THINSCALE

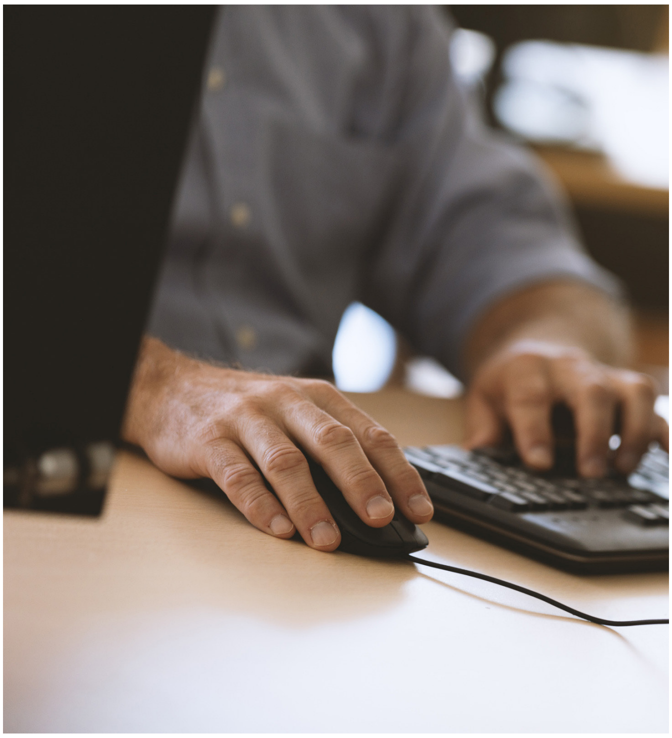
CIO and CTO's Guide to Scalable, Secure Work at Home

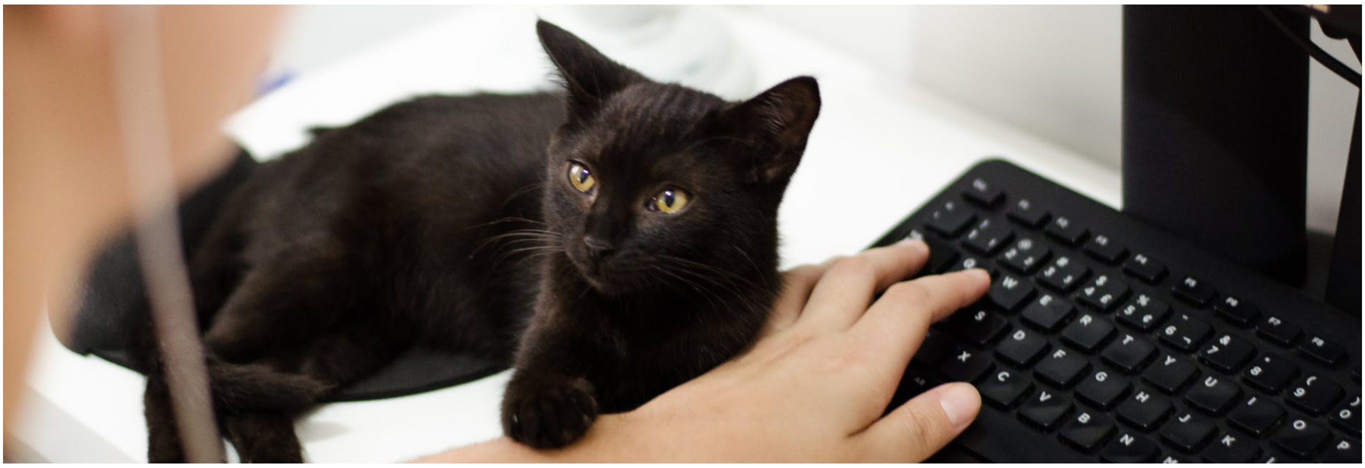
Introduction

The benefits of work at home are well documented: productivity increases, employee satisfaction improves, recruitment and retention metrics increase significantly, and companies gain from savings on office space and other overheads.

It is little wonder therefore that work at home is growing at a dramatic pace with the number of at-home workers in the US increasing by 115% since 2005. And many see this as a means of resolving some of the key challenges facing the Business Process Outsourcing (BPO) industry today.

