White Paper

Data Resolve

itSimple
बैकअप सरल है

Monitoring Remote Employees

www.dataresolve.com

The 9-5 workplace is a thing of the past. Technology has made the workforce more effective, productive, and engaged. With work no longer restricted by boundaries and geographies, remote work is becoming a norm. Employers are looking to hire the best fit for a job irrespective of the location as the connected world allows for flexibility in how, when, and where people work.

> Globally, 56%[1] of companies allow employees to work remotely.

However, cybersecurity remains a challenge for companies. While large enterprises have established security policies for remote employees, SMEs do not pay much attention to this area. Reports suggest that 72%[2] of data breaches occur at companies with under 100 employees.

Why is work from home gaining popularity?

The workforce today demands increased flexibility with hours, location, and personalized benefits. While the reasons for remote working are many and differs across geography and profile, five primary reasons why both employers and employees prefer to work from home are as follows:

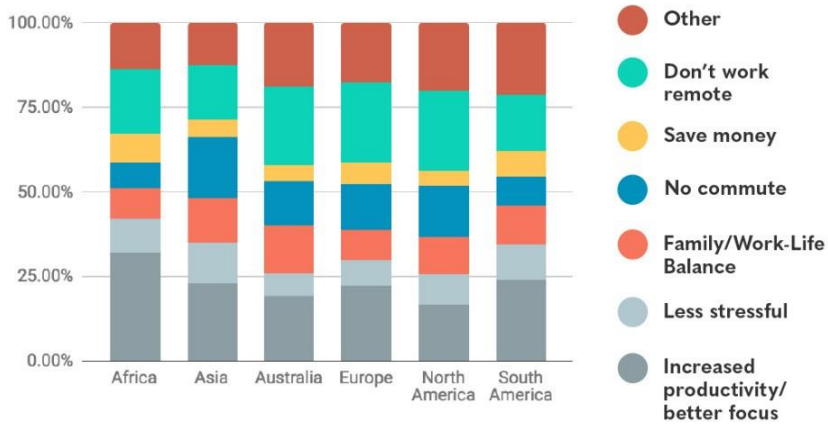
- Increased Productivity: Remote work is helping to boost productivity as it cuts down distractions like talking to other employees, impromptu meetings, discussions, and more. With the employees being more focused, they tend to be more productive and can accomplish more in less time.
- Curb Attrition: Millennials, which account for the most significant workforce across geographies, are tech-savvy and prefer working remotely over being in office. Senior-level employees also find work from homeless stressful and prefer to work remotely over retiring. Therefore, remote work options allow employers to hire younger workers, retain senior employees, and curb attrition.
- Maintain Family/work-life Balance: Working remotely enables employees to spend more time with their family without compromising on productivity. Focused on getting the work done rather than the work timings, they can adjust their calendars to accommodate both professional and personal commitments, without compromising one for the other.
- No Commute: Working remotely also contributes to the environment, as employees do not add on to the greenhouse gas emissions by using a car. At a time when global warming is a severe issue, remote work is responsible for eliminating almost 55%[3] of greenhouse gas emissions (equivalent to emissions from 10 million cars annually).
- Savings: Remote work can significantly decrease operating costs. Forbes report that Aetna saves $78 million in real estate and American Express saves around $12.5 million annually due to remote workers. Additionally, employees also save money as they do not need to spend on the commute and other essentials required to travel.

1 https://www.owllabs.com/state-of-remote-work#keyfindings

2 https://www.helpnetsecurity.com/2018/11/19/remote-working-cybersecurity/

3 https://www.flexjobs.com/blog/post/the-positive-environmental-impact-of-remote-work/

Why do people choose to work remote



What are the risks associated with remote employees?

Flexibility in work schedule might give more freedom to the employees, but it can also be distracting. When employees work out of the home office, it's easy to let boundaries blur between work and personal stuff. Therefore, many organizations resort to monitoring employee activities for the following reasons:

- Cyberslacking: A ballpark estimate suggests that organizations lose 2.5 hours per day per employee on an average to non-productive usage of the Internet, which includes personal emails, using social media, accessing non-work-related (sometimes inappropriate) videos, shopping, or playing games online. Employee activity monitoring can make that loss of productivity count.
- Data theft: A survey reveals that 47 percent[4] of 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.
- 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. With proper employee monitoring, organizations can keep a check on the online activities and data transfer and prevent such loss.

4 https://www.businessnewsdaily.com/5168-employee-monitoring-software.html

How to monitor remote employees?

Monitoring to prevent employees from wasting time on the Internet and protect data – these are the two main reasons for organizations to monitor activities of their remote employees. A research[5] reveals that 66% of employers monitor Internet connections, 45% track keystrokes, and 43% review computer files.

Did you know?

90 percent[6] of organizations feel vulnerable to insider attacks.

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

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

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.
- 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

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, UAE (Dubai)

DATA RESOLVE TECHNOLOGIES HEAD OFFICE
G-24, 2nd Floor, Sector-6, Noida,
Uttar Pradesh, INDIA 201301
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 increasing employee productivity.

Data **Resolve**