inDefend

USE CASES

Data Resolve

Table Of Contents

Use Cases By Solution

Use Cases By Industry

inDefend Product Insights

Use Cases By Solution

Learn how inDefend can be helpful to your organization

Data Loss Prevention

Use Cases

- Stop Intellectual Property from getting stolen
- Protect health records of patients
- Protect personally identifiable information like Aadhar, Social Security Number, PAN, etc.
- Protect Credit and Debit card information
- Protect data regarding upcoming mergers and acquisitions
- Protect strategy and planning data
- Protect information about product launches
- Protect sensitive design schematics
- Protect unreleased and preview prints of upcoming movies
- Protect confidential discount and coupon codes from being used in an unauthorized manner

Insider Threat Response System

Use Cases

- Prevent competitors from getting hands on sensitive internal product data
- Detect undercover employees working for competitor company
- Track illegitimate activities of people working under third party contract
- Prevent whistleblowers from degrading integrity of the organization
- Observe people working as business partners – contractors, suppliers and distribution channels
- Detect serious cyber-crime offenders using the organization as a resident shield for global activities
- Detect terrorism and anti-national criminals masquerading within the organization which pose serious military threat
- Detect anti-social elements working within the organization which pose a serious social threat

Intellectual Property Theft

Use Cases

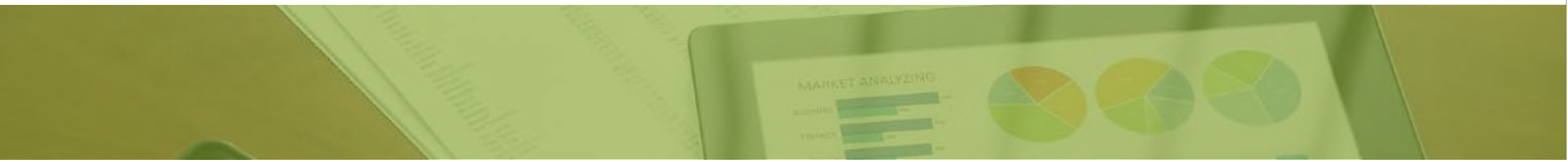
- Prevent getting robbed of design ideas, inventions and plans
- Stop all kinds of design files from being sent automatically based on content detection
- Discover traces of intellectual property that might be hidden with the organization
- Trace which people have access to what kind of sensitive information by detecting footprints of the same data
- Protect authentic examination papers and research material from getting leaked
- Protect confidential business plans and go-to-market strategies from being leaked
- Protect patents, industrial design rights, trademarks, trade dress and trade secrets

Use Cases

- Find needed business information when employee is not available
- Discover silently if an employee is working in the right direction
- Be aware if the employee is handling sensitive data and how careful or careless he or she is about managing them
- Prevent personal use of employer facilities and IT infrastructure which on larger scale could have massive operational and financial impact
- Check for violation of employee policies that takes place through activities like sending abusive/offensive/racial emails or chats
- Check for violation of known crimes like pornography, child abuse, racism, terrorism, etc.
- Detect psychological stability of employees and how it is affecting rest of the team members.
- Investigate complaints of sexual harassment by effecting actual evidence.
- Check illegal and unauthorized installation of risky or pirated software
- Increase bandwidth availability
- Documenting bad employee behavior

Employee Monitoring

Workplace Productivity



Use Cases

- Figure out how and which resources your employees are using to work and proactively improvise
- Find out the employees' most productive period and most unproductive period in a day
- Understand which employees are overworking and who are underworking
- Decrease distractions occurring due to social media engagement, sports, online videos, etc thereby increasing overall team focus
- Reduce peer distractions occurring in a team due to unsolicited activities
- Better insights to evaluating employee performance
- Detect daily dose of cyberslacking or goldbricking amongst your employees and variations across different departments