Work at home expands the available labor pool to include those who could not previously work in contact center jobs including people with disabilities, those living in rural areas, and primary family caregivers. Enhanced job satisfaction also has a significant positive impact on retention rates.





Work at home brings many other benefits including a quite astonishing 55% increase in productivity. Further benefits include significant office overhead savings of up to $11,000 per employee and an effective pay rise for employees through savings in commuting and other work-related costs of between $2,000 and $7,000 per annum.

In addition, it is estimated that if people in the US worked from home just half the time they currently spend working in the office, greenhouse gas emissions would be reduced by 54 million tons.

However, enabling work at home, especially the technical elements, has historically been a challenge for most organizations. Generally speaking, there was a choice between scalable work at home or secure work at home, but not both.

In many cases, scalable work at home meant leaving security gaps by utilizing agents' personal computers without being able to effectively secure them. Secure work at home meant providing corporate devices leading to logistical and support headaches and uncontrollable costs.

This is no longer the case, however, and solutions combining software and agents' own computers can deliver all of the key benefits of work at home at scale and without compromising security or increasing costs.

This paper presents a CTO and CIO's guide on how the most innovative BPOs are using this approach to enable scalable and secure work at home. It primarily focuses on this from a technical and operational perspective. Most importantly, it will show how you can deliver those same innovations.

WORK AT HOME

The Benefits

Work at home is now widely accepted as being a key feature of the future business process outsourcing world. In a low margin industry, work at home has the potential to deliver huge cost savings and consequent bottom line benefits.

> “It’s extremely expensive to open a contact center, provide equipment and infrastructure. Work at home can be upwards of 40% cheaper than a physical contact center.”
>
> *Doug Berry, Former Sr. Director, Global Work at Home,*
> *Sutherland Global and Concentrix*

If you already understand and appreciate the benefits of work at home, please feel free to skip this section. If you need to be convinced, please read on.

Benefits

Improved Retention

Hiring

Reduced Real Estate Costs

Improved Productivity

Positive Environmental and Rural Community Impact

Improved retention

Attrition rates vary widely in the BPO industry. Publicly declared rates range from 21% to 48% annually. Leading contact center analyst firm, Contact Babel, found an average attrition rate of 30% in the industry.

When discussing the issue in private, the industry tends to reveal much higher rates with numbers as high as 70% being reported with the average somewhere in the 30% to 40% range.

The cost impact is very significant. It is estimated that the total cost of replacing a single employee ranges between 90% and 200% of their annual salary. According to Vicki Brackett, a 25 year C-Level contact center consultant, the average cost of replacing a contact center employee in the US is about $20,000.

Work at home can have a significant impact on these costs. A Stanford University study of 500 travel agency employees found that those working from home had a 50% lower attrition rate. Similarly, Global Workplace Analytics found a 25% reduction in attrition among home and remote workers (GWA, 2010).

Hiring

An analysis of the top 30 BPOs by Everest has shown that 77% of those who issued annual reports mentioned hiring as a key risk factor to company performance. That risk factor is exacerbated by high attrition rates.

With an average attrition rate of between 30% and 40%, a BPO must effectively rehire every single employee every three years, and that's before recruiting additional employees to account for growth. For many BPOs, this can mean finding tens of thousands of new employees each year.

At a time of historically low unemployment rates, this poses a major strategic and operational problem. Even if they succeed in finding candidates for the vacancies, the potential cost implications are enormous. For example, a 1,000 employee BPO can expect to incur costs ranging from $9.8 million to $21.7 million annually as a result of attrition. And this ignores the opportunity cost associated with an inability to meet growing customer demand.

Annual Employee Replacement Costs per 1,000 Agent BPO = $9.8 million – $21.7 million

Work at home helps resolve this problem by enabling employers to target recruitment campaigns at the areas of maximum opportunity. These can include regions with higher unemployment and specific groups of people who cannot access conventional jobs for one reason or another.

For example, the location independent aspect of work at home allows campaigns to target rural areas which have traditionally been subject to high unemployment. Rural areas are also highly appealing due to their lower living costs not to mention the political and corporate brand benefits of providing much needed employment in such areas. This could be particularly effective for contact center jobs with relatively low pay which are far less attractive for city workers who have to contend with a much higher cost of living. $31,000 a year goes a lot further in Salem, AL or Huddersfield, England than it would in San Francisco, CA or London.

