# Global Outsourcer Revolutionizes Work at Home Using Secure Remote Worker

### CUSTOMER

Global Outsourcer

### SECTOR

Business Process Outsourcing

### REGION

USA HQ / Global

### EMPLOYEES

55,000 +

### THE CHALLENGES

- Deliver BYOD for work at home agents
- Reduce costs and logistical overheads
- Meet compliance requirements
- Scalability
- Achieving PCI/HIPAA compliance in a BYOD environment

The company in this case study is a digital marketing and customer service global outsourcer, providing customer engagement services to Global 2000 companies. They provide solutions to major companies around the world, primarily in the retail, communications, financial services, technology and healthcare industries.

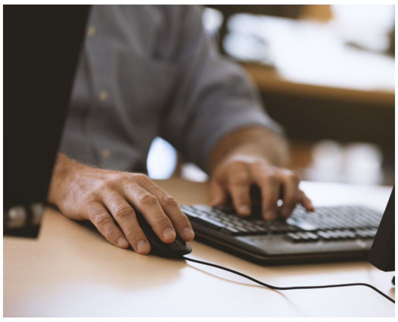
Customers look to this company for their solutions but often bring their own tools with the outsourcer delivering the support. Each client has a unique set of requirements that the outsourcer has the flexibility and expertise to deliver.

## The Challenges

As the largest call center company that offers agents the ability to work at home, this company needed to solve the challenge of how to deliver a secure and compliant workspace environment to those agents.

The original solution was to send a bootable CD to the agents, which booted their PCs into a Linux environment with the relevant connection software. This allowed agents to connect to the outsourcer's central systems. However, as this solution relied on the agent having compatible hardware, the outsourcer began providing hardware for their work at home agents instead. Agents were given a thin profile ASUS PC, complete with a regular operating system that was shipped to the agents' homes. However, it also came with its own set of challenges around logistics and support.

The outsourcer now had to purchase and maintain an inventory of equipment including retrieving devices when an agent leaves the company, which all had a cost associated with it. This also presented a challenge to IT support in trying to keep up with patch levels of the devices that were out in the field.



## THE SOLUTION

- ✓ Delivers a dynamic, secure and PCI compliant workspace
- ✓ Enhances the flexibility for IT and agents working from home using their own device.
- ✓ Reduced time, cost, and complexity of client management

## THE BENEFITS

- Secure Remote Worker locks down the agent's personal Windows device ensuring PCI compliance requirements are met.
- Agent devices can be assessed for suitability as part of the onboarding process, eliminating the need for time-consuming troubleshooting.
- Removes the need to manage a physical hardware inventory and assets, eliminating logistical costs.
- Easily scale up and scale back work at home agents.

Regardless of the deployed solution (including any new solution), security compliance was the number one concern and challenge to solve. The outsourcer needed to ensure that anything deployed outside the brick and mortar sites met PCI and HIPAA compliance and the key question was whether any solution deployed remotely could pass a QSA.

Having looked at the solutions currently available on the market at the time, the company felt that no one vendor had an out-of-the-box solution that met their requirements, other than Secure Remote Worker from ThinScale.

# The Solution

The outsourcer deployed Secure Remote Worker to the work at home agents, allowing them to overlay an existing device with the Secure Remote Worker software. This allowed the agents to use their personal devices and removes the need for the outsourcer to supply and manage hardware.

The ThinScale Validation Tool in Secure Remote Worker allows the outsourcer to conduct specific checks on agents' devices (e.g. the ability to check if the device is adequately patched). This tool compares the device policies against the outsourcer's own policies to check what is required to meet compliance standards.

With the Validation Tool, the outsourcer can provide the work at home agents with a self-help document to help fix any issues that may be highlighted. For example, if a highlighted issue relates to anti-virus, the work at home agent will be provided with a URL that links them to a guide on how to solve the issue.

> “
> The dynamics of how people want to work today is very different from 5 years ago. Work at home is a model that fits many more demographics, enabling us to target medium and large cities to recruit new talent
>
> *Principal Architect*

# Delivering PCI Compliance

How Secure Remote Worker Helped the Outsourcer Achieve PCI DSS Compliance Requirements

PCI DSS COMPLIANT

Secure Remote Worker was assessed and certified by two globally accredited QSAs, Coalfire Systems and Schellman & Company.

