THINSCALE

SECURE REMOTE WORKER

Delivering Secure Remote Working in Healthcare Environments

WHITE PAPER

SECURE REMOTE WORKER

Data Sheet

How Secure Remote Worker enables secure client computing for community-based & remote healthcare professionals

Delivering client computing beyond the boundaries of bricks & mortar

Today's healthcare professionals are not always tied to a static working environment such as a particular hospital or clinic. With the advent of virtual desktop solutions and hosted apps solutions, users now have the freedom and flexibility to deliver healthcare services out in the community. The majority of their time may still be based in one location but having the ability to work at home, work from patients homes and remote surgeries all adds to increased mobility, productivity and patient care. For example, the ability to complete patient notes in real time using what ever device is available at the time, even the clinicians own device at home or on the road means they don't have to travel back in to the hospital location to complete admin tasks.

Ensuring security & compliance for remote healthcare professionals

But herein lies the problem. Typically IT will deploy some form of thin client to access these systems, a secure device perceived as a "cut down PC" that only allows end users to connect to remote environments, and only from the confines of the hospital network. How does the IT department deliver secure mobile working while at the same time maintaining levels of security and data protection for both the end user and the patients, when an end user is working both remotely and using their personally owned device?

When working from the hospital environment, security, PCI and HIPPA compliance is easily achievable. But what about Bring Your Own Device (BYOD), Bring Your Own Personal Computer (BYOPC), or just an end user working on their home PC? These personally owned devices will be used to connect to and access sensitive patient records, apps, and systems. How can IT manage this way of working and at the same time ensure that these devices are secure and offer no risk to the patient data? The answer is Secure Remote Worker.

Secure workspace environment

Deploying Secure Remote Worker enables IT teams to deliver secure, policy driven, segregated workspace environments to Windows-based devices whether personally owned or owned by the healthcare organization, and all regardless of where the end user is working from.

Secure Remote Worker is a software solution that allows Windows devices to securely access remote environments, by temporarily locking down the underlying device OS and in its place delivering a secure workspace environment onto the device all the time Secure Remote worker is running. This allows end users to switch between their personal environment and the secure workspace environment, without the need to reboot, dual-boot, or boot from an external USB device.

SECURE REMOTE WORKER

Data Sheet

Secure Remote Worker Healthcare Features

Full lock-down of personally owned (BYOD) devices

Launching Secure Remote Workers 'worker mode' on a healthcare professionals Windows device denies them access to the underlying Windows OS, rendering it disabled while they are using the secure workspace environment.

Instead of the desktop interface of the Windows OS, they will access a secure workspace environment, 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 Remote Worker session, and full control is returned once they switch worker mode off.

USB device blocking

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

Application Execution Prevention (AEP)

The Secure Remote Worker Application Execution Prevention feature adds an additional layer of security by preventing the execution of unauthorized apps.

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

Data Sheet

Secure Remote Worker Healthcare Features

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. If a service is running and it does not match the defined SEP 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 in 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. This ensures that the end users devices are always up to date, secure, and compliant.

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 Validation Tool

A unique feature to Secure Remote Worker is the ability to inspect the end user's endpoint device prior to on-boarding them. IT admins can run a detailed and comprehensive analysis and report on the device detailing what software it's running, the current patch levels, and whether it has up to date virus and malware protection. This allows IT to plan any remediation required before onboarding the user and granting them access to clinical resources. Being proactive also cuts down support calls and troubleshooting during onboarding.

SECURE REMOTE WORKER

Data Sheet

Secure Remote Worker Healthcare Features

Location awareness

As well as working out in the community, travelling to different hospital sites, patients homes, and even if a clinician is based in a hospital, they can all really be classed as mobile workers.

Secure Remote Worker is location aware, meaning it's contextually aware of where healthcare professionals are connecting from, enabling true mobile working, whether in the confines of a hospital or out in the community, delivering the right level of access at the right time, in the right location, 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.

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 keystrokes, such as Ctrl + Alt + Del 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 Secure workspace environment.

Simplified management, support, and onboarding

As Secure Remote Worker is a software only solution, remote healthcare professionals simply download the app, launch it, switch to 'worker mode' and are connected securely to the clinical 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 Healthcare Features

Secure Browsing

Included as part of the ThinKiosk 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 ThinKiosk 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.