Employee Behaviour Investigations

Use Cases

- Detect attitude problems
- Find out the employees' most productive period and most unproductive period in a day
- Understand which employees are overworking and who are underworking
- Detect false propagandas and weaponized information right from the point of origin
- Detect cyber bullying
- Investigate probable reasons for sudden performance drop
- Have more insights into change in employee behaviours post annual appraisals
- Gain intelligence into employee integrity by understanding how they treat company confidentiality
- Detect causes of change in employee performance due to external issues
- Monitor how your client facing employees actually interact with your priced clients
- Detect if employees are exposing or forwarding confidential company information to family or near relatives
- Detect if any employee is indulging in activities pertaining to unionism and internal conglomeration

Tracking Executive Positions

Use Cases

- More useful to the board of directors in tracking individual CXOs and CEOs in a group of companies
- Silently track activities of power positions within the company, specially hired top executives
- Find out which CXO is going to exit in the next few months
- Find out a defecting CXO who is silently passing out confidential company information to competitors at a price
- Detect cases of insider trading and insider theft among CXOs and VPs
- Give more insights to board of directors in case of what is being convinced during board meeting and what the reality actually is
- Helpful in tracking CXOs in offshore offices and regions and their actual activities

Monitoring Exiting Employees

Use Cases

- Effectively monitor activities of high risk employees who are in the notice period
- Effectively control access to exiting employees thereby mitigating the range of sensitive data that they can send out of the company
- Detect decrease in productivity and work hours during exiting period
- Build chances of finding out if an exiting employee is disgruntled as well which might lead to organizational damage
- Extend security and monitoring layer beyond workstations and laptops to mobile devices and handhelds being used by the exiting employees
- Protect organizational confidentiality by monitoring employees more closely or as a team or as a group when mass layoffs happen
- Safeguard your organization against employees who are fired and switch to revenge mode against the company
- Enable a history check on employee's previous activities after an employee resigns and detect signs of probable breach
- Enable complete remote lockdown on end user laptop in case the employee flees away with the laptop or absconds.

Data Exfiltration Intelligence

Use Cases

- By enabling effective application control policies, reduce chances of malware, trojans or unknown applications from sending out data unknowingly from system
- Enable early detection of sensitive data across the network and apply consolidation measures to decrease impact area in case an internal attack happens
- Build chances of detecting hidden Advanced Persistent Threats within the network and control data being sent out by then
- Stop usage of tunnelling applications like Tor within the company network which otherwise remains undetected at the UTM level
- Enable secure sandbox on all your external devices thereby keeping all data within the company's endpoints
- Completely eradicate chances of data theft when an external USB device is stolen or lost

