REMOTE EMPLOYEE MONITORING

How to Make Remote Work Effective and Secure
Cybersecurity specialists treat remote employees as a threat, and they’re right to do so. However, remote work isn’t a temporary trend — it’s here to stay. Between 2017 and 2018, 36 million (or 25%) of US employees sometimes worked at home according to the US Bureau of Labor Statistics. For lots of specialists, the ability to work outside the office is an important benefit when choosing an employer. Moreover, remote access is required on business trips, for third-party vendors, and during emergencies like pandemics, transport collapses, and extreme weather events.

In such cases, IT specialists have to be ready to ensure effective remote employee monitoring as well as secure and comfortable remote access to corporate systems. It’s also important to keep an eye on employees’ productivity — after all, some employees can be distracted by domestic chores. In this article, we take a look at common myths about teleworkers, cybersecurity issues related to remote work, and the best tools and practices to manage employees working from home.
TOP 5 MYTHS ABOUT REMOTE WORKERS

There are a lot of misconceptions surrounding remote employees. Lots of employers are hesitant to allow employees to work from home because they believe it’s ineffective, costly, and insecure. But statistics prove these beliefs to be largely false. Let’s take a look at the real facts about remote workers and debunk these myths.

Myth #1 — Employees work less when they’re out of the office.

Some managers believe that employees stop working when they aren’t under constant supervision. There are good reasons for such an opinion: after all, it’s easier to get distracted by social media or domestic chores when you’re at home.

Stanford University conducted a two-year study to find out if telecommuters indeed work less. What they found was that most office employees who started to work remotely during the experiment showed a significant productivity boost. Moreover, according to the 2019 State of Remote Work report by Buffer, 22% of remote employees say they have difficulty unplugging after work hours.

However, there are still lots of workers who can’t focus on their work at home. That’s why it’s a common practice to deploy remote employee time tracking and monitoring software to analyze and increase employee performance.

Myth #2 — Remote work is all about traveling.

You’ve probably seen hundreds of pictures and Instagram posts that portray remote work as lying on the beach or traveling to different cities and countries. It’s hard to imagine that with such a lifestyle there’s time to be productive.

But this picture is also rather far-fetched. According to Buffer, 84% of remote employees usually work from home, sometimes changing their working environment to a local cafe. Only 3% frequently work outside of their home city.

Myth #3 — Remote work is for small companies and startups.

This myth is partially true: it’s indeed more affordable for small businesses and startups to hire remote workers and save money on office rent. However, lots of large-scale
organizations offer remote (or partially remote) work as a benefit for employees. Also, the coronavirus outbreak has shown that organizations like Oracle, Amazon, Microsoft, Google, Twitter, and even NASA can switch to fully remote work within a few days.

Myth #4 — Remote workers feel lonely and left out of the conversation.

For lots of people who are used to office chatter, locking themselves up to work from home might seem like social isolation. But in fact, work-related communication doesn't stop outside the office. According to a TINYpulse survey, 52% of telecommuters talk to their manager daily. Another survey by TalentLMS shows that when remote workers feel lonely, 43% use communication apps to talk to their team and 37% visit the office.

Myth #5 — Establishing remote access is costly and insecure.

Establishing secure and fast remote access indeed requires purchasing dedicated cybersecurity solutions (virtual private networks, firewalls, remote monitoring software, time trackers, etc.). However, these tools cost far less than renting an office and creating a comfortable workspace. Companies that participated in the Stanford study mentioned above reported saving up to $2,000 a year per employee on office expenses.

Working remotely is also beneficial for employees, as they don't need to spend time getting to the office, saving them up to $7,000 per year on daily expenses.

Remote employees in figures

- 22% Have difficulty unplugging after work hours
- 84% Usually work from home
- 3% Usually work from a foreign city
- 52% Communicate with their manager daily

Companies save up to $2,000 a year by allowing an employee to work remotely
However, cybersecurity concerns raised by remote access aren't myths. Let's review the key dangers stemming from remote employees and possible ways to mitigate them.

**CONCERNS ABOUT REMOTE WORK**

Remote connections are a known cybersecurity threat. Among IT leaders, 73% treat teleworkers as more dangerous than on-site employees according to an OpenVPN survey.

The key reason for this attitude is the fact that remote employees access sensitive data from outside the traditional cybersecurity perimeter. Lack of knowledge and protective measures make telecommuters (and therefore the data they access) more vulnerable to hacking attacks and data breaches.

