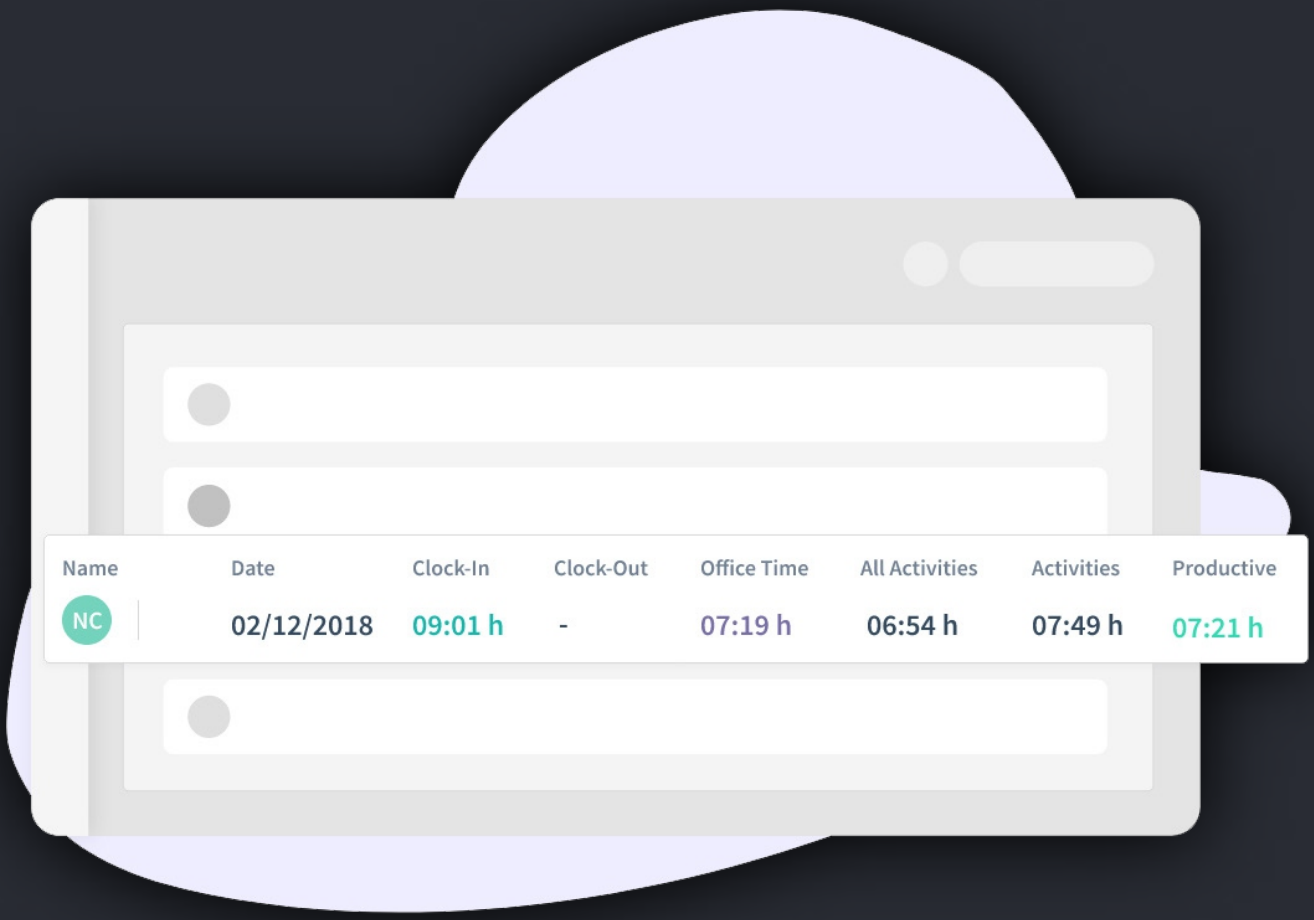
White Paper

itSimple
बैकअप सरल है

Data **Resolve**

Monitoring employee activities through screenshot



www.dataresolve.com

With the workforce becoming global, 9-5 workplace is a thing of the past. The connected world gives employees the flexibility to decide how, when, and where to work. As geographical boundaries blur, employers are now focused on hiring the best fit for a job irrespective of the location.