Corporate Cyber Intelligence

Use Cases

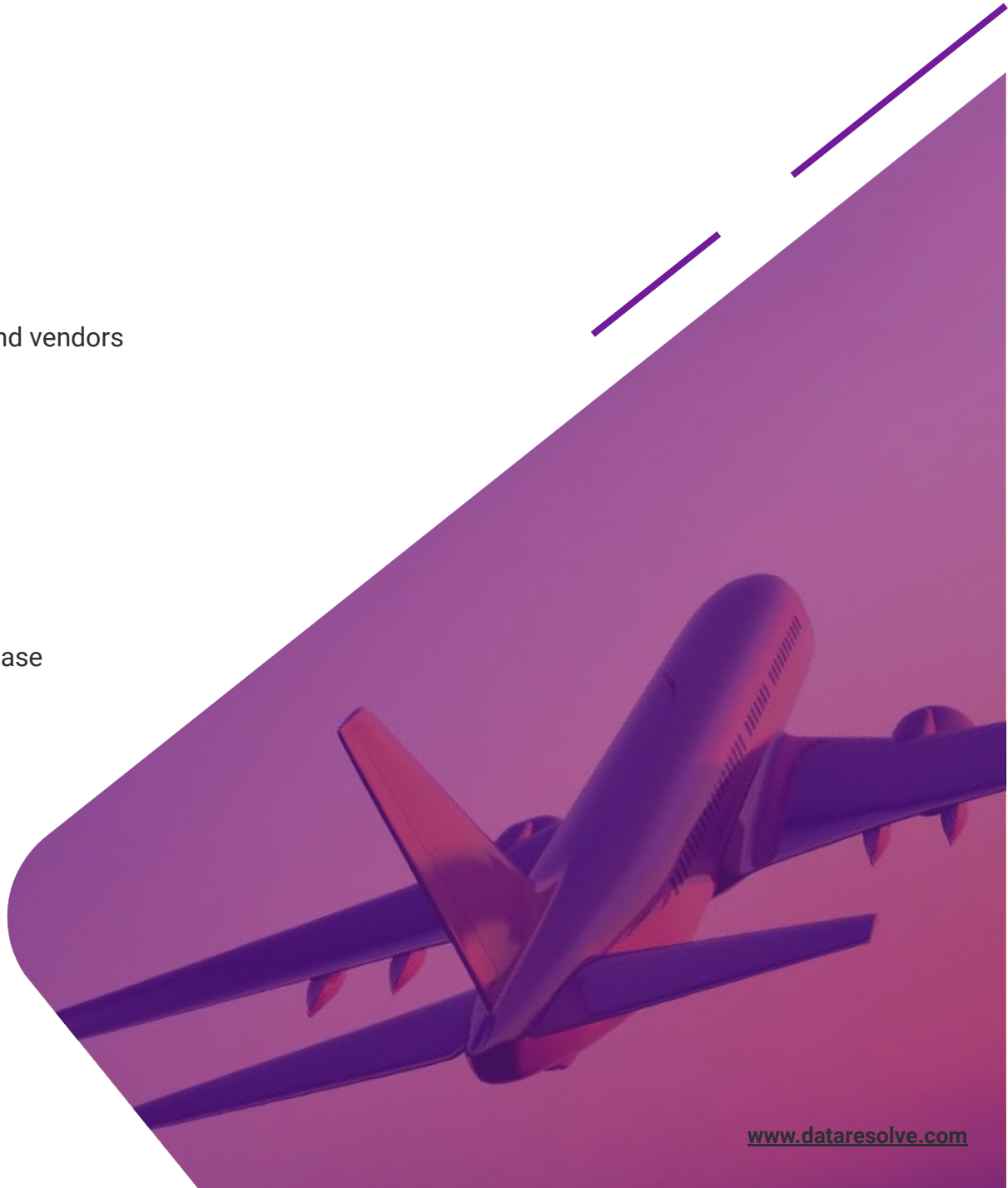
- Establish capability and process to detect internal threats arising out of employees and malicious
- applications Build analytics targeted at reading the internal attacker's real intent
- Proactively discover what vulnerabilities and leak points an attacker might have access to during the course of operation
- Develop and grow an intelligence plan by planning, collecting, processing, producing and disseminating essential organizational information
- Define proper indicators of compromise and establish proper alerting for repeat offenders or attacks
- Gain risk assessments on operational, compliance and productivity parameters to inject more power at strategic decision-making points
- Gain access to various forms of reporting and analytics to be able to draw analysis and conclusions across teams, departments or geographies
- Silently but effectively build reliability scores against every employee to be able to pre-evaluate assignment of specific employees to high sensitivity projects
- Establish Employee Intelligence as a driving engine for HR evaluations and security evaluations thereby reducing the need to assess an employee over a short period of time

