Data Resolve

WHITEPAPER:

Data protection in the time of COVID-19

Overview

COVID-19 (a.k.a. coronavirus) has ushered a new era in the white-collared world where working from home is a necessity and no longer a privilege. As organizations across the globe are asking employees to work from home (WFH) to prevent the spread of the virus, it also necessitates companies to take measures to secure their data from viruses (avoid data leak).

A national health emergency like this is also a health emergency for your organizational data. As more than 1.84 lakhs people across the globe are affected by the virus (as on March 17, 2020), organizations are forced to ask their employees to work from home. This has resulted in endpoints (laptops) and its data necessarily moving out of the office premises, thereby exposing sensitive data to intentional or unintentional leakage.

What are the risks associated with work from home?

Working from home might help quarantine the spread of virus, but it risks misuse and leakage of sensitive data. Therefore, many organizations resort to monitoring employee activities for the following reasons:

Data Theft

A survey reveals that 47 percent former employees take confidential company information with them before they leave the organization, breaking non-disclosure agreements. While the connected world had increased productivity and made the workforce mobile, it has also given employees new opportunities to access and steal sensitive information from organizations. 53 percent of employees send business-related information to personal email and cloud-based file-sharing accounts. Work from home significantly increases the risk of intentional data theft as employees use unprotected and unmonitored home networks.

Frauds

Organizations often suffer a loss due to employees passing sensitive information for their gain.

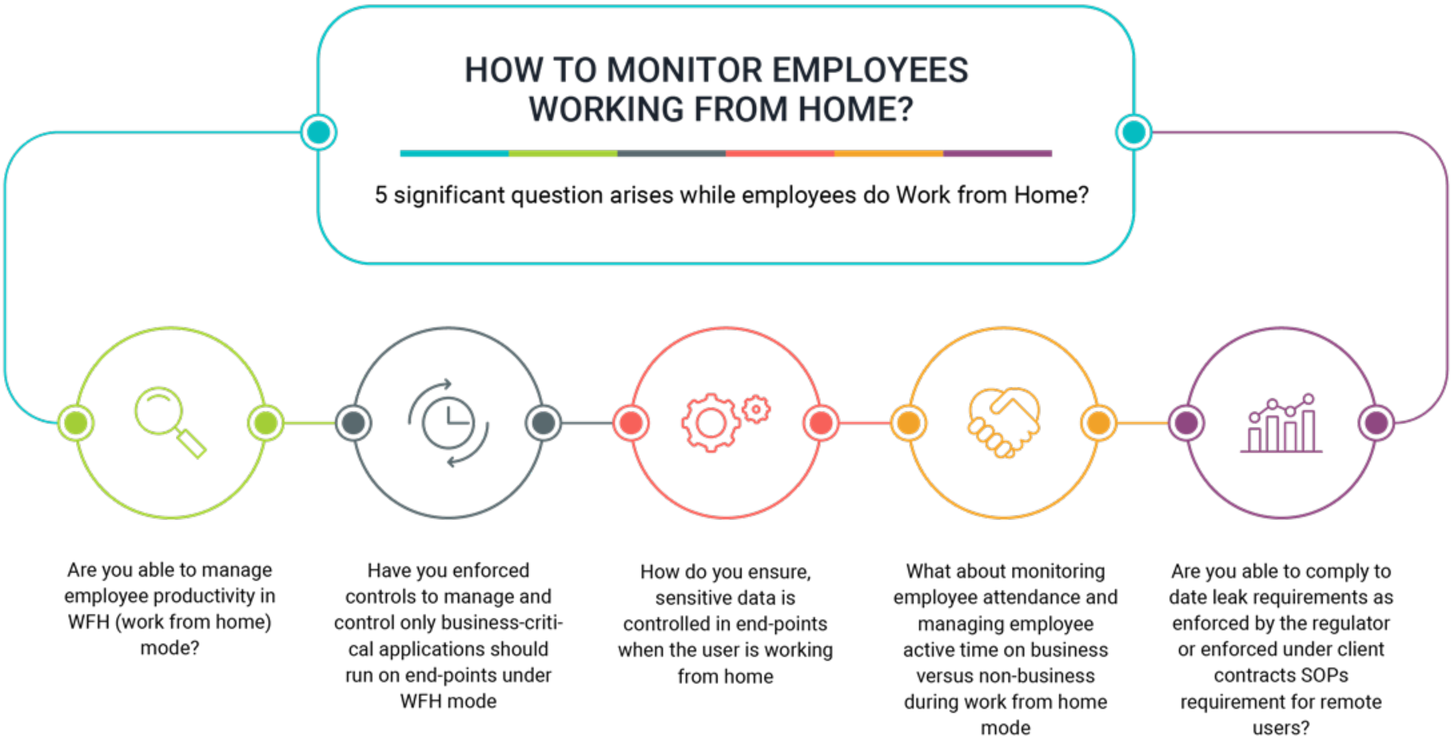
Fraudulent activities do not cost only the company money but also damages their reputation and the confidence of the customer. While employees are working from home, it is difficult for organizations to keep a tab on their online activities to prevent such loss.

