SECURE REMOTE WORKER

Data Sheet

Enabling Bring Your Own Device (BYOD) with Secure Remote Worker

What is Bring Your Own Device (BYOD)?

Bring Your Own Device (BYOD), sometimes also referred to as Bring Your Own Personal Computer (BYOPC), or Bring Your Own Technology (BYOT), refers to a working policy adopted by many organizations that allows its employees to bring their own personal devices, such as laptops, tablets, and smart phones, into the corporate working environment.

These personal devices are then used on a daily basis by the end users in performing their normal job roles and are used to connect to, and access privileged information, apps, and systems.

The BYOD advantage

Deploying a BYOD initiative has numerous advantages, especially when an organization has a remote desktop or remote application solution already in place. For one, an organization can reduce the capital expenditure costs of having to purchase devices for each of its end users, and instead allow them to use or bring their own. This also gives the end users the freedom to choose the device that best suits their individual requirements.

But herein lies the problem, and the potential disadvantages to deploying a BYOD strategy. How does the IT department ensure that the device is secure and isn't going to compromise data security? From the user's perspective, they won't want the IT teams to take control of their personal device, and manage their personal content by installing intrusive agents, or other MDM type solutions.

Secure Remote Worker solves this problem by delivering a secure, policy driven, secure workspace environment onto personal Windows-based devices.

Seamlessly switch between personal and secure corporate environments

Secure Remote Worker allows end users to use their personally owned device and enables them to switch between their personal environment and their corporate environment securely. It does this by temporarily locking down the underlying device operating system and replacing it with a secure workspace interface that presents them with the ability to connect to remote resources, and all without the need to reboot, dual-boot, or boot from an external USB device.

SECURE REMOTE WORKER

Data Sheet

How Secure Remote Worker enables BYOD

The challenge of delivering a secure environment to personal devices

Security is one of the biggest problems faced by organizations today when looking at deploying remotely accessible systems such as virtual desktops and published desktops and applications. Although the solutions themselves are secured behind the firewall and run on server infrastructure within the confines of the datacenter, the edge of the network stops with the end users.

However, the cost savings of BYOD cannot be ignored, and neither can the fact that end users are far more IT-savvy these days and want to use different devices, or their own device. So that leaves the question of how do IT teams ensure that end users are not going to remove sensitive data or introduce malicious files into the corporate environment if they use their own devices?

Is MDM the answer?

Mobile Device Management, or MDM, is designed to allow IT teams to manage end point devices, ensuring that end users only access applications and data that they are authorized to use. However, these solutions come at a price, and that's not just the cost of purchasing a license. It means that the end user's device is now managed by the corporate IT team, which, given that it's a personally owned device, does not sit well with end users. Nobody wants their organization to manage and have control over their personal data and device and tell them what they can and cannot run on it.

So the question is how can IT teams deliver a flexible solution to deliver a secure managed environment rather then a managed device?

Secure Remote Worker delivers secure thin client environments

The simple answer is to solve this with Secure Remote Worker. Secure Remote Worker delivers a thin client experience to the end user's device, which providing all the benefits of thin client computing by locking down the device. As Secure Remote Worker is a software-defined thin client solution, end users can simply launch the Secure Remote Worker application on their personally owned Windows PC's and laptops. They then have access to a secure workspace interface, managed centrally by IT admins, from where they can access their corporate and work environments from.

Security first: Securing end point devices

To ensure that the Secure Remote Worker secure workspace environment remains secure and compliant, Secure Remote Worker employs a number of advanced security management features such as Application Execution Prevention (AEP), and USB blocking. These features ensure that end users only launch the apps that they are able to (based on central policy), and blocks them from accessing USB media devices.

SECURE REMOTE WORKER

What is Secure Remote Worker?

