Stay ahead of Security Risks within your company

Protect your data against Insider Threats within your organization

Introduction to inDefend Advanced

A unified suite for Insider Threat Management and Employee Behavioral Analysis

Overview

inDefend Advanced is a one-stop solution which helps to protect your data from insider threat and prevent the leakage of sensitive data through various communication channels and endpoints. It allows you to monitor the behavioral patterns of the users and also pinpoint the avenues through which confidential data can be leaked. This solution is built to achieve complete transparency over all the digital assets residing within the organization. It provides you with maximum security and solid safeguard against all the threats across the organization

inDefend Advanced Capabilities

Incident Summary

The solution gives a summarized view of all incident violations with respect to different verticals like Internet, Email, Applications and Devices. It also helps you to understand the increasing and decreasing trend of violations over a period of time while also allowing you to drill down into end users to get more details of the incident violations across the entire organization.

The Activity Analytics

The section helps in monitoring the users related to all the activities related to Browsers, Applications, Emails, Devices, File Uploads, Phrases Searched. The admin can drill down to granular logs of which user did what exact activity with the respective timestamps.

Dynamic Rule set section

Offers the customer the flexibility to create custom incident rules based on their organizational requirement, thereby preventing any false positives. The rules can further be classified on their kind of threat and their magnitude of effect in the organization. All the incidents created will get hits based on the users triggering the incidents in the organization which are visible from the Incident Summary section, giving a complete visibility on what did the user exactly perform on the endpoint level which triggered a certain incident.

Productivity Reports

Will generate various reports regarding the Login and Logout times of the users, Productivity Summary report, Application and Web Browsing on a daily basis.

Reflector Module

Added as a report that generates user wise productivity reports on a weekly basis, clearly showing the productive hours, unproductive hours and idle hours spent daily in order to increase productivity in a positive reinforcement manner.

inDefend Advanced System Requirements

inDefend Advanced Server requirements

CPU

Xeon Processor
4 Cores or above

Operating System

Ubuntu 20.04 LTS
(Bionic Beaver)

RAM

8GB RAM or above

Storage

100 GB or above

inDefend Advanced End Point requirements

Windows

Windows 7 SP2 (32bit, 64bit)

Windows 8.1 (32bit, 64bit)

Windows 10 (32bit, 64bit)

Windows 11 (64bit)

Linux

Ubuntu 18.04 (64bit)

Ubuntu 20.04 (64bit)

Ubuntu 22.04 (64bit)

Boss 8.0 (64bit)

MAC

MAC Os 11 (Intel, M1, M2)

MAC Os 12 (Intel, M1, M2)

MAC Os 13 (Intel, M1, M2)

MAC Os 14 (M1, M2)

RAM

8 GB

Storage

15 GB free hard disk space or above
on the system Disk

Key Benefits

- It offers weekly visibility of employee activities
- Offer time spent on productive and unproductive applications
- Offer time spent on productive and unproductive URLs
- It offers idle time, inactive time visibility to users most productive app and unproductive app usage
- Report can be downloaded in pdf & csv forma

Why are Insider Threats important to be managed and harder to detect?

Data in any organisation is an integral part and a key asset to business functions in today's world & it is imperative for any organisation to secure the same. Insider data theft has become one of the key enterprise security issues across the world and current approach of data leak prevention technologies are lacking the required infrastructure and customisability in their applications to tackle these threats. Moreover, without the User and Enterprise Behavior Analytics tool, most DLP solutions could only offer reactive measures based on mathematics and lack the component which enables understanding the psychology of the Risk. Challenges that an organisation faces while encouraging these risks are:

- Insider threats can go undetected for years....
- It is hard to distinguish harmful actions from regular work...
- It is hard to prove guilt...
- It is easy for employees to cover their actions...

Adding to the woes, currently there is not a single Cross-Functioning single platform available in the market for UEBA, Fraud Prevention, DLP and Information Security. Owing to the rising cost of Human Resources and global trends; it is pivotal for any organisation to continuously monitor and enhance the value created by each employee by way of enhanced operational and productivity efficiency.