Secure Remote Worker Use Cases for Healthcare

Scenario #1

Bring Your Own Windows PC

Secure Remote Worker enables healthcare professionals to use their own Windows PC's and laptops, by allowing them to switch between their personal and clinical environments, quickly and simply, without rebooting, or dual booting their device.

It does this by delivering a policy driven, secure workspace environment and user interface on the user owned Windows device, allowing them to switch between environments and securely access the clinical environments and patient data.

Scenario #2

Remote & Home Working

Enhance patient care and productivity by enabling field based healthcare professionals to connect to the clinical resources remotely, to access their remote applications and virtual desktops, while on the move, working from home, or even using their own devices.

End users can work from home or out in the field by simply connecting to Wi-Fi, launching their Secure Remote Worker policy driven secure workspace environment, and then having access to patient records and clinical apps and services they require.

SECURE REMOTE WORKER

What is Secure Remote Worker?

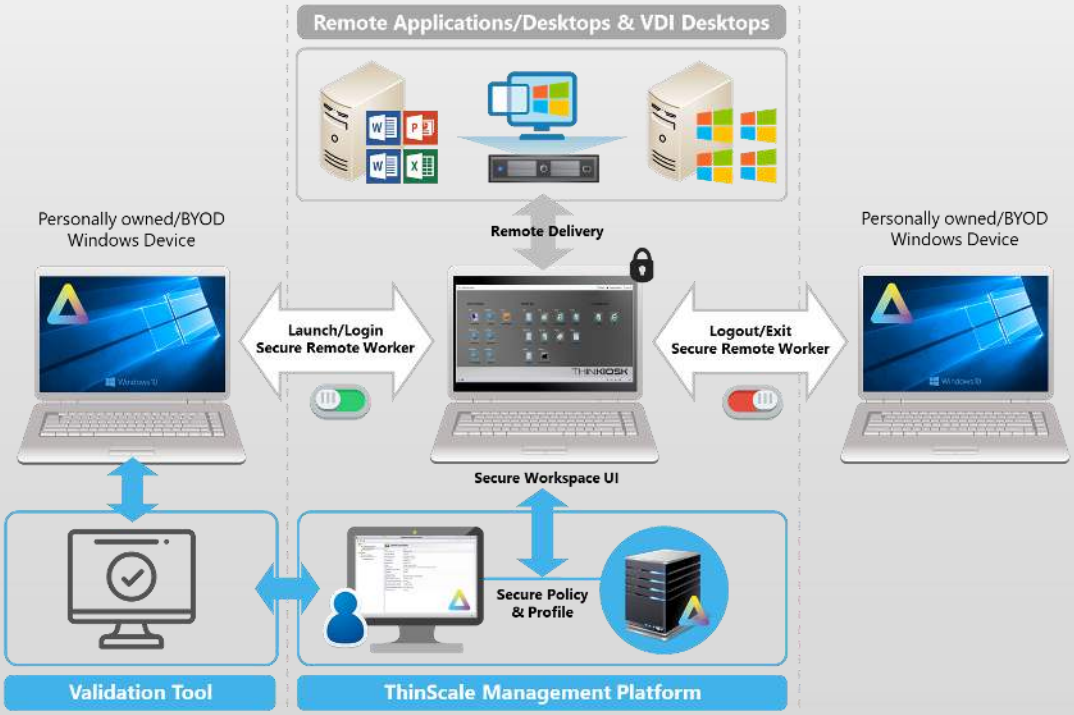
Secure Remote Worker is a software-defined solution that an end user launches as an app on their own personal Windows PC or laptop that creates a secure workspace environment, managed centrally by IT, enabling them to access remote corporate resources and services.

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 whereby lock down polices are 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

Data Sheet

Secure Remote Worker for Healthcare Summary

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 hospital environment, securely. The use case for a clinical organization is the ability to embrace BYOD and also deliver business continuity for those occasions where the end user workforce cannot make it in to work. Taking this approach enhances the ability for healthcare organizations to deliver patient care out in the field.

Deliver PCI & HIPPA Compliance

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

Full device lock-down

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

Familiar end user experience

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

Speed up end user onboarding

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

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 Secure Remote Worker is in 'worker mode'.

Secure workspace environment

Secure Remote Worker gives end users a temporary secure workspace from where they can access apps and services from all the time Secure Remote Worker is running.

Centralized management

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

Reduce cost, increase productivity

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

For more details on the features and benefits of delivering secure remote working and 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

NL: +31 203 690 475

IE: +353 1906 9250

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