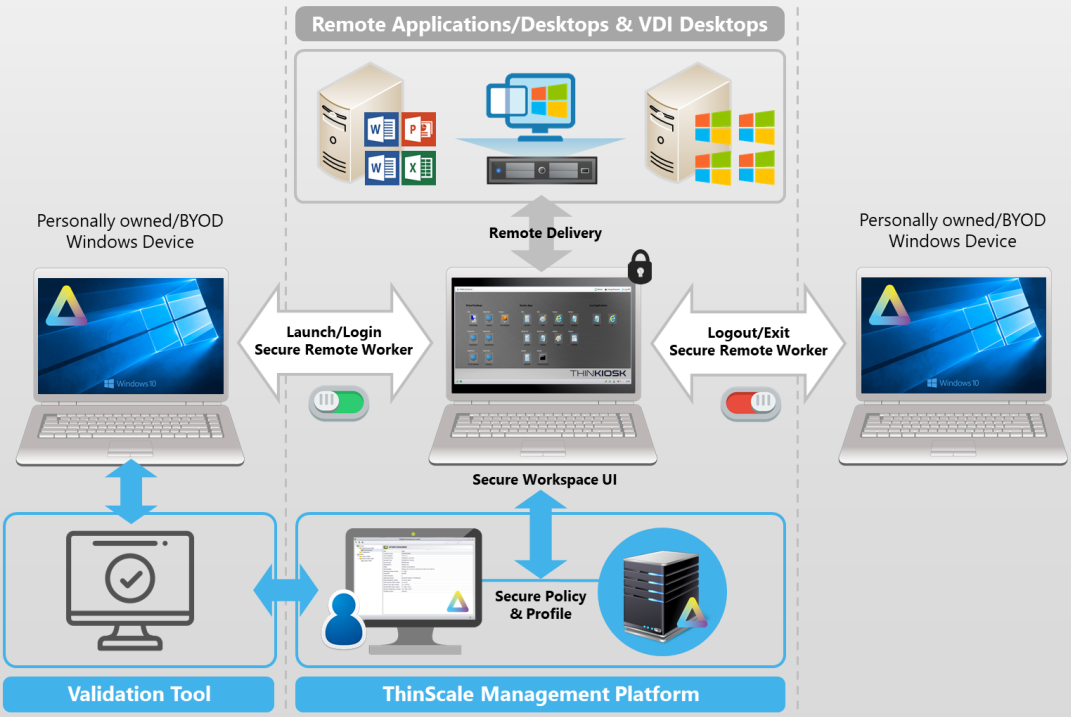
Secure Remote Worker is a software-defined solution that an end user launches as an app on their own personal Windows PC or laptop. It creates a secure workspace environment, managed centrally by IT, enabling end users to have access to corporate resources and services remotely.

How does Secure Remote Worker work?

Secure Remote Worker allows an end user to use their personally owned Windows device. By default, an end user will continue working as normal and will have full access to their local Windows PC or laptop, so when they logon to their device, they still have a start menu and full access to their resources, apps, and settings.

Then, when Secure Remote Worker is launched on their Windows PC or laptop, and the end user enables the Secure Remote Worker feature, their PC or laptop is placed into "worker" mode. Lock down polices are then applied, Windows Explorer is removed, and the Secure Remote Workspace user interface is launched.

Once the end user has finished working with their remote desktops and applications, they simply logout of the remote environment, and exit Secure Remote Worker. All the device restrictions that were applied whilst Secure Remote Worker was running are now lifted and the end user has full control of their local PC again.



SECURE REMOTE WORKER

Secure Remote Worker features for BYOD

Full device lock-down

Launching Secure Remote Worker on a user's personal Windows device denies them access to the underlying Windows operating system, effectively rendering it disabled while they are using the secure workspace environment.

Instead of the desktop interface of the Windows operating system, an end user will access the Secure Remote Worker Workspace, a simple, easy to navigate user interface from where they can connect to their remote environments securely. They also have the ability to access local applications if they have the relevant permission from IT to do so. Their device is only locked down for the duration of the secure session, and full control is returned to the user once they log out.

