Data Resolve

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

The Executive Dashboard

The solution gives a holistic picture of the entire organization's health score based on the data protection score, compliance score and productivity score.

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 and Chat Activities. 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. Based on the incidents created and the incident hits, inDefend Advanced calculates the scores which get populated on the Executive Dashboard, along with the Forensic Timeline of the organization. The scoring is available for a particular zone, department and user.

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.

System Requirements

inDefend Advanced Server requirements

CPU - Xeon Processor 4 Cores or above
Operating Systems - Ubuntu 18.04 LTS (Bionic Beaver)
RAM - 8GB RAM or above
Storage - 100 GB or above

inDefend Advanced End point requirements

Operating System

Windows (32 bit and 64 bit)
Windows 7 service pack 1
Windows 8
Windows 8.1
Windows 10

RAM: 4 GB RAM (Windows 7 to 8.1) & 8GB (Windows10)

Linux (64 bit):

Ubuntu 18.04

RAM: 6 GB RAM

Storage

1 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 pushed from manager to employee on a daily basis
Report can be downloaded in pdf format

Executive Summary

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.

Secures data from critical insider threats of both local and remote users. User programmable and easy to use centralized Administration Console with highly customizable parameter settings.

Ability to record, gather data, analyze and action based on block or reporting (System/Email/SMS) parameters real-time.
Flexibility to be deployed on own premise or on 3rd Party or Private Cloud.
Advanced in-built device control capabilities to enforce encrypted data protection on lost or stolen devices including removable media.

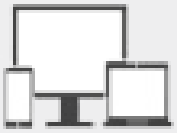
Fraud Prevention
By Monitoring and Analyzing patterns of User Behavior using parameterized red flag patterns and content monitoring.

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.

Key Features

Integrated Dashboard with Unified Console



Multi-Platform Support

Executive Reporting

Activity Monitoring

Hybrid Server Architecture with Multi Tenancy

Stealth Mode

Cyber Intelligence Reporting

Resource Footprint

ML Based UEBA

Easy Deployment

inDefend App Based

ROI Driven with Lowest TCO

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

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

Risk Analysis

Policy Compliance Scores
Data Protection Scores
User Activity Scores
Overall Organisation Health Scores
Regional/Zonal/Departments Analysis of Scores
Identify and Analyse Risky Users
Create Dynamic User watch list
Historical Reliability of Users
Activity Timeline of Users

Policy System

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

Reporting System

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

Executive Dashboard

Provide a bird's eye view of the activities inside the organization to the CXO's of the organization.

Provide various risk scores, productivity score, compliance score and comparative risk scores from overall organization level to individual user level.

Rule Builder Screen

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

Incident Summary Screen

Provides alerts for incidents generated from various channels like email, applications, internet and devices etc. Provides comparative change score between incident counts in previous and current week.

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.

inDefend Secure Email Gateway(SEG) offers the capability to monitor and block outgoing Emails with sensitive content via gateway.

inDefend Secure Email Gateway(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.

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 flow logs
Organization level mail activity analytics
Outbound email security
Content analysis
Email Quarantine
Email Alerts

CONTACT US FOR A FREE TRIAL
Demo Session- https://downloads.dataresolve.com/free-trial

ABOUT DATA RESOLVE TECHNOLOGIES

Data Resolve Technologies is emerging player Data Security company, 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
WhatsApp us at +91 9599936473 | Email: marketing@dataresolve.com
OUR WORLDWIDE PRESENCE India, EMEA, Canada, Myanmar, Sri-Lanka, ASEAN
DATA RESOLVE TECHNOLOGIES HEAD OFFICE
ABL Work Spaces, B-6, Block-B, Sector – 4, Noida – 201301, INDIA
GCC OFFICE Suite 28, 2nd Floor, Clover Bay Tower, Business Bay, Dubai, UAE
CANADA OFFICE 80, Atlantic Avenue, Toronto, Ontario, Canada
MYANMAR OFFICE- 2C/393-395, City shine tower, Bo Aung Kyaw Road, Kyauktada Township, Yangon, Myanmar