SECURE REMOTE WORKER

Quick and Secure Scaling of WAH Using Personal Devices (Secure BYOD)

TECHNICAL DATASHEET

THINSCALE

The Challenges Faced by BPO Organizations Today

As the adoption of work at home increases, IT teams are under pressure to provide technical solutions to some of the challenges typically associated with work at home, including:

- Security and compliance
- Ease and speed of deployment
- Scalability
- Control and supportability
- Cost
- Logistics
- Agent experience
- Agent onboarding

Secure Remote Worker addresses these challenges by enabling agents to work securely from their own personal devices, essentially eliminating the need for the purchase, delivery and management of hardware and the issues associated with this. It does this by converting an unmanaged personal PC into a secure thin client device which is then centrally managed.

Secure Remote Worker Benefits

Deliver PCI and HIPAA Compliance

Secure Remote Worker enables organizations to meet the stringent compliance requirements demanded by QSAs for PCI and HIPAA compliance.

Full Device Lockdown

Secure the agent's device by locking them down with a centralized policy preventing them from accessing the underlying OS.

Familiar Agent Experience

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

Speed Up Agent Onboarding

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

Enables BYOD for Windows

Secure Remote Worker allows agents 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 active.

Secure Workspace Environment

Secure Remote Worker gives agents 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 administrative console.

Reduce Cost, Increase Productivity

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

Endpoint Security and Compliance

Full Lockdown of Personally Owned (BYOD) Devices

Launching and running Secure Remote Worker on an agent'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 agent will access the Secure Remote Worker workspace, a simple and easy to navigate user interface from where they can connect to their virtual/ remote environments securely. They also have the ability to access local applications if set by their IT policy. Their device is only locked down for the duration of the Secure Remote Worker session, and full control is returned to the agent once they log out.

Prevent USB Mass Storage Devices from Being Accessed

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

Secure Remote Worker can prevent these devices from being used while maintaining compatibility with USB hardware (e.g. headsets) with its USB device blocking feature. Enabling this feature means that agents are unable to use USB-based storage devices when accessing corporate systems and data from the secure workspace.

Prevent Unauthorized Apps from Being Launched

The Secure Remote Worker Application Execution Prevention (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 agents are allowed to launch on their endpoint device while Secure Remote Worker is running. These rules allow IT admins to create white/ blacklists which contain a comprehensive list of rule types that delivers a granular level of control over exactly which applications can or 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.

Prevent Unauthorized Services from Running

The Service Execution Prevention (SEP) 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 agent will need to manually stop the service before they can launch Secure Remote Worker on their device.

Securing the Agents' Browsing Experience

An integrated web browser is included as part of the Secure Remote Worker software, complete with a fully customizable user interface that allows agents to securely browse Internet sites or access virtual resources via HTML based on policy set by the IT department, all with the full support of URL white/blacklisting.

The browser is fully compatible with websites as it uses the browser rendering engines of Chrome and Microsoft's Internet Explorer.

Ensuring Devices are Protected and Monitored

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.

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

Prevent Data Leakage on Personal Devices

Secure Remote Worker's Write Filter prevents data leakage between the secure session and local user session. Automatically creating a Virtual File System (VFS) that intercepts all write requests made to the volume, the Write Filter ensures both a clean slate for each new Secure Remote Worker session and a clinical level of separation between your agent's personal session and the secure session.

Furthermore, you can prevent your agents from using locally installed corporate applications with Offline Application Execution Prevention. This allows total control of your agents' access to corporate resources even when outside of the secure session.

Secure Virtual Machines with Contextual Endpoint Information

Secure Remote Worker can also prevent agents from accessing virtual/remote resources from unsecured endpoints using the Virtual Desktop Agent (VDA).

The VDA installs onto any virtual machine/RDSH and will perform checks on any machine attempting to access the VM/RDSH. The VDA can be configured to take a number of actions based on the results of these checks, including denying access from the VM/RDSH outright if it detects an agent is connecting from outside a Secure Remote Worker session. The VDA enables full security and control over your virtual/remote resources across your entire endpoint environment.