How can inDefend help?

inDefend is a Business Application that enables Government Institutes, financial institutes, large and medium corporates to maintain full control of all the end points by way of monitoring, protecting and controlling all activities of users; whilst enabling permitted levels of access specified to each user within parameters of specified user rights.

Used as an Insider Threat Management cum UEBA Suite; the application would proactively monitor, analyse behavior patterns of each individual users and would promptly prevent or report activities that falls outside the specified scope of user activity.

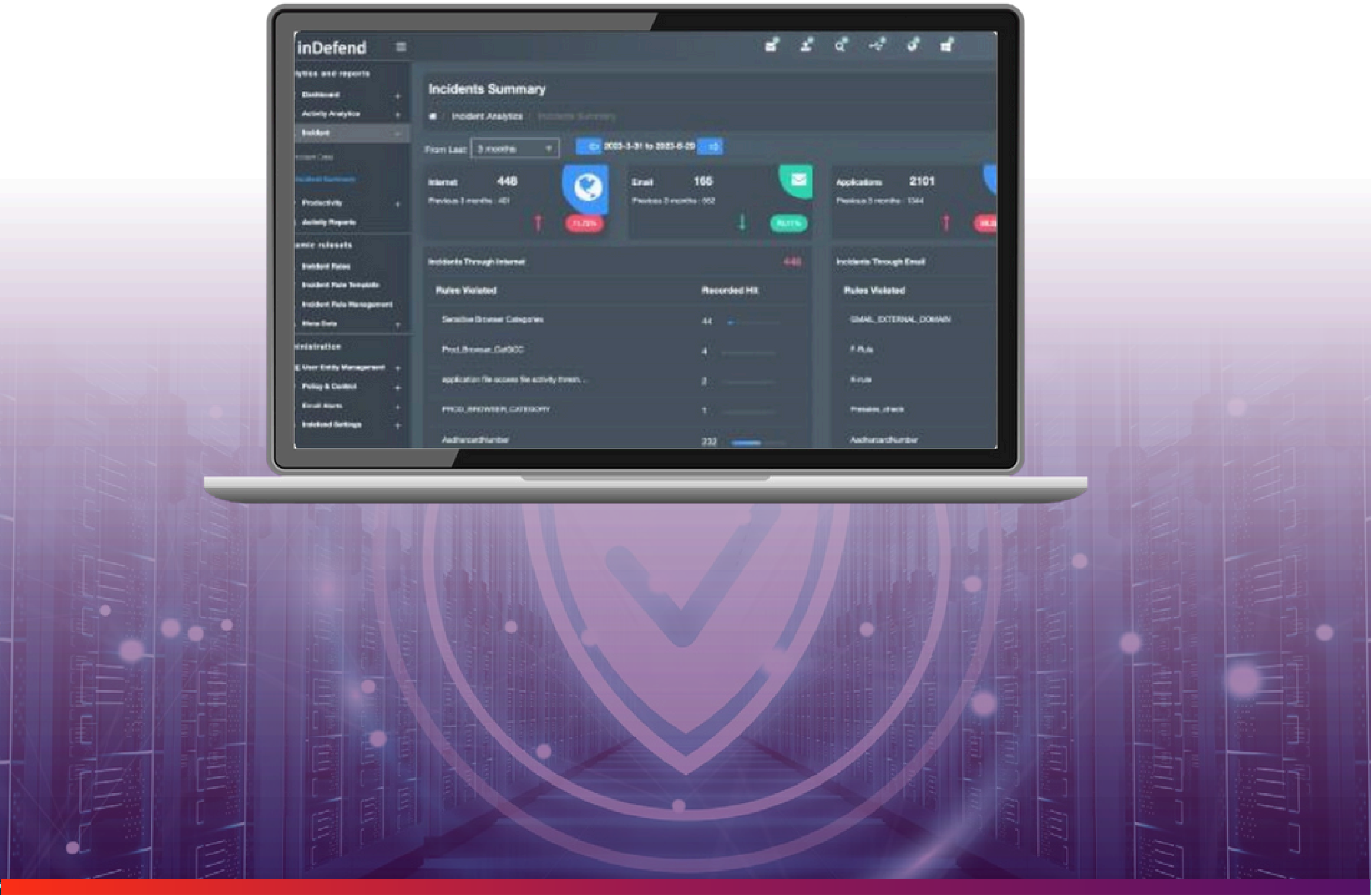
Why choose inDefend?