Secure Remote Worker Validation Tool

Secure Remote Worker includes a unique solution that enables IT admins to check the end user's device before they connect to ensure that it meets minimum requirements. The Endpoint Validation Tool inspects the end point to determine the patch levels, installed software, and whether antivirus is present to name but a few checks. Proactively checking devices before onboarding means that any issues can be rectified in advance, drastically reducing onboarding times and reducing any initial support calls.

Application Execution Prevention (AEP)

The Secure Remote Worker AEP feature adds an additional layer of security by preventing the execution of unauthorized applications.

Employing a rules-based system, IT admins can now configure exactly which apps end users are allowed launch on their endpoint device while Secure Remote Worker is running and active. These rules allow IT admins to create white/black lists which contain a comprehensive list of rule types that delivers a granular level of control over exactly which applications can and can't run.

IT admins can create generic rule sets that allow all Windows OS binaries to run, or they can create a more targeted rule set that allows only those applications signed by a specific digital certificate to launch and run.

SECURE REMOTE WORKER

Secure Remote Worker features for BYOD

Service Execution Prevention (SEP)

The Service Execution Prevention feature of Secure Remote Worker allows you to control which Windows services are allowed to run when a Secure Remote Worker session is active, and running in 'worker mode'. If a service is running and it does not match the defined Service Execution Prevention policies, then the service will either be automatically stopped or the end user will need to manually stop the service before the they can launch Secure Remote Worker on their device.

Windows Patch Management

Secure Remote Worker enables IT departments to easily control the Windows Update feature to ensure that end users are running the correct patches an updates before connecting to the corporate environment.

For IT this means they can configure how often the client devices check for any updates, and then decide when, and if to apply them. End users can also be prompted to install any of the available updates, or the updates can simply be pre-configured by the IT department to install silently, without user intervention or disruption ensures the users devices are always up to date, secure, & compliant.

USB device blocking

USB devices are often seen as one of the main causes security breaches and data leakage within an organization. Users plug in their own USB memory sticks and other write-enabled media devices and copy potentially sensitive data onto them and remove them from the corporate environment.

Secure Remote Worker is able to prevent these devices from being usable with its USB device blocking feature. Enabling this feature means that end users are prevented from being able to access USB-based storage devices when accessing corporate systems and data from the secure workspace.

Windows Firewall Control

Secure Remote Worker allows IT admins to be able to fully configure the Windows Firewall feature automatically. They can remove any existing firewall rules, or configure new firewall rules, and manage this centrally all from the ThinScale Management Platform and the Profile Editor.

SECURE REMOTE WORKER

Data Sheet

Secure Remote Worker features for BYOD

Right place, right time delivery

As well as working from different office locations, customer site, or even the local coffee shop, end users can all really be classed as mobile workers.

Secure Remote Worker is fully location awareness, meaning it's contextually aware of where end users are connecting from, enabling true flexible working, whether from the confines of head office, or other office location, delivering the right level of access at the right time and right location. All delivered securely.

Enhanced end user experience

The end user experience is key to the productivity and speed of accessing patient information and data. Secure Remote worker delivers a familiar Windows look and feel coupled with an intuitive secure workspace user interface that enables fast and easy access to remote environments. It also allows end users to have access to locally installed applications (based on admin set policy) should they need to work offline.

Seamless look and feel with Magic Filter

As part of the end user experience, a unique feature of Secure Remote Worker is Magic Filter. Magic Filter is a dynamic key press pass-through feature that traps the local Ctrl + Alt + Del keystrokes and passes them directly through to the remote environment, just as if the user was working locally on their device.

Magic Filter delivers an enhanced user experience as the end user now has a native Windows feel when using their ThinKiosk thin client.

Simplified management, support, and onboarding

As Secure Remote Worker is a software only solution, end users simply download the application, launch it, switch to 'worker mode' and are connected securely to the corporate environment in minutes!

