Tech Mahindra
BUSINESS PROCESS SERVICES

Work at Home Contact Center

White Paper Data Protection, Security and Employee Safety

Connected World.
Connected Experiences.

Introduction

The Tech Mahindra Work at Home solution is a transformational work-at-home contact center model that delivers a high-quality, geographically distributed people solution combined with a comprehensive suite of remote work tools, CRM solutions, SaaS options and consulting services to support your multi-channel customer experience.

Remote Workforces are growing and a clear trend is emerging in today's workforce.
Embracing work at home programs allows contact center organizations to benefit from greater access to talent, improved performance & productivity business continuity, lower overhead costs and happier employees.

- 83% of organizations that have flexible work policies report an increase in employee productivity.
- 95% of companies that allow teleworking have seen a positive impact on employee retention.
- The average for a full time work at home employee $5,000 -$10,000 annually.
- More than 50% of full time employees are expected to work remotely by 2022.

Pre and post-COVID, work-at-home agents (WAHA's) are the greatest single change is the contact center model in history. However, there is a specific recipe. Standard brick and mortar tools and processes will not ensure a highly secure and safe environment and can put company data and customer information at risk.

Work at Home Safety & Security

People:
The work at home contact center space naturally attracts more experienced and mature people, which is one of the keys to a safe and secure remote contact center solution. In order to successfully attract and hire this kind of talent, a customized approach is required. This approach generally leverages a customized sourcing strategy and features security and technology assessments that are specific to working remote.

Processes:
Human Resources policies and procedures need to be fully customized to support work at home businesses and unique business processes. In addition, work at home providers should implement activity monitoring, physical and virtual audits and one-one coaching sessions to ensure that any risks associated with remote employees are addressed and mitigated. National (State and local) background checks are also generally standard protocol for high quality Work at Home providers.

Technology:
In today's robust technology marketplace and due to the COVID 19 pandemic, many work-at-home technology solutions exist. Customized hardware and software solutions, integrating telephony and securing transactions are all required for to deployment of work at home programs.

Desktop Setup / Device Security

Whenever a work at home agent contact center agent is deployed, access to various systems will be required from the remote location so that the agent can support clients and their customers with outstanding customer experiences. Therefore, a high-speed internet connection and workstation is needed. Generally, a closed-door office, free of noise and disturbances is required along with a standard high-speed internet connection that is hard-wired; not wireless. Companies can elect to send out company-owned workstations or enable a BYOD (bring your own device) model empowering the employee to leverage their existing in-house computer. Desktops or laptops quality; even tablets can be used along with a keyboard and monitor. However, desktops PC's with two 20-inch or larger monitors are preferred for an optimized experience. Some companies assist with associated workstation costs, however in most mature markets, this is an unnecessary corporate expense

Once the workstation solution has been determined, security protocols must be administered on the machines as follows:

Company supplied machines:
For laptops or desktops setup in the office, machines should be "hardened" with software and / or VDI and endpoint managed from office location. Any changes / updates would be managed from the site IT.

BYOD (Bring Your Own Device):
Managing the logistics of machine deployment and retrieval from a physical location at scale can be extremely resource-heavy, time consuming and expensive. Therefore, many companies and BPO's leverage the BYOD model for Work at Home employees and contact center agents. When using this model, it is critical to ensure a secure that the BYOD can securely access the client network, CRM and set of tools with a security tool such as a VPN (virtual private network) or VDI (virtual desktop infrastructure).

Work at Home Security Options - VPN VS. VDI

Let's first look at some facts and definitions:

VPN: A (VPN) virtual private network extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

VDI: Desktop virtualization is a software technology that separates the desktop environment and associated application software from the physical client device that is used to access it.