It also facilitates the hiring of people who find it hard to access the workforce. For example, one UK BPO that operates a pure work at home model has reported that 12% of its employees are registered disabled. Similarly, a US BPO targets military moms who move from place to place and base to base and who ordinarily experience difficulties finding work due to that mobility. With work at home that mobility ceases to be an issue.

Reduced Real Estate Costs

Global Workplace Analytics estimates that contact centers save $10,000 on real estate costs for each agent who works from home. Work at home allows BPOs to utilize an employee's own infrastructure rather than paying rent, electricity, insurance and other costs on physical contact center space.

AT&T saved over $6 million annually as a result of 600 employees telecommuting in New Jersey – exactly $10,000 in savings per agent. A report compiled by Telework Research Network showed real estate savings can be as high as 18%.

Improved Productivity

Improving productivity is a key challenge for all commercial organizations. Labor is the largest single cost for contact centers by far with many reports showing it comes in above 70% of total costs. Increased employee productivity therefore has a far greater impact on contact centers than other industries.

There is a considerable body of research to indicate that work at home leads to an increase in productivity. On the low end, a Harvard Business School led research project found a 4.4% increase in productivity from work at home. For contact center workers, Global Workplace Analytics found work at home increases productivity by up to 55%.

Positive Environmental and Rural Community Impact

According to Wharton professor Dipak Kumar the main reason people leave rural communities is a 'lack of academic and economic opportunity'. Work at home brings much needed economic opportunity to those communities. And it allows companies that are struggling to hire in cities to specifically target areas where labor is available.

From an environmental perspective, it leads to improved sustainability through a reduction in commutes with consequent CO_2 and other greenhouse gas emissions decreases.

WORK AT HOME

Key Challenges

While work at home undoubtedly offers many benefits both human and to the bottom line, it also presents a range of challenges. While these challenges vary widely, the focus of this white paper is on the technical issues faced by BPOs when implementing work at home programs.

Indeed, while the range of solutions for the delivery of work at home is potentially very wide each has technical issues which must be resolved before the benefits can be realized. These issues range from security and compliance to difficulties providing support to many hundreds of remote agents who are potentially using a diverse range of devices and operating systems

Security and compliance | Remote Communication and collaboration | Recruitment and Onboarding | Maintenance and Operation | Supporting Agents

Security and Compliance

Security is absolutely critical in the BPO world with compliance requirements ranging from PCI, HIPAA, GDPR and numerous financial regulations. The relatively easy part is securing the backend infrastructure. The main players including VMWare, Citrix, and Microsoft all provide blueprints on how to implement compliant environments and checks. Dizzion, for example, offers ongoing compliance as a service built into its solution.

The home environment presents an altogether stiffer challenge. Policies have to be put in place for a whole range of eventualities not normally considered in the workplace, particularly in relation to credit card data. Every point in a credit card transaction must be secure and comply with PCI and other regulations. Additional risks in the home environment include data leaking from employee devices, malware running on a computer, employees taking pictures of screens, and so on.

Organizations must use a mix of people, process and technology in order to achieve their desired security and compliance outcomes, regardless of the employee's location. The people aspect tends to be most difficult and is usually dealt with by HR. The HR solution normally requires an employee to sign an agreement regarding their behavior but there is no guarantee of adherence and such agreements are very difficult to police. Indeed, ThinScale has encountered instances of employees being required to video their home working environment on a webcam to ensure it meets workplace regulations. However, employers cannot be assured that the images in the video are actually of the employee's home.

Greater certainty can be achieved with process and technology, but this usually comes at a cost with the employer having to retain ownership and control of all devices and software used by the home worker. This has contributed to a mistaken belief that work at home solutions cannot be delivered successfully using employees' own devices.

Remote Communication and Collaboration

Remote communication and collaboration have always represented a barrier to remote work and work at home. Research shows that remote workers face issues not shared by office workers. A study carried out by Igloo Software shows that seven in ten remote workers face challenges they would not face in an office. These include missing important information communicated in person, being excluded from meetings and not having the technology to do their job.

According to Harvard Business Review, different management methods are required for remote teams while it is also important to consider the technical solutions that are needed to ensure effective communication and collaboration. This virtual workplace technology includes both internal and external communications and chat software.

