keepod

REMOTE WORK IS NOT A TREND.
IT`S HERE TO STAY.

SRW-20

digital
whitepaper

デジタルホワイトペーパー

secure remote working

Remote work is not a trend — it's here to stay. Research estimates that the number of worldwide remote workers has increased by 159% in the last 15 years. This is of no surprise given its significant benefits to both employees and companies. Workers enjoy increased flexibility, autonomy and potential improvements in their work-life balance, leading to overall better performance. Companies can profit from spikes in productivity, increased employee satisfaction and talent attraction as well as a reduction in office costs. In light of these incentives, more and more companies devote IT resources to the implementation of remote working solutions that deliver tangible results and ensure business continuity even throughout times of systemic shocks such as the currently faced pandemic. In fact, nearly two-thirds of global enterprises already embrace certain kinds of remote working policies. Nevertheless, in order to fully exploit the potential benefits of remote working, certain challenges, particularly in terms of business environment disturbances, data security and costs of support, need to be addressed.

Problems

Significant problems may greatly vary in size and scope and should not be underestimated in order for organizations to stay ahead in the game.

In this document we will discuss **business environment disturbances**, **data security** and **cost of support**.

Business environment disturbances

Throughout the transition to remote work, companies must ensure sound management of potential disruptions to the operational and working environment as well as employees' adaptation to those.

Even if companies successfully provide off-site employees access to appropriate tools and resources, related technical issues could arise, necessitating troubleshooting and potentially grinding work to halt. System incompatibilities might require costly and time-consuming adjustments in IT infrastructure in order to grant remote workers continuous access to the company platforms. Likewise, connectivity failures, obsolete personal devices software/ hardware and insufficient IT literacy of workers could additionally disrupt workflow efficiency.

Data security

Because of the continuing and persisting threat from malicious parties, securing a corporate network is complex. It is all the more laborious when employees work remotely using personal devices and expect quick and easy access to their work environment. Thus, organizations must ensure the security of both corporate data and personal information stored on their corporate networks in order to ensure business continuity.

Remote work provides a risky environment and a potential threat to the organization. Five main threats are identified, namely: disclosure, modification, removal, human error as well as physical and cyber-attacks.

- Confidentiality refers to the inappropriate or unauthorized access to information by non-employees, such as any resident or guest at home, that could disclose information to external parties. This can be due to insufficient security features (e.g. insecurely stored passwords), lack of authentication and authorization, negligence, or human mistake.

- Because employees might access information on unprotected personal devices or communicate information through unsecured channels, data modification can occur, leading to the loss of system and information integrity.

- Removal refers to the frequent loss of sensitive assets (e.g. removable devices drives, laptops, etc.) or data (any critical information regarding customers, employees, etc.) by either theft or misplacement.

- Remote work extends an organization's exposure to human error. As communication might be less effective between employees, the probability of mistakes increases leading to potential cybersecurity gaps with the shift to a remote workplace, IT teams open internal systems to external work by introducing new devices, networks or VPN configurations, resulting in a widened attackable surface.

- Because of increased online communication, employees, especially the ones possessing sensitive information, will be more vulnerable to targeted and non-targeted cyber-attacks (e.g. phishing, malware, etc). This could allow malicious external parties to obtain information without bypassing heavy layers of security of an enterprise.

Therefore, organizations implementing remote working practices must focus on security in order to prevent the above-mentioned threats, protect their data, enable quicker retrieval of lost information and minimize the often-unquantifiable damage that could be caused.

Cost of support

The transition to remote work involves bearing unpredictable costs starting right from the on-boarding process when trying to deliver a secure and reliable work environment.

Firstly, even though gross pay expectations of a remotely working employee might be as less as 60-70% relative to an on-site employee, the transition process from on-site to off-site working implies high costs in terms of training and development as well as cumbersome onboarding processes.

Secondly, the cost of buying uniform take-home devices (laptops or tablets) for every employee is largely uneconomical, eventually defeating the purpose of the transition. Therefore, organizations often look into BYOD (Bring Your Own Device) alternatives which introduce a complicated heterogenic end-point scenario with multiple hardware, operating systems, applications, and configurations to support. The likelihood of security cracks in BYODs, and thus the cost of preventing and countering them, increases with the number of different devices being used.