DEVICE LOCK DOWN

Together, they agreed that Secure Remote Worker is to be treated as *the* endpoint for PCI DSS purposes. As the underlying device OS is not transmitting any data and is not accessible by the agent during the Secure Remote Worker session, it is treated as a Point of Sale device (PoS). In turn, Secure Remote Worker is treated as the operating system.

This vastly simplified the outsourcer's approach to auditing as they no longer had to audit each PC sent to agents. Instead, all the PoS devices would make up one line in the inventory: *X number of BYOD devices*. This hugely reduced the overheads of device support.

> “ The daily grind of having to patch, having to evaluate, and having to talk to auditors was removed. The other solutions were all missing something that performed all the 'checks and balances'.  Other vendors' solutions don't check for compliance, they just give you a desktop or an application.
>
> *Principal Architect Systems*

FIREWALL POLICIES

Instead, Secure Remote Worker checks all the PCI related requirements before a device is allowed to connect to the outsourcer network. Details on these requirements can be found in the PCI DSS Compliance White Paper created by Coalfire Systems.

With Secure Remote Worker, the outsourcer could set up a single virtual machine within their environment that simulated a BYOD for each unique PCI client and a line of business profile that would be accessible for the auditing team. Audit testing is then accomplished via the line of business virtual machine in the environment.

WINDOWS PATCH MANAGEMENT

Taking all the features and elements delivered by Secure Remote Worker into account, enabled the outsourcer to work with the QSAs to certify their work at home with BYOD solution is PCI compliant.

### BYOD & WORK AT HOME

With Secure Remote Worker, the outsourcer can allow work from home agents to use their own devices.

### WORK AT HOME AGENT SCALABILITY

Agents can be quickly onboarded as companies scale to meet seasonal business demands.

### LOWERING COSTS

Removing hardware management and logistical challenges reduces costs.

> “
>
> It’s a true partnership working with the team at ThinScale. In the 26 years I have worked in the IT business, this is truly the first time a partnership I’ve been involved with has really been a partnership.
>
> *Sr Director Global Design Engineering*

## The Benefits

Deploying Secure Remote Worker takes the outsourcer out of the hardware business, removing the need for device inventory maintenance. It removes the logistical pressures required to manage and deliver devices out to work at home agents. It also takes away the burden of patching and evaluating the agent’s personal device for compatibility and auditing, resulting in a dramatic cut in costs and time.

The outsourcer no longer needs to send out a physical device, and more importantly they no longer have to retrieve devices when an agent leaves the company.

IT operations like the ability to send out the Validation Tool to ensure the device is patched and the AV is up to date. It used to take several hours for IT to work with a new agent to check the agent’s device, but that is no longer the case. Secure Remote Worker saves time in troubleshooting PCs and has cut the initial deployment failure rates from 30% down to around 5%. The outsourcer also integrated the Validation Tool into their hiring process, which allowed them to set criteria for pre-existing devices such as internet quality and security status for prospective agents. This way, they could hire agents knowing that the device would meet their standards. This simplifies the hiring process for work at home and ensures that agents would be able to work on validated machines from the get-go, with no time lost on incompatible or severely outdated machines.

PCI DSS Compliance was the primary concern for the outsourcer when deploying work at home agents. With Secure Remote Worker, the outsourcer can not only deliver a PCI compliant working environment to agents working from home, but it also allows them to use their own devices.

The ability to deliver work at home means that the outsourcer can broaden the resource pool for its workforce. Prospective agents can fit their working life around family life, and for the outsourcer, this leads to an increased talent pool.

## In Summary

With Secure Remote Worker, the outsourcer is now able to offer and deliver a secure working environment to agents working at home, using their personal devices. This results in substantial cost savings, reduced time spent by IT in troubleshooting, an improved onboarding process and most importantly, PCI compliance.

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

**+353 1906 9250**
**hello@thinscale.com**