IT admins have the ability to manage the secure workspace environment remotely, allowing them to update security policies on the fly, with no need for a deskside visit or end users to travel in or send devices back.

SECURE REMOTE WORKER

Data Sheet

Secure Remote Worker features for BYOD

Secure Browsing

Included as part of the Secure Remote Worker Client software, is an integrated web browser, complete with a fully customizable user interface, that allows users to securely browse Internet sites based on policy set by the IT department.

The Secure Remote Worker integrated browser is fully compatible with websites as it utilizes the browser rendering engine used in Microsoft Internet Explorer.

Windows Security Center Detection

Secure Remote Worker proactively checks and monitors the security components of the device OS. Components such as Firewall Protection, Anti Virus, and Anti Spyware protection, can all be monitored.

Should one of these components not be compliant or configured correctly, then Secure Remote Worker can take the appropriate action for remediation, ensuring that issues are not only quickly identified, but also quickly resolved.

Reducing the cost of remote working

Deploying remote or published desktops and apps is seen as a way to reduce costs, however the initial upfront costs incurred in deploying the new infrastructure that is required to run remote desktop and applications can be expensive. As part of this you also need to consider how end users are going to securely connect to the environment.

ThinKiosk and the Secure Remote Worker feature offers a single solution for all end users to connect to their remote environments. Rather than purchasing expensive and obtrusive MDM solutions that end users will push back on, or different solutions for internal and external users, instead deliver a single secure workspace with the same look and feel for every user.

Managed access to local applications

With Secure Remote Worker, IT can manage which apps an end user can have access to while they are in “worker” mode, ensuring security and protecting corporate data. This means that they could also have access to any local applications that are installed on their device if IT grant them permission.

SECURE REMOTE WORKER

Data Sheet

Secure Remote Worker feature summary for BYOD

Secure Remote Worker is designed to enable end users to use personally owned Windows PC's, or even their own home Windows PC's and laptops. This allows end users the freedom and flexibility to work from outside the office environment, securely. The use case for an organization is the ability to embrace BYOD and also deliver business continuity for those occasions where the end user workforce cannot make it into the office.

Deliver PCI & HIPPA Compliance

Secure Remote Worker enables organizations to meet the stringent compliance requirements demanded by QSA's for PCI and HIPPA compliance.

Enables BYOD for Windows

Secure Remote Worker allows end users to use their personally owned Windows device. This gives IT teams peace of mind knowing that the device is secure while SRW is active.

Full device lock-down

Secure the end users device by locking them down with a centralized policy preventing them from accessing the underlying OS.

Secure workspace environment

Secure Remote Worker gives end users a temporary secure workspace from where they can easily access apps and services when running in worker mode.

Familiar end user experience

Secure Remote Worker delivers a familiar and intuitive user interface, with a Windows look & feel, along with enhanced productivity features.

Centralized management

Manage your entire remote device estate using a single management platform with a single administration console.

Speed up end user onboarding

Setup and onboarding takes just minutes to complete and is a simple case of installing the SRW software on the end users device, and then switching SRW to worker mode.

Reduce cost, increase productivity

Secure Remote Worker enables organizations to reduce the cost of hardware acquisition and management. It increases end user productivity with faster onboarding and easier support.

For more details on the features and benefits of how Secure Remote Worker solves your BYOD and mobile computing security challenges, please visit the ThinScale website, or contact the ThinScale team to discuss your specific use case.

THINSCALE

Software solutions that enable IT to deliver the modern digital workplace without compromising on end user experience, security, or performance.

Contact Us

US: +1 516 321 1774

IE: +353 1906 9250

NL: +31 203 690 475

UK: +44 203 854 0944

Request a Demo

sales@thinscale.com

thinscale.com

ThinScale,
The Media Cube,
Kill Avenue,
Dún Laoghaire,
Co. Dublin, A96 X6X3
Ireland