DTEX
THE WORKFORCE CYBER INTELLIGENCE COMPANY™

EBOOK | REMOTE WORKFORCE SECURITY

Top 3 Security Risks to Address When Managing a Remote Workforce

Need to secure hundreds or thousands of remote workers and their devices?

Learn how in this new remote workforce security ebook.

Remote Working is a Global Trend

As organizations tap into the global workplace and provide more work-life balance, there has been a significant increase in the number of employees working from home

Over the past decade, there has been a significant increase in the number of employees working from home (WFH).

Since 2007

159% Rise in US remote workforce
26 Million – Americans working from home

50% Increase in UK mobile workforce

68% Percentage of Australian companies that allow employees to work remotely

WFH is clearly a growing, global trend.

DTEX

3 Major Security Risks Raised by a Remote Workforce

With the outbreak of COVID-19 and the desire to #flattenthecurve, hundreds of thousands, perhaps millions of additional employees are now working from home.

Despite the health and corporate benefits of working remotely, there are serious security risks that come with this trend, including these top 3 security concerns:

Increase in Accidental Data Loss

Increase in Malware Infections

Increase in Unprotected Backups

If not addressed, these risks could mean negative consequences for companies and their employees, including the loss of valuable data and confidential information, as well creating vulnerabilities that can be exploited by malicious attackers.

Security Risk #1

Increase in Accidental Data Loss

78%

Increase in accidental data loss when employees work from home

We know from previous experience that there is a 78% increase in accidental data loss when employees work from home since users often sacrifice compliance and security policies for usability.

Fairly Safe Behavior

Many organizations use Microsoft OneDrive or Google Drive for collaborating, storing and sharing confidential business documents.

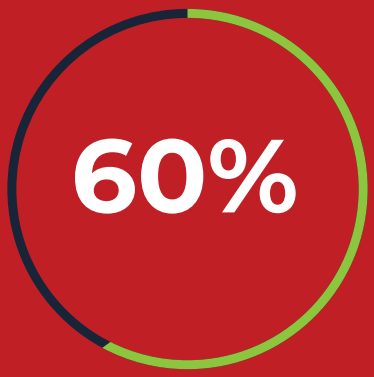
Risky Behavior

To make access easier for others, remote users purposely or accidentally publicly share links to confidential documents. This means that sensitive information and/or intellectual property may be exposed.

DTEX

Security Risk #2

Increase in Malware Infections



Increase in malware infections from remote users

Organizations can also expect a 60% increase in the number of malware infections for remote users.

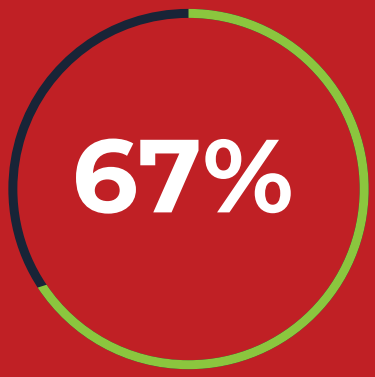
Risky Behavior

- Remote users increase recreational web browsing on corporate devices instead of personal devices.
- Corporate laptops, for example, that were once kept in the office are now usable all the time, including nights and weekends when personal web browsing and emailing spikes.
- WFH employees don't stay connected to the corporate VPN 100% of the time. Devices will more frequently be connected to relatively unsecured home and public networks where phishing attacks and malware infections are more prevalent.

DTEX

Security Risk #3

Increase in Unprotected Backups



Increase in the number of unprotected backups

When a large number of employees work from home, we've seen a 67% increase in the number of unprotected backups.

Risky Behavior

Remote employees realize they can work faster with large amounts of data on their local machine vs. constantly accessing databases through their corporate VPN. This provokes them to copy large amounts of data to local hard drives or USB tokens.

While this might mean faster and easier work for the employee, it also means that potentially large amounts of confidential or proprietary data is openly stored on local devices for attackers and malware to access.

The widespread decision organizations have made to allow users to WFH is a great thing – both for business and for humanity during the COVID-19 crisis.

However, it must be done safely.

To solve these issues, we recommend:

1) Reviewing (and potentially updating) your corporate policies with respect to acceptable use of company devices and information.

2) Installing security software & controls on company devices that are now headed home.

3) Communicating your policies to employees and workers to ensure they are trained and aware of how to safely work from home.

If organizations heed this advice, they can ensure that their business runs smoothly and, just like their users, is protected from harm during these trying times.

DTEX

As a result of the recent surge in numbers of remote workers and the corresponding increase in potential security risk, DTEX has created a program to provide extra assistance to customers and select companies that need to rapidly secure remote workers.

Contact us today at **remote.work@dtexsystems.com** to learn more and better secure your remote workers.

About DTEX Systems

DTEX Systems is the world leader in Workforce Cyber Intelligence and committed to helping enterprises run safer and smarter. Only DTEX dynamically correlates data, application, machine, and human telemetry to stream context-rich user behavior and asset utilization analytics that deliver a first-of-its-kind human-centric approach to enterprise operational intelligence. Hundreds of the world's largest enterprises, governments and forward-thinking organizations leverage DTEX to prevent insider threats, stop data loss, maximize software investments and deployments, optimize workforce engagement, and protect remote workers. DTEX has offices in San Jose, California and Adelaide, South Australia and is backed by Northgate Capital, Norwest Venture Partners, Wing Ventures, and Four Rivers Group. To learn more visit: www.dtexsystems.com.