Use Cases By Industry Type

Industry specific use cases of inDefend

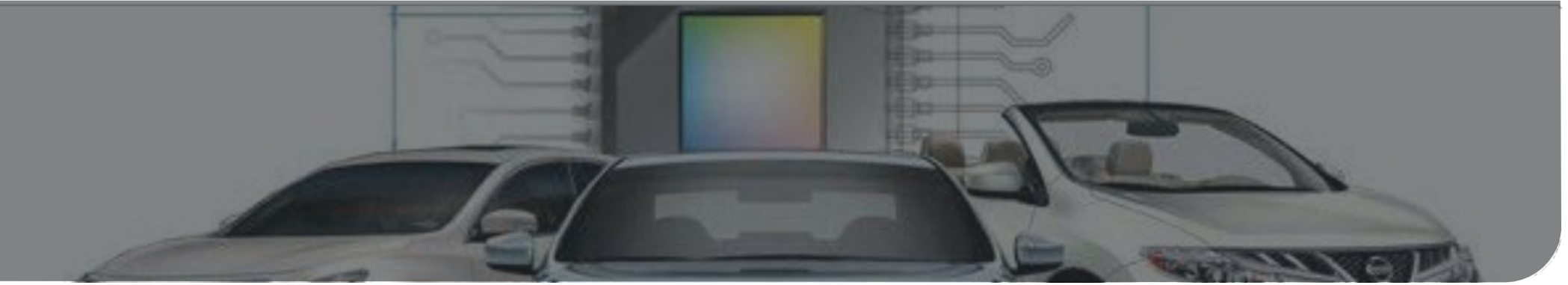
Aerospace

- Protecting confidential aircraft designs
- Safeguarding sensitive project plans
- Protecting contractual and pricing data of suppliers and vendors
- Defending Critical Infrastructure (CI)
- Securing vulnerable supply chain data
- Securing air traffic control
- Avoiding trade secret theft
- Safety of data on mobile devices, IoT and cloud database
- Protecting confidential data of customers



App Development Firms

- Avoiding leakage of app designs
- Securing data related to client requirements
- Maintaining confidentiality before launch
- Protecting end user endpoints from possible data leaks
- Granting proper access control to authorized users
- Encrypting messages through various transmission channels
- Maintain access control policies based on user role to keep track and control on productivity of employees
- Enable managers to keep track of correct direction of work within their team
- Protect design data being shared with third party consultants and designers
- Effectively manage and monitor remote office location sales and support team



Automobiles

- Protecting design and features of upcoming models
- Protecting supplier information and their confidential pricing
- Securing tender quotations
- Securing data of Original Equipment Manufacturers (OEMs)
- Protecting data related to supply chain integration
- Protecting each sensor, actuator, microcontroller (MCU), and microprocessor
- Safely and effectively managing the entire vehicle over the air (OTA)
- Monitoring and controlling of data leak at all dealer showrooms and service outlets
- Productivity monitoring of all employees across all offices, dealers and service centers of the company

Banking and Financial

- Security of customer's credit card, debit card and bank account details
- Protecting KYC documents of clients
- Securing customer email address, username and passwords
- Shielding financial logistics data
- Shielding ATM logistics data
- Securing IT operations
- Identifying internal security and employee trust issues in real time
- Recording employee forensics for post crime analysis
- Monitoring tablets and mobile devices of on-field sales agents

Business Intelligence Firms

- Safety of data transferred from clients
- Monitor USBs and external devices
- Protecting client database on servers
- Encrypting emails that have client-side data
- Monitoring BYOD within the organization
- Granting proper access control to authorized users
- Blocking unauthorized transfer of excel sheets and other spreadsheets to unknown domains
- Protect accounting and financial statement records of client companies
- Protect credentials of client companies

BPO and Call Centres

- Monitoring and tracking temporary employees
- Monitoring outbound client communications
- Safeguarding customer confidential data like credit card information, phone numbers, etc.
- Protecting servers containing confidential information and prevent them from getting tampere
- Protecting database of clients and vendors to prevent insiders from compromising confidential data
- Preventing employees from taking away data in personal USB drives or smartphones
- Monitoring activities of employees closely through web, application and screenshot monitoring
- Protecting prospect databases related to cold calling, upselling, cross-selling, etc.

