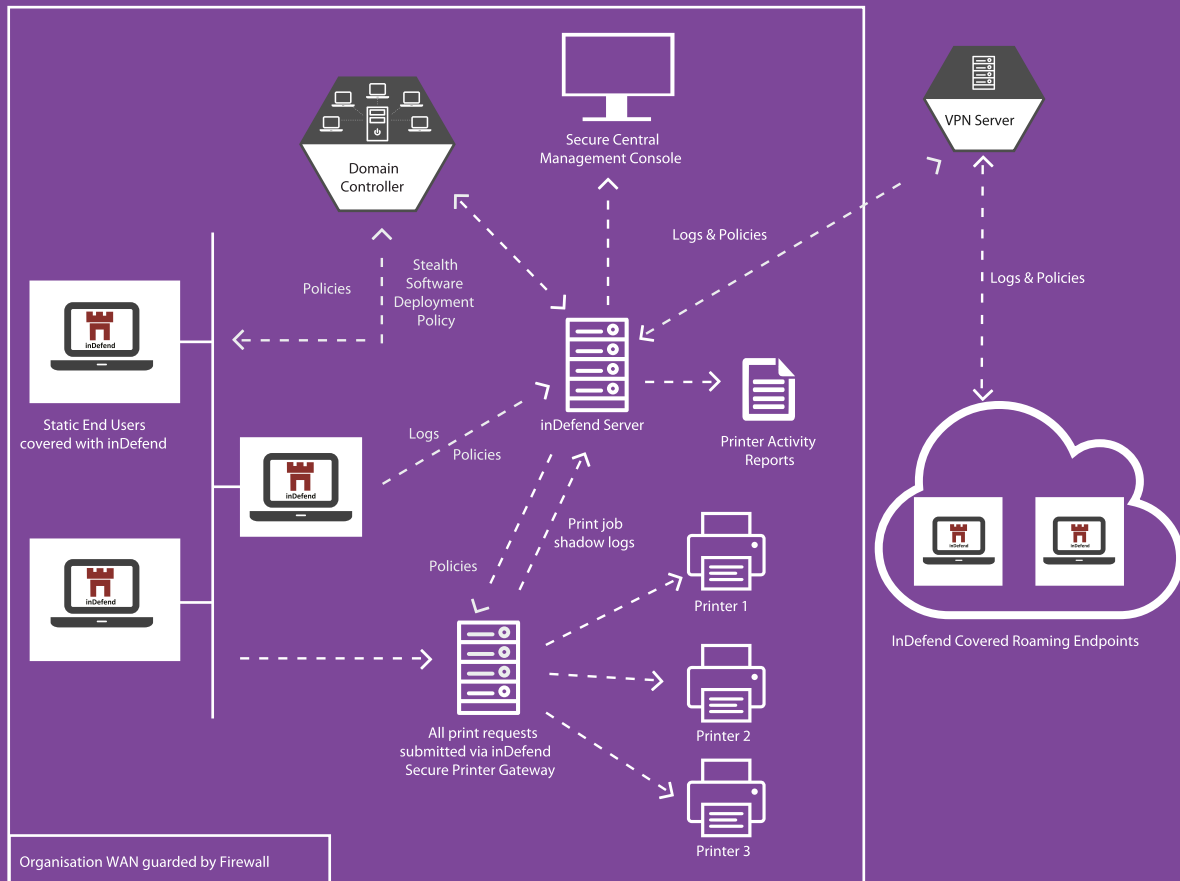


Figure 1: SPG Architecture

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

CLOUD PARTNERS



* All logos used are copyrights of the respective owners