Hassle-Free Agent Onboarding

Self–serve Device Readiness Testing on Agents' Machines

Secure Remote Worker includes a unique solution that enables IT admins to check the agent's device before installation of the software to ensure that it meets minimum requirements set by your company policy. The endpoint Validation Tool 'interviews' the endpoint to determine the patch levels, installed software, and whether antivirus is present to name 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.

Simple and Familiar User Experience

The agent experience is key to the productivity and speed of a remote workplace environment. Secure Remote worker delivers a familiar Windows look and feel coupled with an intuitive and customizable secure workspace user interface that enables fast and easy access to virtual/remote environments. It also allows agents to have access to locally installed applications (based on admin set policy) should they need to work offline. Secure Remote Worker also passes through local Ctrl + Alt + Del and other keystrokes and passes them directly through to the remote environment, just as if the agent is working locally on their device.

As a result of being a Windows application, the UI also uses the existing, user-familiar device options such as display, mouse and keyboard, volume and more.

Single Click Installer

Using Secure Remote Worker's Single Click Installer, the initial deployment is as simple as providing your agents with a link. The Single Click Installer is a pre-set installation profile configured by the IT department that will instantly run when the agent clicks the link. The installation profile will also direct the new Secure Remote Worker machine into your Management Console without any user interaction needed, lessening the time spent on initial onboarding. Secure Remote Worker's Single Click Installation allows you to onboard your agents into their secure environments quickly and with little to no intervention from IT.

Scalable Enterprise Architecture

Secure Remote Worker can scale to deliver secure and managed workspace environments for thousands of remote Windows-based PCs, laptops, and thin clients, all managed from the ThinScale Management Platform.

As a software-only solution, Secure Remote Worker delivers flexible scalability and as such, it supports any Windows-based device from any vendor, meaning IT no longer need to worry about what device the agent has. New devices are simply deployed and configured in minutes by applying the pre-configured policies and profiles when the agent switches to 'worker mode'.

Centralized management and control

Ensuring Windows is Always Secure and Up To Date

Secure Remote Worker enables IT departments to easily manage Windows updates, ensuring that the agents are up to date with all the relevant patches 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. Agents can also be prompted to install any of the available updates, or the IT departments can set updates to be installed silently without user intervention or disruption. This ensures that the agents' devices are always up to date, secure, and compliant.

Manage Network Security

Secure Remote Worker allows IT admins to fully configure the Windows Firewall feature internally. They can edit or remove any existing firewall rules, or configure new firewall rules, and manage this centrally from the ThinScale Management Platform and Secure Remote Worker's profile editor.

Third Party Software Deployment and Installation

Through the ThinScale Management Platform, IT can centrally create, save and deploy software packages across their whole environment to be installed locally at the agent's endpoint. Anything from VDI clients, applications and security certificates can all be deployed as software packages. These packages will be installed as per the settings dictated within the ThinScale Management Platform.

Simplified Management, Support, and Onboarding

As Secure Remote Worker is a software-only solution, agents simply download the app, 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 agents to travel in or send devices back.

Solution Brief

What is Secure Remote Worker?