Construction and Real Estate

- Protecting data related to property management, lease administration, finance, treasury and other tenant related activities
- Data related to potential clients and high value client
- Confidentiality of upcoming deals for acquiring land areas
- Avoiding infiltration into accounting systems and accessing personal information of tenants and addresses
- Avoiding risks of wiping out historical payment data
- Securing building management and communication technology ecosystems
- Protecting data related to virtual construction needs of a large construction project
- Monitoring many design and construction software systems
- Protecting multitude of cross-functional representatives such as legal, compliance, privacy, government affairs, audit and ethics
- Protecting confidential bottom margin data and sensitive pricing data

Defence and Homeland Security

- Securing information related to location of sensitive and secret basecamps
- Protecting sensitive information about secret raids and sting operations
- Monitor endpoints for possible data leakages
- Avoiding damage of critical evidences
- Protecting national security secrets and operational data
- Securing multi domain and multi-level data
- Protecting data of hidden assets and minimizing damage due to espionage
- Securing national level defence secrets from terrorists
- Proactively identify probable crime plot
- Accessing evidences for security investigations

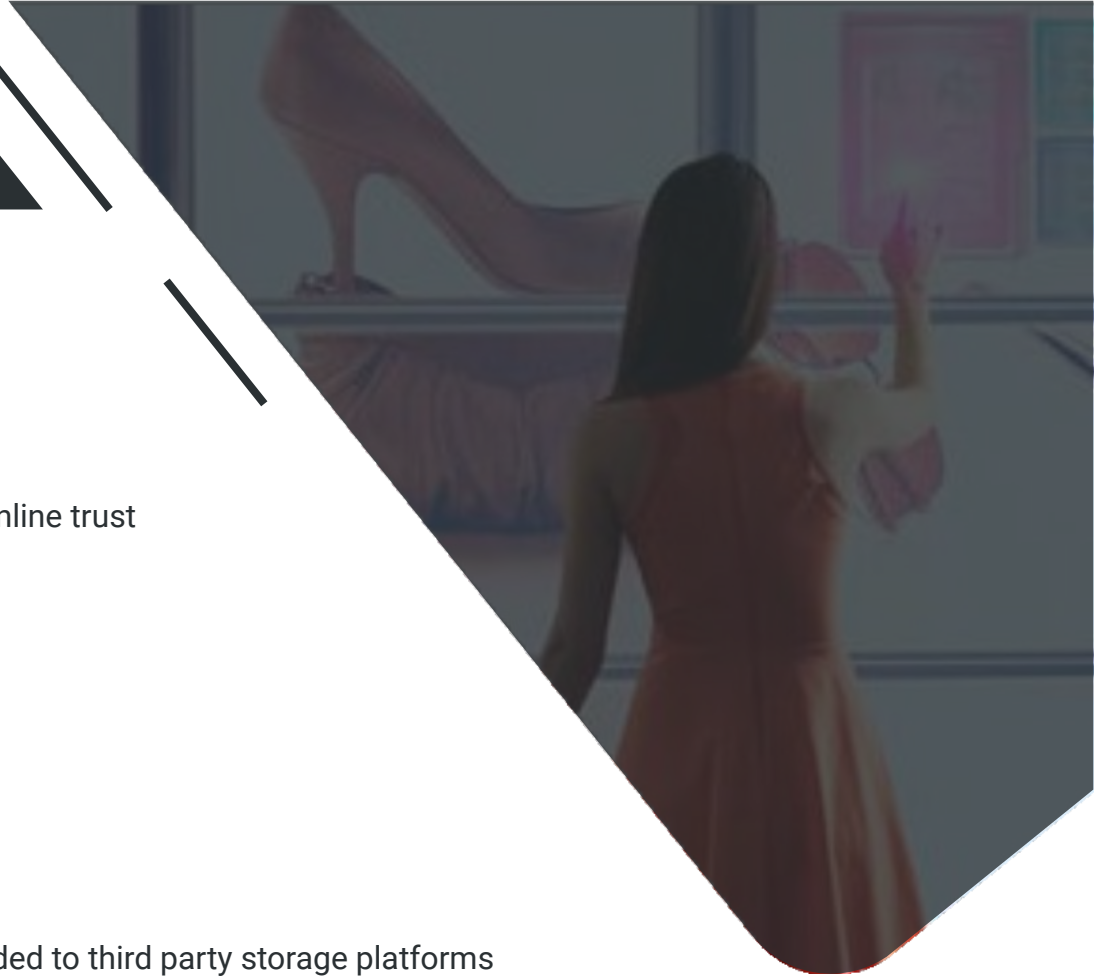
Digital Payment Providers

- Securing email addresses and mobile numbers of customers
- Confidentiality of 3rd party partner tie-up information
- Protecting financial records and social security numbers of customers
- Protecting transactional records of customers
- Avoiding cyber espionage and personal identity theft
- Securing transactions on mobile devices
- Safeguarding information exchange in case of third party service providers
- Protecting Application Program Interface (APIs)
- Protecting saved credit card information of customers
- Maintain compliance related to PCI and ISO 2700-series

Education

- Preventing leakage of exam question papers
- Monitoring cyber activities of students and teachers, lockdown mature and offensive content
- Detect probable cases of child pornography and uploading illegally recorded MMS
- Securing private records of students like parent information
- Protecting core intellectual asset that needs to be stored, accessed and used appropriately to fully realize its academic or commercial value
- Reporting of information risks between the institution's board and the owners, controllers and users of information assets
- Protecting recruitment and marketing data
- Securing staff data, especially when engaged in controversial or valuable research
- Protecting confidential training material

Fashion and Retail



- Adhering to compliances and security certifications to build online trust
- Monitoring and tracking logistics workforce