InDefend provided monitoring modules of end-points including computer terminals, and servers + additional modules of e-mail and a UNIFIED and SINGLE CONSOLE and a DASHBOARD for reporting and control! InDefend solutions are tailor made based on subject matter expertise of each industry and delivered in modules that are further customizable. InDefend solutions come at competitive prices that are significantly lower than market prices for DLPs.

Highly qualified professionals hailing from different nationalities and expertise in IT, banking and finance and consulting fields would work with you to enhance the implementation and value added by our products.

- Insider Threat Response System
- Data Leakage Prevention
- Intellectual Property Theft
- User and Entity Behavior Analytics (UEBA)
- Application Monitoring/Whitelisting
- Workplace Productivity
- Tracking Executive Positions
- Data Exfiltration Intelligence

- Corporate Cyber Intelligence
- Proactively analyzes and facilitates the employers to detect and analyze various sensitive activities performed by end users by monitoring Browser activities, Application Usage, USB devices and time-based reports.
- Protect organization’s confidential data against all Insider Threats and Data Leak.
- Track illegitimate activities of people working under third party contracts.



Incidents Summary

Incident Analytics

From Last: 3 months

2023-3-31 to 2023-6-29

Internet 448

Email 166

Applications 2101

Incidents Through Internet

Rules Violated	Recorded Hit
Sensitive Browser Categories	44
Prod_Browser_CatSOC	4
application file access file activity threshold...	2
PROD_BROWSER_CATEGORY	1
AadharcardNumber	232

Incidents Through Email

Rules Violated
GMAIL_EXTERNAL_DOMAIN
F-Rule
K-rule
Pressure_check
AadharcardNumber

Ability to record, gather data, analyze and action based on block or reporting (System/Email) parameters real-time.

Flexibility to be deployed on own premise or on 3rd Party or Private Cloud. Advanced inbuilt device control capabilities to enforce encrypted data protection on lost or stolen devices including removable media

Fraud Prevention

By Monitoring and Analyzing patterns of User Behavior using parameterized red flag patterns and content monitoring.

Data Leakage Protection

By Monitoring and Blocking all modes of leakage of data by content; including emails, uploads and removable media.

Productivity and Operational Efficiency

By Monitoring screen-time and activity on each of the applications and usage of each application. Ability to Monitor each computer terminal in stealth mode using minimal memory usage and advanced analytics performed in a dedicated server capable of handling 3000-4000 users real-time.

Product Differentiators

Integrated Dashboard with Unified Console DLP + SEG + Productivity+ Activity in 1 Box

Multi Platform Support WIN, LIN, MAC, BoSS

Multi Level Reporting

Employee Monitoring

Supports On Prem/Cloud

Stealth Mode

Use Cases – Sector Specific

Resource Footprint

Custom Rule Sets

Easy Deployment

Dynamic Level Repor ting

ROI Driven with Lowest TCO

Key Features

Analyse

- Capture and Understand DNA of specific organizational data
- OCR based content and Deep Scan Content Detection
- Predefined and Built-up Sensitive Keywords, Phrases, Patterns
- Department and Role Wise Data Capture
- Intent-Mining - Studying of Application Titles to understand User Intent
- Intent-Mining – Studying of User Searches to proactively determine impending threats or risky users
- Analyse Event based / Periodic Screenshots for detailed Forensics
- Analyse off-work hours and off the network activities
- Analyse sensitivity of files each application is accessing at any point of time