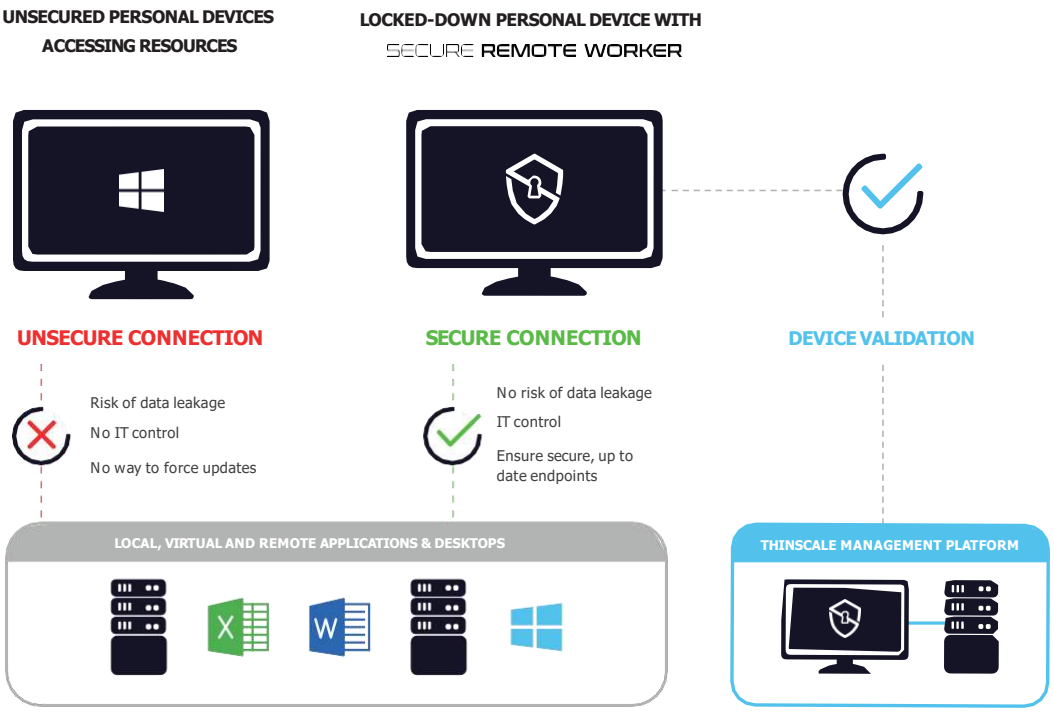
Secure Remote Worker is a Windows application that is installed on the personal PC. On demand, it converts the unmanaged personal PC into a fully managed secure thin client device.

What isn't Secure Remote Worker?

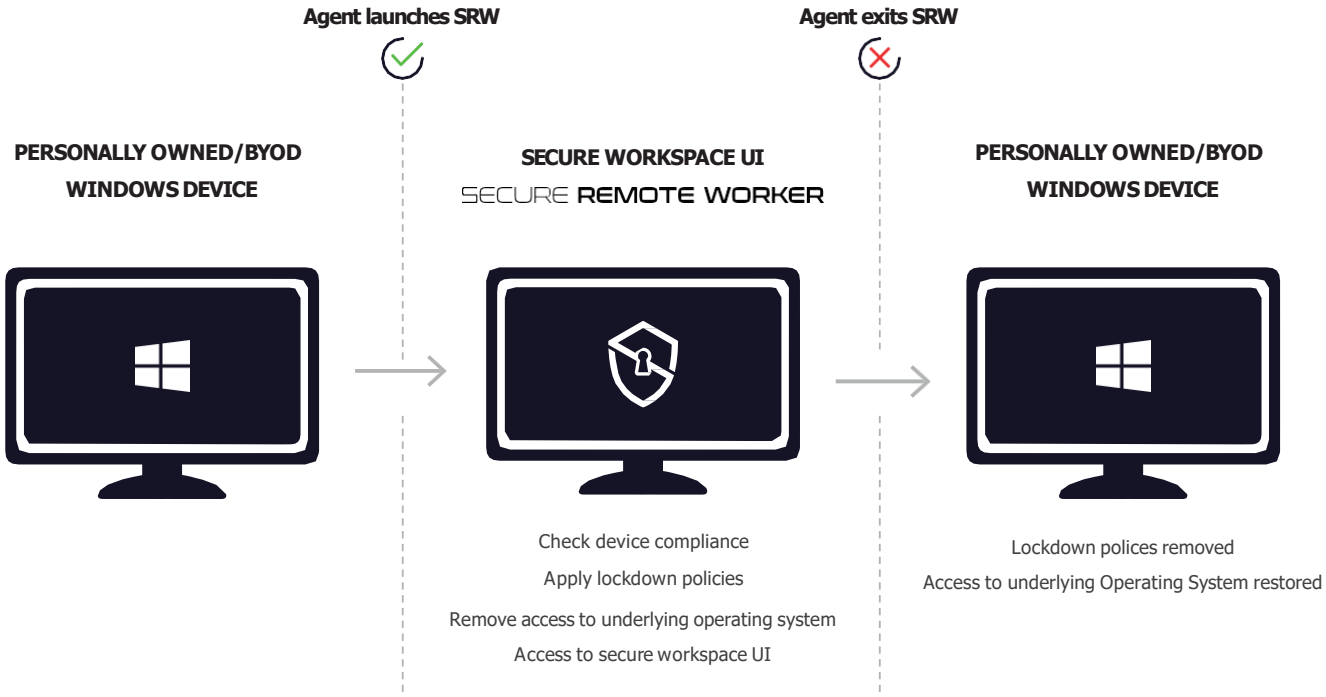
Secure Remote Worker is not a dual boot solution. It runs on top of the existing Windows operating system and does not use container or virtualization technology to run another operating system instance.