However, computer and internet have become a double-edged sword. Be it SME, multinational organization, or remote opportunities, the misuse of e-mail and internet can impact productivity and can also lead to expensive lawsuits.

Did You Know?[1]

> **American businesses lose 40% productivity each year due to non-work-related internet surfing**

> **64% of employees visit non-work-related websites on the job every day**

> **46% of employees actively looking for a new position on the internet during work**

> **85% of employees use organization email for personal reasons**

> **37% of employees constantly surf the internet at work**

Apart from hampering business productivity, employees and system administrators, who have access to database servers, desktop computers, and external devices can also risk sensitive enterprise data by leaking them knowingly or unknowingly. According to 'Cost of a Data Breach Study' by Ponemon Institute[2], the global average cost of a data breach in 2018 is **$3.86 million,** up by **6.4% from 2017.**

To address these issues, employers monitor screenshot to capture visual evidence to serve as an audit trail or for use in after-action follow up. In this white paper, we will detail:

- How screenshot monitoring helps in combating data leak?
- Benefits of screenshot monitoring
- What else to monitor?
- Characteristics of an employee/screenshot monitoring software

1 https://www.sentrypc.com/business/statistics.htm

2 https://www.ibm.com/security/data-breach

How screenshot monitoring helps in combating data leak?

Employee monitoring, specially screenshot monitoring, recording computer activity and history playback, or keystroke monitoring is an accepted norm at many organizations. While the reasons to monitor are many, we have highlighted three losses that employee activity monitoring can save your organization from.

Did You Know?

A research[3] reveals that 66% of employers monitor Internet connections, 45% track keystrokes, and 43% review computer files.

Frauds

Organizations often suffer loss due to employees passing sensitive information for their gain. Fraudulent activities do not cost only the company money but also damages its reputation and the confidence of the customer. By monitoring computer activity, organizations can keep a check on the online activities and data transfer and prevent such loss.

Cyberslacking

Cyberslacking refers to employees becoming distracted by technology in the workplace, usually due to personal, non-work-related Internet usage. Employees may use the internet at work to check and send personal emails, use social media website to connect to friends, access non-work-related videos, or shop and play games online. A ballpark estimate suggests that organizations lose 2.5 hours per day per employee on an average to cyberslacking. Screenshot monitoring can make that loss count.

Legal Hassles

According to the ePolicy Institute[4], 9% of organizations have battled lawsuits triggered by employee email, which can cost them millions of dollars. The violation of ePolicy do not only result in multi-million-dollar lawsuits but can risk the organization to public relation disasters, public embarrassment, industrial espionage, and deliberate sabotage. Monitoring your employees' activities can save your organization from all these threats.

3 https://www.computerworld.com.au/article/print/320518/dark_side_dlp/
4 http://www.epolicyinstitute.com/

Benefits of screenshot monitoring

While the benefits of deploying an employee monitoring software are many, let us look at some of the most common benefits:

Prioritization

If the senior leadership/managers have visibility on what employees are working on, they can help them prioritize work and prevent errors at the initial level, before it goes out of control. A monitoring tool can also measure the amount of actual time taken to complete a task, and plan future tasks accordingly.

Transparency on Employee Performance

Screenshot monitoring does not only prevent unethical usage of time, internet, or information by an employee but also provides valuable insights into the performance. It helps the management identify the top performers and the lowest performers, thereby making the appraisal system transparent.

Less Time Wastage

Employees spend almost 30% of their work time on an average doing personal work, which includes surfing the internet, sending emails, etc. Monitoring software can help organizations keep a check on unproductive time.

5 https://www.computerworld.com.au/article/print/320518/dark_side_dlp/

6 http://crowdresearchpartners.com/wp-content/uploads/2017/07/Insider-Threat-Report-2018.pdf

What else to monitor?

