Global Outsourcer Achieves Secure, PCI Compliant Work at Home Environments While Reducing Overheads with Secure Remote Worker

CUSTOMER

Global Outsourcer

SECTOR

Business Process Outsourcing

REGION

Global

EMPLOYEES

223,000+

THE CHALLENGES

- Costly and time-consuming logistics
- Lack of control with existing BYOD model
- Seasonality changes requiring scaling of service
- Stringent security and compliance requirements
- Slow and expensive onboarding of agents

The company in this case study is one of the worlds largest call center companies or Business Process Outsourcing (BPO) providers, connecting the biggest and the most respected brands on the planet with their customers.

Currently there are circa 223, 000 employees, or agents, delivering call center services ranging from technical support, customer care, sales, offshore, and research. Agents are based across 350 contact centers in 76 countries, covering 265 different languages.

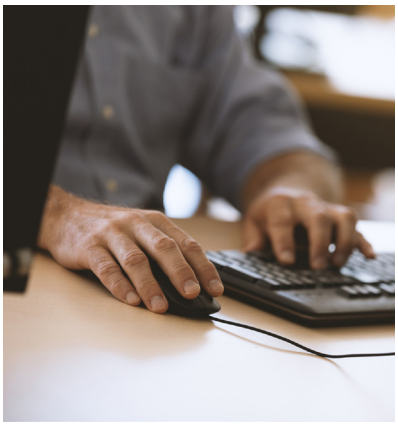
In order to attract new talent and respond quickly to the ever-changing customer demands, this company needed a modern solution that enabled them to deliver a flexible working initiative. They wanted to allow agents to work at home using their personal devices, instead of a company-supplied device. Above all else, the solution needed to deliver a secure working environment.

The Challenges

In the past, in order to enable agents to work at home, the outsourcer would provide agents with their entire IT setup, including a physical phone, home phone line, and a thin client device. This process soon became costly, time-consuming and problematic. The IT team effectively became a hardware delivery service and a support desk to manage queries and issues associated with that.

This process also hindered the length of time for new agents to get up and running, slowing down the overall onboarding time.

> “Certifying work at home is challenging. Unlike an office environment you can’t change an agent’s PC, or have a supervisor overlooking an agent’s work to guarantee productivity.”
>
> *Principal Architect*



THE SOLUTION

- Software-only BYOD model with centralized control
- Fast and hassle-free onboarding of new agents
- Secure and compliant work at home using agents' own personal devices

> "Secure Remote Worker has revolutionized security for our BYOD model, enabling us to leverage an agent's home PC securely and without them breaking out of the session"

Director of Work at Home

Agents often struggled with the unfamiliar new device and often struggled to connect to monitors and other hardware.

To reduce costs and to simplify and speed up the recruitment of new agents, the outsourcer looked to move away from this model. With the growing popularity of BYOD, the outsourcer explored ways to set up the agents on their own home PC to connect back to the outsourcer's systems for their work session.

However, that model presented a whole new set of security challenges.

One of the biggest issues was with controlling the remote sessions. Even though agents were forced into a full screen session, they very quickly worked out how to break out of that session. For the outsourcer, this meant that they could not guarantee that the agent was delivering their services to the customers. If they were surfing the Internet, or running other apps, there was also a huge potential for data leakage. While they believed in the benefits of this BYOD model for the business and for their agents, they needed to ensure that it was secure.

The outsourcer also needed to deliver an experience that closely resembles a hardware-based experience to guarantee that the agents received the best performance possible, therefore ensuring maximum productivity.

Being in the service business, there are times when they need to scale up the number of agents to cater for seasonal demands. For example, they tend to add thousands of agents in the United States between Thanksgiving and Christmas to cope with the extra demand.

The other onboarding issue was around training. There are two weeks of training before the agents start working. During this time, there can be substantial turnover (anything up to 20%), and the outsourcer has to start the cycle of retrieving the devices and sending them out to the new agents. This attrition has led to increased costs and frustration for the IT team.

The Solution

Before selecting Secure Remote Worker, the outsourcer looked at several alternative solutions. However, none of them delivered the features and requirements needed to allow agents to use their personal devices for secure work at home. Key obstacles included the fact that the devices were not domain joined and required many changes to be made to the agent's underlying PC.

“From a single click, the whole process takes under four minutes and the agent is up and running. No comparison to hardware-based solutions!”

Director of Work at Home

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

The secure workspace environment is managed centrally using the ThinScale Management Platform. Manage your entire remote device estate using a single management platform with a single administrative console.

Secure Remote Worker Delivers Flexible, Scalable and Cost-effective Work at Home

Secure Remote Worker is a software-only Windows application that is installed on the agent’s personal Windows PC. On demand, it converts the unmanaged PC into a fully managed secure device.

This allows the outsourcer to deliver its work at home initiative, safe in the knowledge that agents are secure when connected to their work sessions and that they cannot break out of sessions or compromise data. The flexibility of Secure Remote Worker means that they can solve their challenges in delivering a secure work at home environment.