How Secure Remote Worker Works

- Uses a separate, low-privilege, encrypted user account created and managed by Secure Remote Worker
- Access policies are evaluated ensuring the personal PC meets security requirements
- Windows Patches are installed
- AV/AS are installed and running
- FireWall policies are applied
- Checks whether or not it is running inside of a virtual machine
- Applies Windows policy settings to prevent access to the underlying OS
- Removes the Windows shell and replaces it with the Secure Remote Worker secure workspace
- Enables its Write Filter to prevent data leakage
- Enables its Application Execution Prevention (AEP) and Service Execution Prevention (SEP) technologies to prevent the execution of unauthorized applications



AGENT LOG ON EXPERIENCE



TECHNICAL SPEC

Secure Remote Worker Components

Secure Remote Worker Client

A lightweight and simple application that launches and blocks the underlying Windows OS on personal devices, compatible with all Windows x64/86 devices.

ThinScale Management Platform

The ThinScale Management Platform provides easy management and control over your entire endpoint environment.

Validation Tool

Secure Remote Worker's Validation Tool runs as a separate executable before Secure Remote Worker itself is installed, it performs checks on the connecting endpoint ensuring they meet the standards set by your IT policy.

Virtual Desktop Agent

Installs on the VM/RDSH and performs checks on the connecting device and performs actions based on whether the connecting device is running Secure Remote Worker.