Detect and Alert

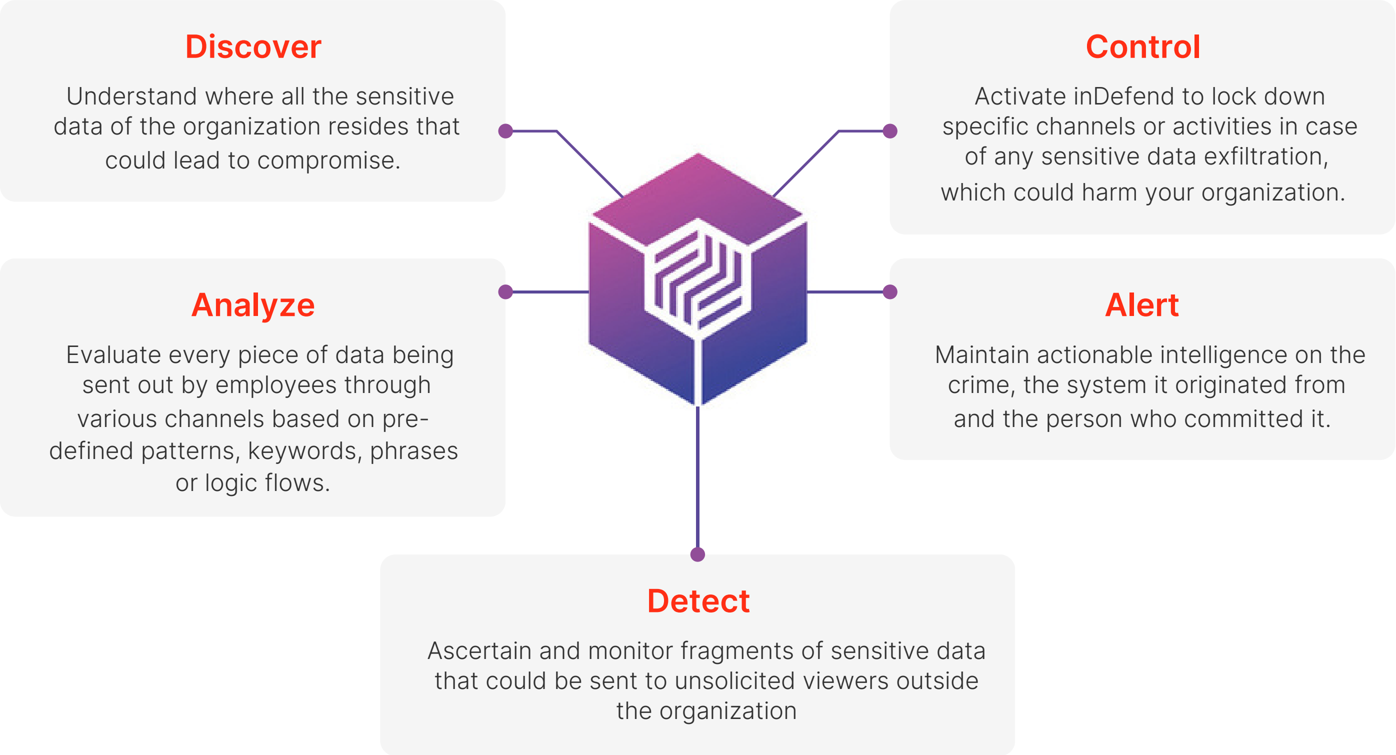
- Sensitive Data Creation Detection
- Sensitive Data Flow Detection
- Anomalous User Behavior Detection
- Malicious/Unproductive Application Detection
- Detection of Unauthorized/Unproductive Website Detection
- Meaningful Incident Generation
- Admin role wise alert generation in Dashboard Alerts
- Summary of Daily/Weekly generated Alerts
- Sensitivity towards correct policy or protection enforcement
- Alerts towards policy changes or protection removal

Policy System

- Policy Templates
- User or Machine Specific Policy System
- Temporary Policies

Data Resolve's - Insider Threat Management

User Behavior Centric System



Discover

Understand where all the sensitive data of the organization resides that could lead to compromise.