Recruitment and Onboarding

From a technical perspective, work at home introduces new dynamics into the recruitment and onboarding process, primarily concerning the endpoint and bandwidth.

Simplicity is essential due to the distance between the agent and the support team. Hardware can present a variety of issues such as keyboards not working and hardware not connecting to the network. BYOD, or more accurately AOD (agent owned device), introduces device readiness and compliance issues.

It is important to include self-service checks of agents' computers in the recruitment and hiring stages if BYOD/AOD is to be utilized. Agents also need to be provided with the tools and knowledge to fix issues they may run into. In addition, a key facet of managing the onboarding of large numbers of devices is a highly effective validation tool that checks the devices prior to centralized software distribution.

Such a validation tool is offered free as part of ThinScale's SRW (Secure Remote Worker) software, the only fully secure BYOD/AOD solution available on the market today.

It is critically important that automated device validation take place prior to hiring. This ensures a smooth onboarding process with work at home employees effectively moving directly from hiring to work.

Maintenance and Operation

Ongoing maintenance of infrastructure, software, endpoints and so on can be a challenge when agents are distributed.

All business applications remain centralized whether with a cloud provider, VDI or on premise. The same backend infrastructure is required regardless of where people are sitting. The challenges remain the same as with a physical contact center.

Centralized software is as easy to maintain for at home agents as those in physical contact centers. It is important to consider how to keep home workers' software updated, however. This will require the devices to be kept on the company domain or the utilization of management software solution that can deploy the updates.

Endpoints are where the challenges really start to mount up. Where the employer provides the device, work at home at any real scale can pose massive difficulties with the tipping point being at between 100 and 200 devices in most cases. This is the point where the company effectively becomes a hardware distributor as well as a BPO. ThinScale is aware of at least one case where a BPO had to acquire its hardware supplier in order to manage its work at home device estate.

Getting devices back from agents when they leave is another vitally important consideration. Even when companies pay post and packaging in advance, they frequently do not receive them back from a departing employee.

Device damage is also common when with the agent or en route to the agent. Finally, when using corporate devices, agent downtime may occur when computers need to be returned to IT for problem resolution and maintenance. In most jurisdictions, companies are required to continue paying staff during these periods.

Supporting Agents

For IT, it is important to consider how hundreds if not thousands of agents are supported when they are distributed remotely. Interestingly, front line engineers and helpdesk employees suggest treating everyone largely the same – once you have the desktop, apps and resources available alongside a centralized management and deployment solution the physical location of the agent is irrelevant. Standardization also reduces cost.

This is corroborated by industry leaders like Amy Freshman and Amy Anger who say this approach fosters employee equality, inclusion and diversity.

Some IT support issues encountered will be due to a lack of environment standardization – people working on different networks, devices, etc. This can actually lead to less downtime due to risk diversification. If a device stops working, it's likely to be an individual case. The same will apply to network, security and other issues.

Technological diversity does introduce its own issues though. A common problem is poor quality audio due to either bad headsets, softphone quality or high bandwidth demand within the agent's home. It is essential that support teams be equipped with the tools to address these new challenges as they arise.

WORK AT HOME

Key Considerations

1. Technology

a. Endpoint Options

When implementing work at home, a BPO has two main options in terms of an overall technology/endpoint solution. The first is to provide the work at home agent with some kind of company owned hardware while the other is for the agent to use their own device (BYOD/AOD).

Up until now, the latter option has been rejected by many BPOs as unworkable for a variety of reasons. However, under closer analysis it becomes clear that BYOD/AOD is actually the only sustainable solution from security, support and cost perspectives, especially at scale. Below we describe the three options in more detail.

✓ Company Owned Hardware

Companies tend to employ a mix of virtual, cloud and local applications depending on the use case. Backend technology (VDI, DaaS, etc.), endpoints, headsets, and so on have to be included. The options run from adopting a fully DIY approach using the organization's own servers, VDI, hardware, software, and so on all the way to a fully managed and compliant solution such as that offered by Dizzion.

Up until now there have been three main options available to BPOs for providing agents with hardware.