- Maintaining secrecy of upcoming designer launches
- Establishing security of loyal customer data
- Securing printing channels so that designs cannot be printed
- Monitoring and control of documents and photographs uploaded to third party storage platforms
- Monitoring work from home employees and temporary employees
- Monitoring productivity of employees at various outlets and factories
- Blocking applications and websites like movies, videos and adult content that can degrade employee productivity and culture
- Protecting vendor and supplier pricing data and information

Food and AgroTech

- Confidentiality of genetic data and recipes for best harvest seedlings
- Protecting IP related to genetic data
- Protecting patented formulation of hybrid species
- Protecting data that is being shared with suppliers and companies
- Protecting pesticides and GMO formulas
- Avoiding data leakages taking place unintentionally
- Securing information related to food distribution system, supply chain
- Securing food chemical information
- Protecting composition data of secret chemicals and ingredients in food manufacture
- Monitoring activities of employees in factory locations and warehouses

Government Organizations

- Monitoring worker productivity at all hierarchies
- Confidentiality of infrastructure information
- Prevention of media leaks
- Protecting sensitive payroll information of salaried government workforce
- Protecting confidential data of citizens
- Protecting public policy intellect
- Securing Information and Communication Technology (ICT)
- Building a predictive, preventive, protective, response and recovery action
- Securing product, people, process and technology information
- Protecting data while storage and transit of public information

Hospitals and Healthcare

- Protecting confidential patient health data
- Fortifying Healthcare Information Systems (HIS)
- MDM in healthcare such as online consultation, e-prescription
- Monitoring vendor transactions
- Reducing sensitive data leakage via email or printer channels
- Recording employee forensics for post crime analysis
- Defending contractual claims from partner organizations and third parties
- Protecting customer details from passing to third parties
- Protecting sensitive health information of diseases like HIV, cancer, sexual abuse cases, etc.

Insurance Companies

- Protecting KYC documents of clients
- Confidential corporate strategy data
- Protecting biometric data of customers
- Monitoring tablets and mobile devices of on-field sales agents
- Monitoring point-of-sale intrusions
- Protecting confidential strategic business information of commercial policies
- Protecting data from cyber espionage
- Securing company's server where customer data is stored
- Monitoring of call center employees where time is critical for performance
- Protecting personal information of clients like auto registration number, health record declarations, personal delinquency or wealth data, etc.