Solution: Keepod SRW-20

The question now is: how can we overcome the highlighted obstacles and create a remote working environment that is simultaneously convenient, secure and economical — no matter where and when workers connect day-to-day?

Keepod provides the solution. Delivering a secure, lightweight workstation that can start on any PC from a dedicated removable drive, fully compatible with an array of enterprise platforms, cloud-based applications and features necessary to work remotely.

Keepod SRW-20 delivers a secure office-experience for any remotely working employee.

Business continuity

In today's fast-moving world, Keepod strives to help organizations to improve their business agility. With Keepod SRW devices, employees' unsecured computers can be easily turned into trusted workstations, ensuring an uninterrupted and seamless workflow anywhere and at all times.

Bypassing the host operating systems, Keepod SRW allows users to gain homogeneous access to the enterprises' platform and the appropriate tools and resources. Its sleek, fast and modern desktop environment provides a user-friendly interface that minimizes distractions and avoids the need for additional complex training. Moreover, its lightweight operating system allows for top tier performance in the face of all the organizations' resources even on older and outdated PCs. As a stand-alone environment that boots itself directly from the USB device, it does not require any installation on the concerned host device.

Keepod SRW brings five significant features to provide the desired level of business continuity.

Powerful VPN client supporting all major VPN solutions and authentication methods allowing the user to easily gain access to their remote environment.

A pre-installed set of client applications including the most utilized VDI and remote desktop platforms from Microsoft, VMware, Citrix, Amazon, and many others; allowing users to remotely access and operate desktop running in the organizations' backend via BYODs.

Web access to collaboration, project management platforms, such as Microsoft Teams, Slack, G Suite Asana, Trello, Skype, Zoom, Monday, Zoho, etc., guarantees coordination among remote workers, ensuring effective long-distance work.

Google Chrome and Mozilla Firefox on-board too, ensure compatibility with enterprise web platforms and web standards. With privacy and continuity in mind, browsers are preloaded with ads/trackers blocker and password manager extensions.

Keepod SRW provides users with a set of utilities to support a wide range of hardware configurations and extensions for connectivity audio, video, print, touch screens, and more.

Conclusively, Keepod SRW provides an all-running system with no impact on the user host system and smooth integration with the organizational IT structure, ensuring an easy use and an obstacle-free workflow.

Data protection

Keepod SRW was designed to stamp out the five main aforementioned threats induced by remote work.

Keepod SRW's secured operating system works only in LiveOS mode. Once the device is plugged in, users can work normally and access their VPN, remote desktops, applications, corporate files, etc., but once the OS is shut down, all local data is discarded. Indeed, Keepod SRW's uniqueness comes from its zero-knowledge and zero-trust approach. While information is being saved on the corporate servers, no data footprint is left on the host device or on the Keepod device. Therefore, at the beginning of each session, users have to re-enter their login credentials and settings, such as personal or WIFI passwords, creating a little discomfort that should be considered as an essential tradeoff for a safe working environment and a transparent security.

As the entire environment runs from the device, no interaction with the host's OS occurs, leaving zero impact on the users' device. This keeps corporate information safe from corruption and provides a non-invasive environment that reduces the risk of liabilities potentially arising from leaks of confidential or sensitive information.

No organization can afford data leaking. By virtue of Keepod SRW's above-mentioned characteristics, even in case of device loss or theft, corporate data will remain protected.

Cost efficiency

By offering a standardized, easy-to-use and one-time cost solution, Keepod SRW eliminates the need to standardize existing BYODs or to equip every employee with uniform take-home devices. Additionally, extensive security & privacy policies (e.g. privacy-enhancing devices such as thin-client terminals), large-scale onboarding and training programs, as well as extensive insurance costs against loss or damage of assets can be avoided. The physical durability of the device combined with its affordable cost per unit results in significantly lower Total Costs of Ownership (TCO) for companies.

Conclusion

With the evolution of information technologies and the uncertainty of business environments worldwide, workforce flexibility and agility are becoming increasingly valuable sources of competitive advantage for companies. Organizations cannot afford to be passive but must act accordingly. The sooner the better. Standing still is not an option since, as mentioned before, remote work is not a trend — it's here to stay.

Keepod Ltd
147 Station Road
E4 6AG London, UK

keepod.com
info@keepod.com