Control

Activate inDefend to lock down specific channels or activities in case of any sensitive data exfiltration, which could harm your organization.

Analyze

Evaluate every piece of data being sent out by employees through various channels based on pre-defined patterns, keywords, phrases or logic flows.

Alert

Maintain actionable intelligence on the crime, the system it originated from and the person who committed it.

Detect

Ascertain and monitor fragments of sensitive data that could be sent to unsolicited viewers outside the organization

Control

- Selectively Control web based and application based data transfers based on sensitive data patterns and block them from source of origin
- Selectively control devices and transfer data in encrypted form into them
- Sandbox applications to connect to only select list of domains or IPs
- Selectively block malicious/modified versions of specific applications
- Application Whitelisting
- Web Category based Blacklisting
- Email Recipient Based Whitelisting/Blacklisting
- Complete Lockdown in case of High Risk or Suspicious Users
- Tamper Proof Protection Systems

Reporting System

- Cyber Intelligence Report
- Dynamic Incident Generation Framework
- Email Based Alert System
- Exportable Reports (CSV.XLS)
- Exportable to SIEM systems
- Admin Role Specific Reporting

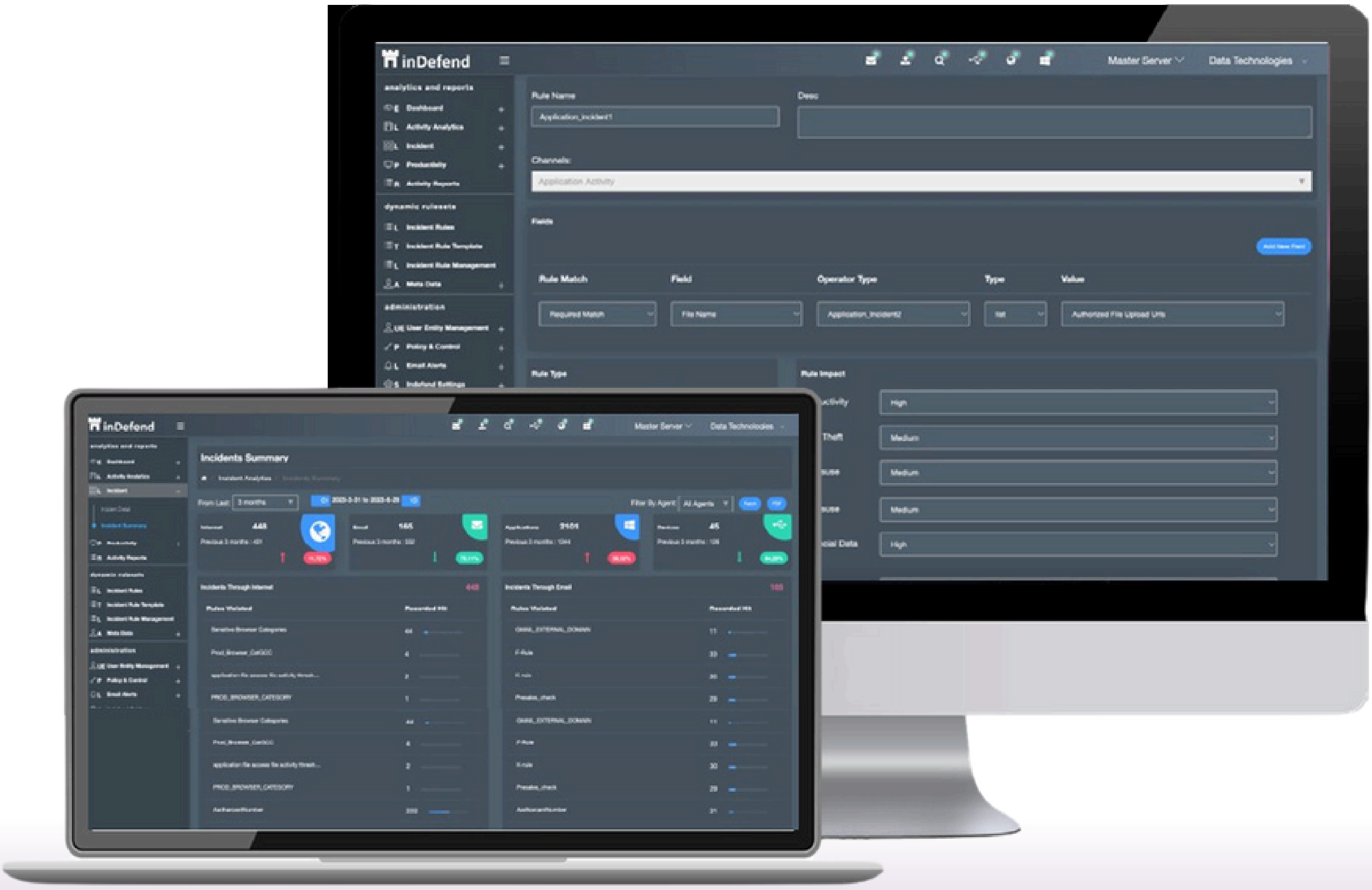
Incident Summary

Provides a summarised view of all incident violations with respect to different verticals like Internet, Email, Applications and Devices.

Helps you to understand the increasing and decreasing trend of violations over a period of time while also allowing you to drill down into end users to get more details of the incident violations across the entire organisation.

Rule Builder Screen

This screen allows inDefend admin to create dynamic rules and define what is an incident as per their organization needs.



Rule Name: Application_incident1

Desc

Channels: Application Activity

Fields

Rule Match	Field	Operator Type	Type	Value
Required Match	File Name	Application_incident2	list	Authorized File Upload Urls

Rule Type

Rule Impact

...ctivity	High
Theft	Medium
...buse	Medium
...buse	Medium
...cial Data	High

Incidents Summary

From Last: 3 months

Internet	Email	Applications	Devices
448	165	2101	45