A 2018 Crowd Research reveals that 94% of organizations deploy some method of monitoring users and 93% monitor access to sensitive data. Thanks to technology, organizations can now monitor almost all employee activities including:

Email

Survey reveals that nearly 43% of employers monitor emails of employees. Since the organization owns the email system, they have the right to monitor and review the messages sent and received both within and outside the organization. Some employers also encrypt the messages to protect the content privacy, which ensures the message can be read only by the sender and the intended recipient.

Internet

More than two-thirds of the organizations worldwide monitor internet and app usage of the employees, including the URLs visited, comments and posts on various forums and social media websites, and transactions made online. Many companies also block URLs of specific categories that are not necessary for their business.

Phone

Monitoring of phone depends on the nature of the business. While customer care centers monitor all calls for quality assurance and to measure the performance of the executives, organizations concerned about phone misuse and productivity loss only track the phone numbers and the time spent on the phone.

Location

With employees going mobile, location tracking has gained popularity, mainly to keep track of the salesforce. Employee monitoring tools can track the exact location of the employees with the help of Global Positioning Systems (GPS) devices, to keep a check on the activity and location of the mobile employees during work hours.




Characteristics of an employee/screenshot monitoring software

Employee monitoring software gives organizations the ability to:

Discover

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

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

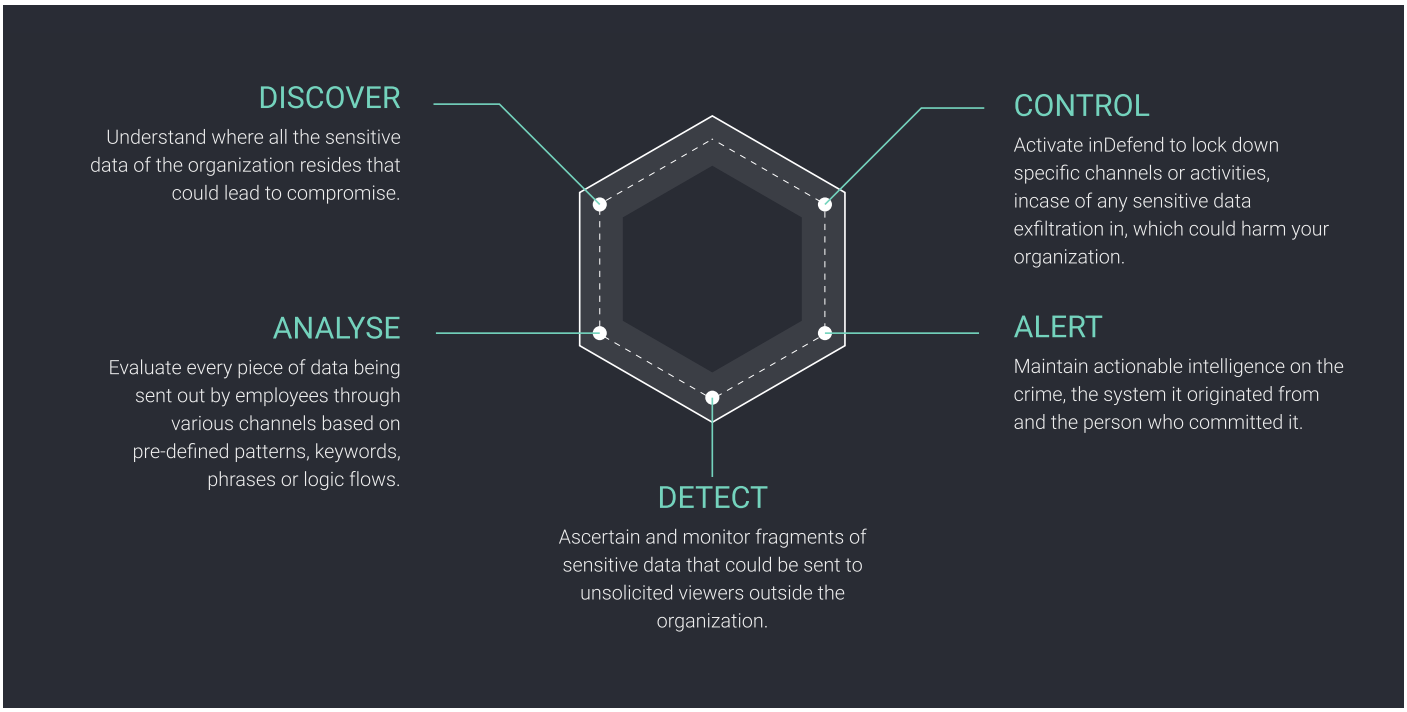
Maintain actionable intelligence on the crime, the system is originated from, and the person who committed it.