The Benefits

Secure Remote Worker Solved the Security Risks and Challenges of Work at Home

With Secure Remote Worker, the outsourcer can now trust the Windows session. Its ability to temporarily deploy a secure workspace environment using the agent’s personal Windows device, disabling access to the underlying OS provides a peace of mind to the outsourcer.

As Secure Remote Worker locks down the device and prevents other apps or services from running on the agent’s PC, it has resulted in better performance due to fewer resources being consumed.

Enabling PCI Compliance for BYOD and Work at Home

To achieve PCI compliance, the outsourcer had to successfully complete a questionnaire and audit to ensure that all compliance criteria had been met. In the case of Secure Remote Worker, the secure workspace environment that Secure Remote Worker delivers to the agents is considered to be *the* managed endpoint for PCI DSS compliance. Therefore, Secure Remote Worker provides the coverage for the PCI DSS requirements that outsourcers need in order to meet compliance standards.

> “Secure Remote Worker is instrumental in certifying [the outsourcer’s] work from home platform, especially when it comes to BYOD and ‘compensating control’ to achieve PCI compliance”
>
> *Director of Work at Home*

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’.

FAMILIAR AGENT EXPERIENCE

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

BUSINESS CONTINUITY

With business continuity in mind, work at home agents can easily access their digital environments through Secure Remote Worker on their personal device.

Fast, Quick and Hassle-Free Agent Onboarding

Without having to ship physical devices to new agents, the onboarding process is reduced from days to just minutes, while at the same time removing the cost of shipping devices. Agents are able to download and run Secure Remote Worker immediately, on a device they are familiar with, allowing them to become productive much quicker.

On the flip side, if they drop out of initial training or when the seasonal demand is over, the outsourcer can simply retract the Secure Remote Worker license, instantly taking away the agent’s access.

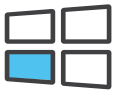
To onboard an agent, the outsourcer simply sends them a link that upon clicking, installs the Secure Remote Worker software. Once installed, Secure Remote Worker can be launched and the device will be temporarily locked down as the agent enters secure ‘worker mode’. In this mode, the agent can connect to the outsourcer’s environment and download settings, updates and security policies and software packages. The agents can then access their work sessions securely.

Increasing Availability and Business Continuity

By delivering services with work at home agents using their personal devices and Secure Remote Worker, the outsourcer has seen an increase in the availability of services they deliver to their customers. If an entire call center goes offline, hundreds of agents are affected. Whereas, if a work at home agent has connectivity issues, they would be the only one affected. This results in much higher availability for work at home.

This has also been the case for faulty devices. In some cases, work at home agents would be able to deploy work avoidance tactics, knowing that a faulty device would take around three to four days to be replaced and shipped to them. Secure Remote Worker removes this problem by allowing the software to be reinstalled or fixed remotely. If it is a hardware issue, the agent can quickly get this fixed without having to wait for new hardware to arrive.

> "We have a specific requirement to deliver BYOD and home working with Secure Remote Worker. In fact, we can't do it without Secure Remote Worker"
>
> *Director of Work at Home*



SOFTWARE-ONLY

Secure Remote Worker runs on existing Windows devices as an application without overwriting them, without needing to dual-boot, or booting from an external USB device.

Reducing Costs With Secure Remote Worker

Although security was the main driver, Secure Remote Worker, by default, helped reduce costs. The cost of deploying a software-only solution is only around 25% of the cost of a physical hardware-based thin client. Without having to purchase physical thin client devices and instead deploy a software-only solution on agents' existing devices, deployment and onboarding costs were dramatically reduced.

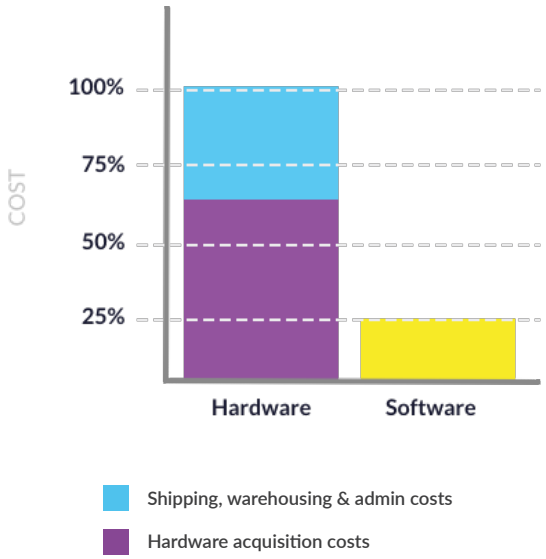
There was also the question of managing this process. At peak times, there could be anything up to 20% of agents that would leave the outsourcer and not return the devices they were provided with. Therefore, replacements would need to be purchased which led to an increased cost and delay in onboarding new agents.

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.

With Secure Remote Worker, there is no physical device to worry about, so there is no loss of physical assets. It's just a simple case of retracting the Secure Remote Worker license from the leaving agent, and then applying it to the new agents.

The cost of hardware versus Secure Remote Worker



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

+353 1906 9250
hello@thinscale.com