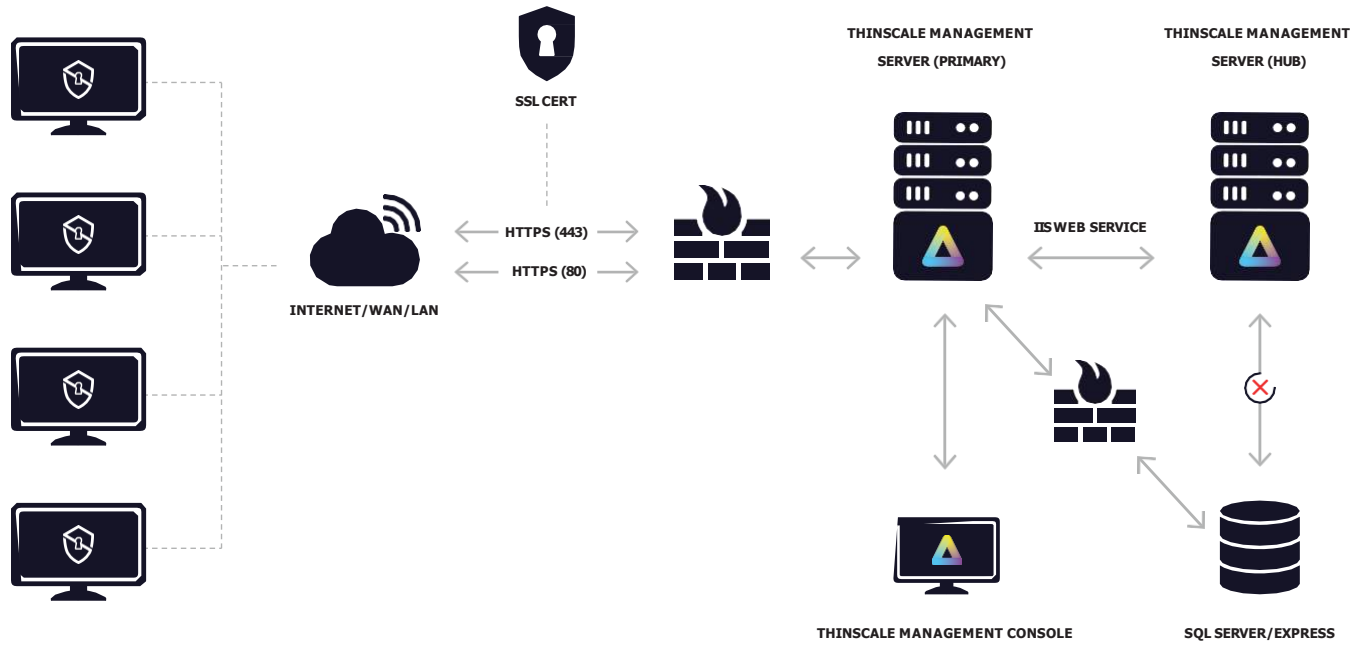
SECURE REMOTE WORKER REQUIREMENTS

Secure Remote Worker Client	• .NET Framework 4.7.2 or above • Windows 10 1809 or higher • Firewall rule allowing Secure Remote Worker to take inbound connections (created by the installer) • At least 4GB of RAM • At least 500MB of free HD space • DigiCert Trusted Root G4 Certificate

Management Server	• Windows Server 2012 or above
	• .NET Framework 4.8 or above
	• .NET Core 6.0.6 Runtime specific
	• Internet Information Services (IIS)
	  ◦ 8.5 for Server 2012 R2
	  ◦ 10.0.14393.0 for Server 2016
	  ◦ 10.0.17763.1 for Server 2019
	• 2GB RAM or above
	• 1GB Free space or above
	• SQL Server 2012 or above (if using SQL for your database)
	  ◦ 1GB minimum DB size
	• SQL Express is also supported
	• BitLocker Drive Encryption
	• BitLocker Network Unlock

Management Console	• Windows 8 or above • .NET Framework 4.7.2 (or above) • 500MB minimum free disk space
Virtual Desktop Agent	• Windows 7 / Windows Server 2012 (or above) • .NET Framework 4.5 (or above)

THINSCALE MANAGEMENT PLATFORM ARCHITECTURE



SECURE REMOTE WORKER FEATURE LIST	
Central Management	• ThinScale Management Server • ThinScale Management Console • Software Package Installation • Scripting Functionality • Roles-Based Administration • Windows Patching Management • Firewall Control Management • Multiple Profile Support • Authentication Provider Integration • Device Analytics
Control	• Local Application Access • Internal VDI/RDSH Connection (Citrix, VMware, RDS, WVD) • Whitelist and Blacklist URLs • Local Application Control (Personal Session)
User Onboarding	• Configuration of Local Settings • Validation Tool • Single Click Installation • Browser Multi-Tab Implementation • Support for Magic Filter • LDAP Integration • Support for 4K Display, DPI Scaling, Duplicate, Extends and Identify
Security	• Endpoint Protection Features • Endpoint Security Features • Secure Browser • Dual Persona • Windows Security Center Detection • Virtual Machine Detection • Anti Virus Definition Detection • Anti Spyware Definition Detection • WiFi Detection • Application Execution Prevention (AEP) Implementation • Service Execution Prevention (SEP) Implementation • USB Mass Storage • ThinScale Virtual Desktop Agent (VDA)

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

+353 1906 9250
hello@thinscale.com