Detect

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

Control

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



To deliver these capabilities, typical employee monitoring software includes features such as:

Centralized console for

- Advanced reporting & analytics framework for all device and network activities
- Silent monitoring of all activities
- Central installation of upgrades on end-user computers
- Flexibility to monitor and control offline computers

Activity analysis for

- Detailed view of the suspicious and unauthorized events happening within the organization
- Insights of the critical data leakage, user non-compliance with respective proofs
- Option to filter the activities for a duration
- Real-time alerts in email for sensitive events

Monitoring, alerting, and/or blocking capabilities for

- Emails
- File uploads
- Attachments
- Rogue or unproductive applications
- USB storage
- Malicious web browsing activity

Detailed logging of

- Browse Activities
- Application Usage
- Searches
- USB devises usage

Shadow logging

Screenshot monitoring

inDefend: Unified User Behavior Analytics and Insider Threat Management Solution

inDefend is a one-stop solution to help protect your data from all kinds of insider threats within your organization. It allows you to monitor your employees' behavioral patterns and pinpoint potential avenues for data exfiltration. This solution is built to achieve complete transparency over all the digital assets residing within your organization. With our unified solution, you can quickly tackle various kinds of security issues related to data exfiltration. It offers a proactive approach to the organization as follows:

Insider Threat Management

Get a complete user behavior analysis to protect your sensitive data from being compromised by employees by monitoring their activities and communication habits.

Real-time Alerts

Get real-time incident alerts for any data exfiltration activity that takes place within the organization.

Event-based screenshot monitoring

Notify IT administrators only of the events they are interested in, and not the rest. Security experts can also customize the alerts, including the message, the source, the level, the time, and the event ID.

Title-based screenshot monitoring

Monitor and sort user activity logs for the computers using title-based monitoring. Take screenshots only when users use certain keywords in the title. For example, when a search contains ‘job’ in the title, activate screenshot monitoring.

Accurate Analytics

Get detailed cyber intelligence reports which highlight the critical and sensitive data leakage scenarios with granular visibility into team dynamics and organizational ecosystem.

Superior Control

Block specific channels or devices in case any sensitive data exfiltration is detected.

Enforced Encryption

Secure multiple endpoints with implemented encryption on external storage devices to restrict the use of sensitive information or files.

Optical Character Recognition (OCR)

Extract text from images and process them further to detect the presence of sensitive content like keywords, regular expressions, or file types with OCR.

Implementing a better security system is the need of the hour for all organizations. Our unified solution inDefend can secure your organization from data exfiltration. inDefend is designed to prevent data leakage via various communication channels and proactively keep you informed of any sensitive data exfiltration attempt on-the-fly. So, start securing your organization against data exfiltration with inDefend.

CONTACT US FOR A FREE TRIAL

ITS Technology Solution Pvt. Ltd.
Tel. : +91 120 4155477 | Mail : sales@itsimple.in | Web : www.itsimple.in | C-10, Sector-3, Noida, U.P (Delhi)

VISIT OUR WEBSITE
www.dataresolve.com

TO SPEAK WITH OUR CYBER SECURITY CONSULTANT
Call : +91 92666 03983
Email : sales@dataresolve.com

OUR WORLDWIDE PRESENCE
India, UAE (Dubai)

DATA RESOLVE TECHNOLOGIES HEAD OFFICE
ABL Work SpacesB-6, Block-B,
Sector – 4, Noida -201301

ABOUT DATA RESOLVE TECHNOLOGIES
Data Resolve Technologies is an IIT Kharagpur incubated company, focused towards 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 behaviour and report any anomalous intentions detected, helping them build a secure ecosystem and increasing employee productivity.

Data **Resolve**