SECURE REMOTE WORKER

Data Sheet

How to Deliver Secure Client Computing for BYOD & Work at Home

Delivering client computing beyond the office boundaries

Today's end users are no longer tied to a static working environment such as a desk in an office. With the advent of virtual desktop solutions and hosted application solutions, users now have the freedom and flexibility to choose where they work from. It may well still be mostly office based for the majority of the time, but having the ability to work at home, work from customer sites, work from other office locations, or even work from the local coffee shop, all adds to increased end user freedom and productivity.

Ensuring security & compliance for remote workers & BYOD

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. How does the IT department deliver this method of working while at the same time maintaining corporate levels of security and data protection for both the end user and the organization, when an end user is working both remotely and using their personally owned device? In short, they need to deliver all the security benefits of thin client computing without tying the end users down.

When working from the office environment, security Payment Card Industry Data Security Standard (PCI), and Health Insurance Portability and Accountability Act (HIPAA) 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 privileged company information, apps, and systems. How can IT manage this way of working and ensure that these devices are secure and offer no risk to the corporate environment? The answer is Secure Remote Worker.

Secure Remote Worker software-defined thin clients

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

At it's core, Secure Remote Worker delivers a software-defined thin client experience, allowing existing Windows devices to securely access remote environments, by locking down the underlying device OS. This allows end users to switch between their personal environment and their corporate workspace environment, without the need to reboot, dual-boot, or boot from an external USB device. Secure Remote Worker delivers a familiar end user experience, via a secure workspace interface, with the same Windows user experience and advanced levels of security enabling organizations to achieve compliance requirements.

SECURE REMOTE WORKER

Secure Remote Worker Key Features

Full device lock-down

Launching and running Secure Remote Worker on an end user's 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

Data Sheet

Secure Remote Worker Key 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, 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 Key Features

Right place, right time deliver

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 Key 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

Scenario #1

Bring Your Own Windows PC

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

For the IT team, Secure Remote Worker enables them to deliver a BYOD policy or strategy that can be managed centrally, but more importantly, ensures that the end users device is locked down and secure so that corporate security and compliance policies are met.

Scenario #2

Remote & Home Working

Increase workforce productivity by enabling end users to securely connect to the corporate environment, 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 non-office based locations by simply connecting to Wi-Fi, launching their Secure Remote Worker policy driven, secure workspace environment, and then accessing the remote applications and services they require.

Data Sheet

SECURE REMOTE WORKER

What is Secure Remote Worker?

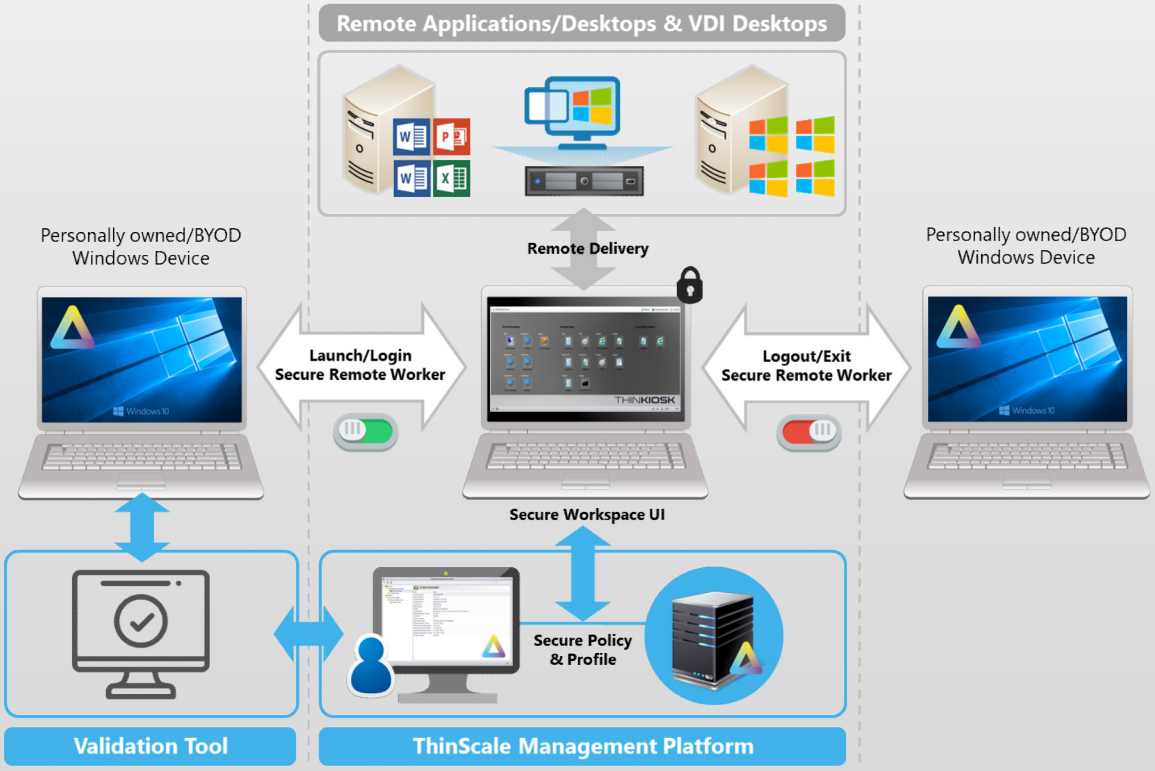
Secure Remote Worker is a software-defined solution that an end user launches as an app on their own personal Windows PC or laptop. It creates a secure workspace environment, managed centrally by IT, enabling end users to have access to corporate resources and services remotely.

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

Data Sheet

Secure Remote Worker 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 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 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

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