IT Service Providers

- Confidentiality of offshore client data
- Mobile Device Management for specific workforce
- Enabling trusted removable devices for enabling secure large data transfer
- Maintaining security of sensitive client data
- Monitoring personal and corporate emails for secured communication
- Securing critical data like inventory data, IT log management etc
- Protecting Information and Communication Technology (ICT) infrastructure
- Monitoring and blocking file uploads to various file servers
- Productivity monitoring of work from home and roaming employees

Manufacturing

- Confidentiality of product and manufacturing process designs
- Safety of supplier's data confidentiality
- Safeguarding factory layouts and process designs
- Protecting competitive tender quotes and pricings
- Preventing unauthorized access to sensitive systems and data
- Mitigating changes of malware infecting multiple industrial plants
- Safeguarding patented materials and composition data of produced materials
- Monitoring employees for productivity and remote factory locations
- Controlling web activities of employees thereby sanitizing internet usage and controlling available bandwidth
- Keep close track of temporary employees and third party consultants

Pharmaceutical & Biotech

- Protecting access to content formulation of drugs
- Securing drug APIs
- Safeguarding drug manufacturing and production processes
- Securing critical IPR formula of drugs
- Protecting R&D of new drugs
- Protecting customer details from passing to third parties
- Defending contractual claims from partner organizations and third parties
- Recording employee forensics for post crime analysis
- Reducing sensitive data leakage via email or printer channels
- Prevent internal espionage attacks on biotech companies that handles dangerous or hazardous material

Private Airlines

- Protecting confidentiality of travellers' confidential data like DOB and PAN
- Protecting confidentiality of frequent flyers database
- Protecting tariff variation and pricing strategy
- Safeguarding confidentiality of internal staff data
- Defending Critical Infrastructure (CI)
- Securing vulnerable supply chain data
- Securing air traffic control data
- Avoiding trade secret theft
- Safety of data on mobile devices, IoT and cloud database
- Safeguarding flight data logging systems

Product Companies and Start-ups

- Monitoring high value employees for probable attrition
- Safeguarding user information and payment details
- Confidentiality of product architecture and designs
- Protecting first-mover advantage
- Security of vendor software
- Productivity Monitoring work from home employees and BYOD environment
- Lock down data as per schedule of work or relax restriction on website usage outside office hours
- Gain value by complying with standard data security policies to gain more confidence from customer
- Protecting sensitive code base or design case from being infiltrated and leaked
- Helps managers to understand how team is working by tracking their online searches

Production and Media

- Securing scripts of highly rated unreleased movies and tele productions
- Protecting censor and certification previews from being leaked before public release
- Protecting cloud solution of video production industries where their creative assets are stored
- Protecting broadcast infrastructure of media houses
- Protecting content supply chain ecosystem
- Protecting data stored in video datacenters of broadcasting houses
- Managing effective URL filtering for inhouse and roaming employees
- Managing content on mobile devices effectively and blocking cameras as per geographical locations
- Blocking of large file transfers to usb devices and smartphones thereby protecting secured data
- Detecting hidden media insiders within the company who leak ”breaking news” information before they are broadcasted

Travel Service Providers

- Confidentiality of discount coupon codes
- Protecting loyal customer database
- Securing confidential marketing plans
- Avoiding unauthorized insider access
- Securing user identification, biometrics, digital ids of customers
- Protecting deal data with travel partners and protecting contact data
- Monitoring productivity of employees especially work from home and remote employees
- Apply web filtering, application filtering and screenshot monitoring to monitor high risk employees

inDefend Product Insights

Learn more about our product

Product Highlights

Wider Monitoring & Lockdown Coverage

- Devices
- Printers
- Corporate Emails
- Cloud Emails
- Websites
- Web File Uploads
- Chat Clients
- FTP Clients
- Servers
- Bluetooth
- Wifi and Hotspots

Advanced Pattern Recognition

- Text based
- Pattern based
- Credit card patterns
- Social Security Number patterns
- Optical Character Recognition
- Able to read most commonly used file formats

Widest Platform Coverage

- Windows
- Macintosh
- Linux
- Android
- iOS
- Windows Servers

User Behaviour Analytics

- Analyse end user behaviour
- Works in remote and work-from-home scenarios too
- Supports data transferred through public WiFis, internet dongles and personal hotspots
- Build up user profiling based on Employee Reliability score
- Mirror and compare specific employees' activities against rest of team or department or region
- State of the art organizational risk assessment dashboard and app