Here are the most common threats posed by remote employees:

1. **Using public Wi-Fi networks.** No authorization is required to connect to public Wi-Fi, and hackers can hijack data a user sends via these unsecured connections. Such data may include anything from work-related emails to sensitive corporate information and user credentials.

2. **Using personal devices for work.** An employee's office workstation is usually secured with dedicated antivirus and firewall software, encryption algorithms, etc. For a remote employee, it's best to issue a corporate laptop or set up special software on a personal device. However, employees are often tempted to use a corporate laptop for personal purposes, share it with family members, or use a different device to do their work.

3. **Lack of cybersecurity awareness.** In addition to cybersecurity software, remote employees need knowledge of how to use this software and why it's important. Without such knowledge, they're likely to ignore security measures to make their work faster and more comfortable. For example, organizations commonly use VPNs with a limited number of connections. This slows down the work, and so employees turn off the VPN whenever possible.
4. **Susceptibility to social engineering attacks.** Phishing, smishing, pretexting, social network hacking, and other attacks are a threat to any employee. During emergencies, when lots of companies allow their employees to work from home, there’s usually a rise in social engineering attacks targeted at telecommuters. *Scams created during the coronavirus* outbreak are a great example. Due to a lack of cybersecurity knowledge and tools, hacker attacks have a higher chance of success.

5. **Lack of authorization and access control tools.** Stealing credentials from a remote employee is easier than from an on-site employee because of the reasons listed above. Despite that, organizations fail to enforce additional authentication measures for remote employees.

6. **Using outdated software.** Nobody likes to update their software frequently. It causes disruptions, takes time to install updates, and requires you to get used to a new version. However, one of the key reasons for updates is to fix security issues. IT administrators can enforce mandatory updates on corporate endpoints. But remote employees are usually more hesitant about updating their software. By abusing known vulnerabilities of old software, hackers can perform successful attacks.

7. **Malicious actions with data.** While remote employees have the same level of access as their colleagues in the office, they’re usually less controlled by the IT security team. Therefore, it’s easier for teleworkers to conduct unnoticed data theft, abuse, misuse, and other types of *insider attacks*.

8. **Resting instead of working.** While most employees are productive both at home and in the office, some may find it difficult to focus without their manager nearby. Such employees can easily be distracted by cleaning, browsing the news, playing games, etc. Without dedicated remote employee monitoring software, it’s hard to evaluate if a person really doesn't work.
Key concerns about remote employees

1. Using public Wi-Fi networks
2. Using personal devices for work
3. Lack of cybersecurity awareness
4. Susceptibility to social engineering attacks
5. Lack of authorization and access control tools
6. Using outdated software
7. Malicious actions with data
8. Resting instead of working

It’s possible to mitigate these concerns by implementing cybersecurity and remote worker monitoring best practices. Let’s review key time-proven methods to secure remote connections and employees.

BEST PRACTICES FOR MONITORING REMOTE EMPLOYEES

We’ve prepared a list of best practices to help you monitor and secure remote activities. Some are purely organizational, while some require dedicated remote employee monitoring software such as Ekran System.

Best practices for monitoring remote employees

1. Create a written remote access policy
2. Inform employees of social engineering attacks
3. Secure remote connections with a VPN
4. Enforce multi-factor authentication
5. Restrict shared accounts or use secondary authentication
6. Control employee productivity
7. Get alerts on suspicious events
8. Monitor and record user activity
9. Manage credentials and secrets
1. Create a written remote access policy. This policy should include:

- a list of software and access control measures
- instructions on how to connect to your network remotely
- measures for protecting credentials
- conditions for providing remote access to employees (if your company doesn’t usually allow remote work)

Make sure your employees can read this policy at any time and that you answer any questions they may have about it.

2. Inform employees of social engineering attacks. Such attacks are usually successful because of an employee’s inattention, haste, or because hackers have new tricks up their sleeves. The best way to mitigate these attacks is to educate workers on recent social engineering attempts and remind them of the threat. For example, you can share this quiz on phishing from Google or tips from the US Department of Homeland Security.

3. Secure remote connections with a VPN. This technology creates a secured point-to-point connection between an employee’s computer and the corporate network using an encryption algorithm and authentication. Therefore, a VPN is an effective tool to protect connections via untrusted networks such as public Wi-Fi.

4. Enforce multi-factor authentication. Checking several factors allows you to positively authenticate someone trying to connect to your network. Ekran System checks credentials (a knowledge factor) and sends a one-time SMS password to a user’s phone (a possession factor).