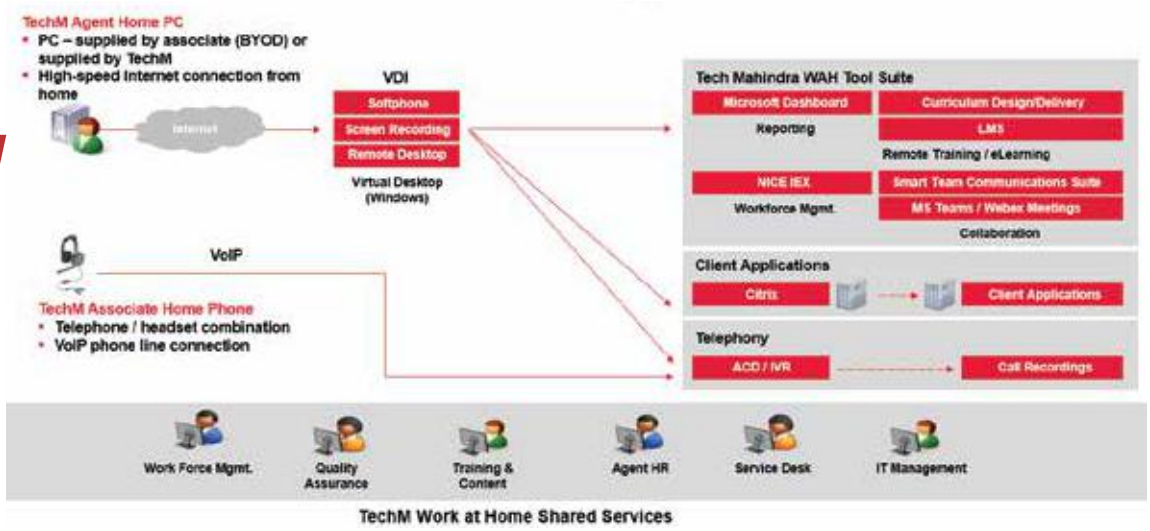
In other words: A VPN is designed to protect a data hack from the home users connection and the private network needed to access customer data. A VDI solution also contains VPN security that connects a private network to a secure cloud, thereby creating a separation from the machine that is being used and the private network. This solution is more expensive, but contains more features and is used in BYOD operating models.

This way of working has proven to be just a safe and secure as any thin client or physical device deployment solution.

More about VDI

- Device Agnostic.
- Easy to scale across multiple global geographies.
- Access via desktops, laptops, tablets, thin/zero clients and even smartphones.
- Ideal for BYOD programs and markets.
- Secures the endpoint against device theft or loss.
- Controls where data resides by getting it from the endpoint.
- PCI and HIPAA compliant desktop solutions so you can easily extend desktop compliance to all employees everywhere.
- Manage all desktops from a central location-whether the desktop is onsite or with a remote worker.
- View infrastructure, monitoring and reporting from a single pane of glass.
- Rapid build and deployment of secure image.
- 99.95% uptime.
- Fail-over and redundant cloud data centers.

TechM Work at Home Technology Infrastructure



TechM Work at Home Shared Services

Technology Controls

- Fully redundant global Virtual Desktop Infrastructure (VDI) with colocation facilities in US, Europe and APAC regions
- BYOD model includes work station specification check and internet speed connectivity testing
- Dedicated agent operating system with secure connection to all work related data and client networks
- Data always resides within the VDI environment
- Multi Factor authentication
- Lock down of workstation; users cannot toggle from VDI
- Disable printing, faxing, connectivity to any peripheral device
- No ability to copy data inside the VDI and paste outside
- Masking of sensitive data on screen and voice
- Internet browser restrictions (white listing)
- VDI Login logs are captured in central logs repository for audit purpose
- TechM applications accessible using Active Directory Sing Sign On
- Covert and overt supervisor remote access to agent desktop
- Screen recording and archival
- Agent level productivity reporting
- PCI Compliant / HIPAA Compliant

Data Protection Culture

In our experience, the “people” element is just as important as the “technology” element in keeping a work at home contact center safe, secure and free of fraud. The following are business controls that are implemented in the TechM work at home contact center solution:

- Live Control Center monitoring - real-time user interface that shows all virtual agents, work status
- Application usage monitoring & trends
- While working, all TechM WAH agents are in a virtual community, which is dedicated to each program
- Work at Home Associate Handbook
    - Legally binding Employee Agreement including all facets of home working including safety, security of data, access control
    - Physical workplace environment and home visits
    - Clean desk policy - no recording devices or cameras are allowed in work place
- Virtual audits
- Leverage a geographically distributed hiring model to access high quality talent
- Background checks for all TechM agents