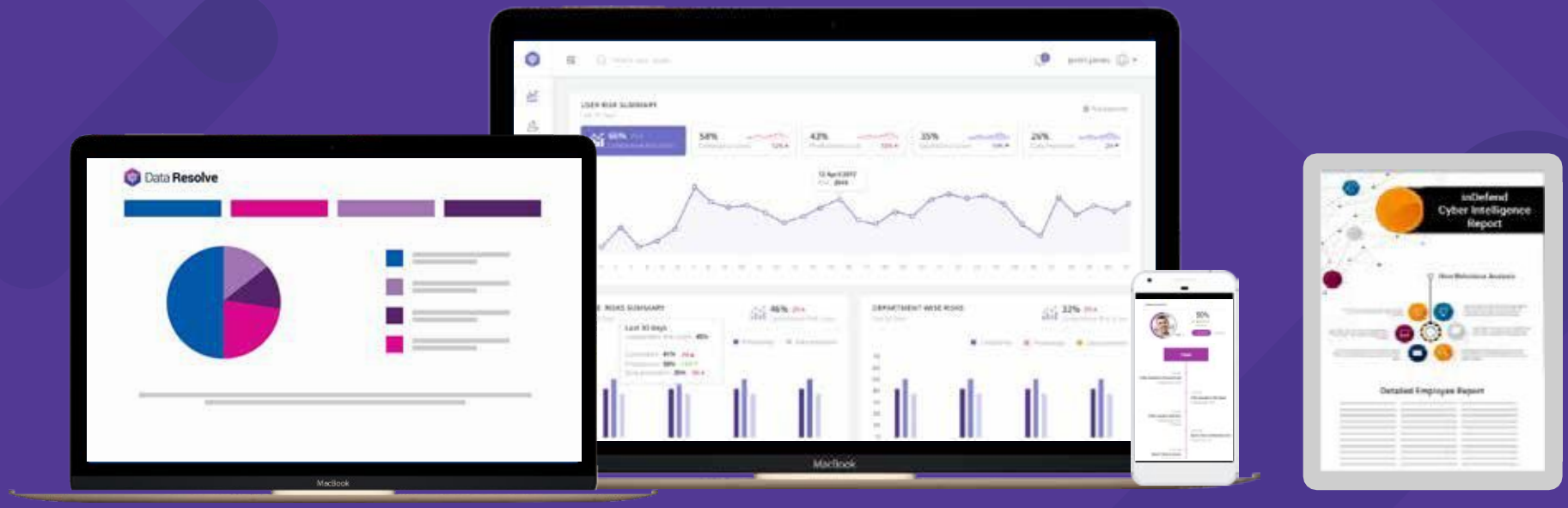
Advanced Features

- Silent Remote Installation of Agent
- Password protected uninstall of agents
- Offline tracking capability
- Remote tracking capability
- Separate report based on daily schedules and work times
- Role based reporting
- Screenshot capability to better insights
- Email, SMS, App based reporting
- Daily scheduling of reports and notifications

Deployment Options

- Cloud server based deployment – highly scalable, low setup cost, rapid deployment capable
- Dedicated server based deployment – scalable in steps, higher setup cost, sets up in an hour
- Private Dedicated Cloud deployment – best of both above

inDefend - Flexible and Powerful Analytics



ABOUT DATA RESOLVE TECHNOLOGIES

Data Resolve Technologies is emerging player in Data Security, focused on 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 behavior and report any anomalous intentions detected, helping them build a secure ecosystem and increasing employee productivity.

VISIT OUR WEBSITE

www.dataresolve.com

TO SPEAK WITH OUR CYBER SECURITY CONSULTANT

Call : +91 9599936473

Email : marketing@dataresolve.com

OUR WORLDWIDE PRESENCE

INDIA, EMEA, ASEAN, CANADA, UK

Data **Resolve**