Secure Remote Worker (SRW)

Enable Secure & Compliant BYOD Workspaces on Any Windows Device

What is it?

Secure Remote Worker (SRW) is a software solution that locks down personal or unmanaged Windows devices, creating a temporary, IT-managed workspace. It enforces corporate policies while keeping the user's personal environment untouched, enabling secure access for remote staff, contractors and third parties.

How is it installed?

Devices are first validated with ThinScale's Validation Tool to ensure security and performance. Once approved, SRW installs in minutes using a Single Click Installer. Users launch a secure session from their desktop, entering an isolated workspace without altering their personal device.

What will it do?

- **Secure, isolated session:** Users log into a controlled workspace, separate from personal profiles.
- **Corporate access:** Access to VDI or local apps without admin rights.
- **App & URL controls:** Whitelisting/blacklisting stops malware and blocks unauthorised access.
- **Encrypted storage:** Temporary, BitLocker-protected drive.
- **Location-based access:** Only from approved geographies.
- **USB/media control:** Blocks untrusted devices and only allows essentials such as keyboards and mice.
- **Data Loss Prevention (DLP):** Prevents data transfer. Data can self-delete after sessions.
- **Seamless exit:** Returns user to personal desktop unchanged.

Key Benefits

Lower Costs
Secure BYOD reduces reliance on corporate hardware.

Easy On/Offboarding
Validation tool screens devices, quick setup, no hardware to recover.

Enhances Endpoint Security
Isolated workspace with app controls, USB restrictions, and DLP.

Rapid Scalability
Deploy in minutes, ideal for large rollouts.

Key Use Cases

Remote & Hybrid Employees
Use personal laptops securely. SRW enforces corporate policies without company-issued hardware.

Third-Party Contractors
Onboard quickly and securely. Provide controlled access to workspaces and corporate resources without exposing sensitive data.

BPO Teams
Manage high-turnover environments. Enforce security policies on devices outside IT control.