Unintentional Data Breaches

Due to absence of edge security controls like Firewall, which protects unintentional data breaches within the organizational network, the risk of data being exposed to hackers increases significantly. While COVID-19 is raging across the globe and forcing the workforce to work from home, hackers are on the hunt for such unsecure endpoints.

Employee Productivity

For organizations that do not otherwise encourage work from home do not have metrics to monitor employee productivity at home. For example, many organizations log attendance on the basis of first log-in last log-out. With employees working from home, tracking their involvement in work, measuring KPIs, and keeping a tab on the time spent on various applications and URLs to understand how productive they are is a challenge.



HOW TO MONITOR EMPLOYEES WORKING FROM HOME?

5 significant question arises while employees do Work from Home?

Are you able to manage employee productivity in WFH (work from home) mode?

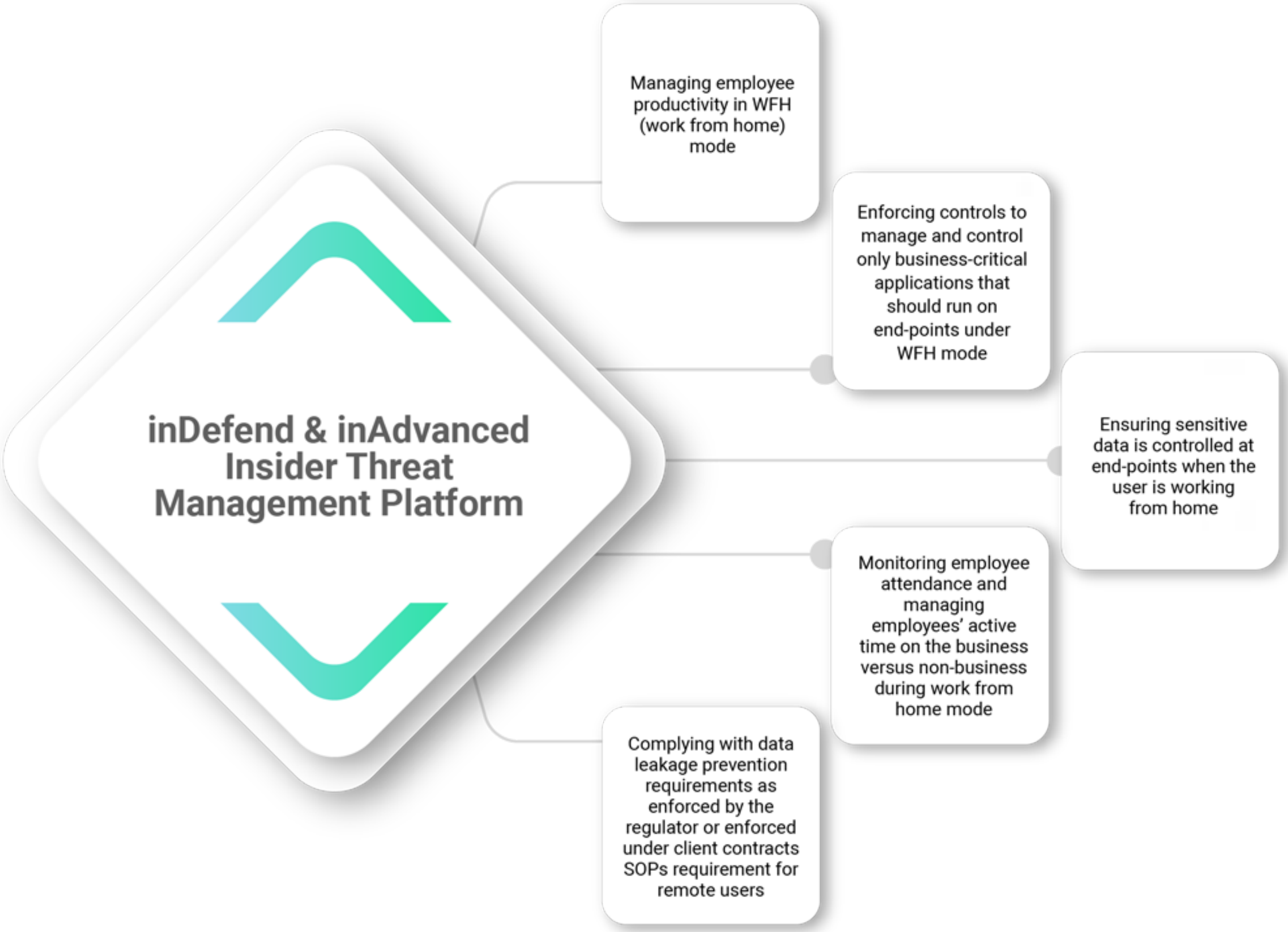
Have you enforced controls to manage and control only business-critical applications should run on end-points under WFH mode

How do you ensure, sensitive data is controlled in end-points when the user is working from home

What about monitoring employee attendance and managing employee active time on business versus non-business during work from home mode

Are you able to comply to date leak requirements as enforced by the regulator or enforced under client contracts SOPs requirement for remote users?