Incidents Through Internet 448

Incidents Through Email 165

inDefend Secure Email Gateway (SEG)

In today's digitally connected world, Electronic mail is the top medium of communication by organizations. With heavy reliance on email as a medium of corporate data communication and exchange, it is important for organization to protect their important and critical data against leakage or confidentiality breaches happening through corporate email.

A large number of Emails are sent by the organization's employees from their official Email accounts on daily basis. 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 employees who have motivation to leak data outside office hours, from official or personal device.

inDefend Secure Email Gateway(SEG)

provides protection layer on sensitive content going via corporate Email channel to any third party, via agent-less approach.

offers the capability to monitor and block outgoing Emails with sensitive content via gateway.

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.

Key Benefits

- Functionality of Secure Email Gateway
- Information about sender & recipients
- Time stamp of e-mail transaction
- BCC email tracking
- Usage of corporate mails sent via alien devices
- Detection of misuse of corporate accounts
- Data security and data leakage prevention for corporate emails
- Forensic evidence of all detected corporate email incidents via shadow logs
- Organization level mail activity analytics
- Outbound email security
- Content analysis
- Email Quarantine
- Email Alerts

Data Resolve Technologies is an emerging data security company specializing in user behavior-driven Insider Threat Management. The organization offers a User Behavior Centric reaction system that prevents access to unauthorized removable media devices, websites, and applications. Data Resolve award-winning platform inDefend Advanced to detect, record, and prevent malicious user behavior in addition to helping teams drive productivity and efficiency.

CONTACT US FOR A FREE TRAIL

Demo session

https://downloads.dataresolve.com/free-trial

VISIT OUR WEBSITE

www.dataresolve.com

TO SPEAK WITH OUR CYBERSECURITY CONSULTANT

WhatsApp us at: +919599936473

Email: marketing@dataresolve.com

OUR WORLDWIDE PRESENCE

INDIA, EMEA, ASEAN, CANADA and UK

Data **Resolve**