5. Restrict shared accounts or use secondary authentication. Shared profiles such as for remote administrators simplify employees’ lives but make it extremely hard to link security violations to specific users. Some IT specialists prefer to ban such accounts. If you can’t do that, implement secondary authentication to identify the user behind a faceless profile.
6. **Monitor and record user activity.** Continuous monitoring of remote computers provides you with full visibility into employees' actions taken with sensitive data and their overall performance. Activity monitoring software such as Ekran System records:

- on-screen activity
- audio input and output
- keystrokes
- opened folders and files
- executed commands
- and more

With Ekran, monitoring and recording continues even without an internet connection. With such records, you'll be able to clearly establish the context of any action and prove your point during an investigation.

7. **Control employee productivity.** A simple time tracker often isn't enough to estimate a worker's efficiency. With data from user activity monitoring, you can evaluate an employee's effectiveness and dedication during working hours. Analysis of screen records, opened files, folders, applications, and websites helps you detect workers that prefer to browse news and social networks instead of working on the document they're tasked with. It's also a good practice to track productivity by conducting periodic meetings and asking remote employees to write daily or weekly status reports.

8. **Get alerts on suspicious events.** A timely alert on a possible security violation with a link to the session in question helps a security officer stop suspicious activity. It's always better to stop a threat than to deal with its consequences. Apart from providing an alert, Ekran System can:

- notify a user of a rule violation
- block an activity
- block a user
9. **Manage credentials and secrets.** As we mentioned, the credentials of remote employees are especially easy to steal. You can protect them by deploying a password management solution. A password manager allows you to create, store, transmit, and rotate logins and passwords in a secure manner with no involvement from users. Besides securing credentials, Ekran System also manages Windows Active Directory secrets, SSH/Telnet keys for Unix environments, and more.

Let's see how you can mitigate major remote employee-related threats with the practices and tools we've discussed.

### How to manage threats posed by remote employees?

<table>
<thead>
<tr>
<th>Threat</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using public W-Fi networks</td>
<td>Secure remote connections with a VPN</td>
</tr>
<tr>
<td>Using personal devices for work</td>
<td>Create a written remote access policy</td>
</tr>
<tr>
<td></td>
<td>Monitor and record user activity</td>
</tr>
<tr>
<td>Lack of cybersecurity awareness</td>
<td>Create a written remote access policy</td>
</tr>
<tr>
<td></td>
<td>Monitor and record user activity</td>
</tr>
<tr>
<td>Susceptibility to social engineering attacks</td>
<td>Inform employees of social engineering attacks</td>
</tr>
<tr>
<td></td>
<td>Monitor and record user activity</td>
</tr>
<tr>
<td>Lack of authorization and access control tools</td>
<td>Enforce multi-factor authentication</td>
</tr>
<tr>
<td></td>
<td>Restrict shared accounts or use secondary authentication</td>
</tr>
<tr>
<td>Using outdated software</td>
<td>Create a written remote access policy</td>
</tr>
<tr>
<td></td>
<td>Manage credentials and secrets</td>
</tr>
<tr>
<td>Malicious actions with data</td>
<td>Enforce multi-factor authentication</td>
</tr>
<tr>
<td></td>
<td>Restrict shared accounts or use secondary authentication</td>
</tr>
<tr>
<td></td>
<td>Monitor and record user activity</td>
</tr>
<tr>
<td>Resting instead of working</td>
<td>Monitor and record user activity</td>
</tr>
<tr>
<td></td>
<td>Control employee productivity</td>
</tr>
</tbody>
</table>
CONCLUSION

Teleworkers help companies save money on office rent, are as dedicated as in-office employees, and stay in touch with their managers. Sometimes they're even more productive than their on-site colleagues. On the other hand, cybersecurity threats of remote access call for considerable protection measures. Even if your company usually employs on-site employees, there are situations when you need to provide remote access and monitor your remote workers — and it's best to prepare ahead.

In this article, we reviewed the major cybersecurity risks of allowing your employees to work from home. Some of them can be eliminated by organizational measures such as creating policies and educating your workers. But in order to ensure maximum security and transparency, it's best to deploy dedicated remote employee monitoring software such as Ekran System.

With Ekran, you'll be able to verify user identities, manage user access (including access of privileged users), and monitor the activity of any user inside and outside your protected perimeter. Ekran System is a universal lightweight solution that can easily be deployed in 20 minutes on 10 or 10,000 endpoints.