Companies are able to overcome several Work from home challenges in these times, by leveraging our inDefend & inAdvanced Insider Threat Management Platform



inDefend & inAdvanced Insider Threat Management Platform

Managing employee productivity in WFH (work from home) mode

Enforcing controls to manage and control only business-critical applications that should run on end-points under WFH mode

Ensuring sensitive data is controlled at end-points when the user is working from home

Monitoring employee attendance and managing employees' active time on the business versus non-business during work from home mode

Complying with data leakage prevention requirements as enforced by the regulator or enforced under client contracts SOPs requirement for remote users

Data Resolve

Cloud Based Cyber Security And Intelligence for Enterprises

CONTACT US FOR A FREE TRIAL

VISIT OUR WEBSITE

www.dataresolve.com

TO SPEAK WITH OUR CYBER SECURITY CONSULTANT

Call : +91 92666 03983
Email : ask@dataresolve.com

OUR WORLDWIDE PRESENCE

India (Noida, Gurgaon, Mumbai, Bangalore)
UAE (Dubai)

DATA RESOLVE TECHNOLOGIES HEAD OFFICE

ABL Workspace, 3rd floor, B-6, Sector-4,
Noida, Uttar Pradesh 201301, INDIA
Phone: +91-9266603983

ABOUT DATA RESOLVE TECHNOLOGIES

Data Resolve Technologies is an IIT Kharagpur incubated startup, 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 increase employee productivity.

Start your **FREE Trial** today **SIGN UP**