These are:
- a laptop,
- a thin client while they use their own monitor, keyboard, etc
- a USB stick with a Linux bootable OS loaded onto it

Each of these options have their own pros and cons. Laptops work but are very expensive. When costs of device damage, losses, logistics, and so on are taken into account, running costs can reach more than $1,000 per agent in capital spending and over $350 annually in ongoing operational spending.

A thin client is quite a neat approach and offers similar results to a laptop. It is cheaper from a capital expenditure point of view but tends to be more expensive in support bills. And the support issues get magnified at scale.

The USB solution is the cheapest of the three options. The company can choose to purchase and ship them to the agent or reimburse the employee when they buy them. Failure rates are problematic, however.

Dual booting a Linux OS and connecting to a backend infrastructure is not a simple operation and agents who lack Linux knowledge can quickly run into difficulties. Other problems include driver compatibility and video/audio performance issues. As with thin clients, supporting this solution at scale presents major challenges.

> “With one of my larger work at home clients we were losing hundreds of thousands of dollars sending out hardware. We were sending $1,000 machines to employees and they weren’t getting returned. BYOD is the only way to make largescale work at home effective”
>
> *Doug Berry, Former Sr. Director, Global Work at Home, Sutherland Global and Concentrix*

✓ Unsecure BYOD/AOD

BYOD/AOD, where an employee uses their own personal device, addresses most of the challenges presented by company-owned hardware but only if implemented properly. For example, some companies have opted for an unsecure BYOD/AOD solution, but this creates as many problems as it solves.

Its main failing is the fact that it is almost entirely reliant on HR for security and other key aspects. Employees are asked to ensure they have their computers updated, anti-virus running and so on. Generally, the support team requires agents to send screenshots of their security center during set up and holds regular calls to ensure the agents are meeting their obligations.

This approach is fraught with danger. There is absolutely no guarantee that the agents will keep systems and software updated and finding out that they haven't during a meeting will frequently be too late as security breaches may well already have occurred.

Unsecure BYOD/AOD can, of course, work for tasks like social media monitoring and posting but is unsuitable for anything involving sensitive data, taking phone calls or carrying out knowledge work due to the data risk. GDPR in Europe and PCI and HIPAA in the US render it untenable in many cases.

Some companies still take this approach despite the high risks. But a single data breach can cost up to $4 million under current regulation and instances have increased by 50% in the last four years. This is too great a risk to take.

✓ Secure BYOD/AOD using Secure Remote Worker

The only sustainable solution for more sophisticated work including support calls and dealing with sensitive information is secure BYOD/AOD using ThinScale's Secure Remote Worker (SRW) product. ThinScale developed SRW to address the absence of a secure BYOD/AOD solution on the market.

SRW is a simple Windows application that creates a secure workspace on a Windows personal computer without being intrusive – a critically important feature.

> “Secure Remote Worker has revolutionized security for our BYOD model, enabling us to leverage an agent's home PC securely.”
>
> *Marlon Beltz, Director of Work at Home, Telepeformance*

Onboarding of personal devices is reduced to a less than 10-minute process due to a mix of self-service tools for agents to update Windows and so on as well as built in deployment automation.

The application looks like any other on a desktop. Agents launch it, get logged out and logged back into the secure mode. SRW automatically carries out security checks in the background to verify Windows is updated, the correct firewall is applied, anti-virus is reporting good health, mass storage USB devices are blocked, and can even stop the execution of any services or applications chosen by the employer. Step by step guides are provided to self-fix any failures.

To all intents and purposes, the agent is not using their own device when they are working. Logging into the Secure Remote Worker application takes them to a secure, cloud-based environment controlled by the IT Department. All data, sensitive and otherwise, resides in that environment and never migrates to the agent's computer. In essence, the software rather than the device becomes the endpoint.

The solution offers a range of security, compliance, onboarding and other benefits as our customers attest:

> “The daily grind of having to patch, having to evaluate, and having to talk to auditors was removed. Other vendors’ solutions do not check for compliance, they just give you a desktop or an application.”
>
> *Principal Architect Systems, PCI, the world’s largest work-at-home BPO*

b. Patching and software updates / Device Management

All work at home solutions must have management systems in place to ensure the software deployed to agents and the device OS are updated. Most hardware will come with a solution to deal with that issue. In order to assist with support and compliance the solution should include central event reporting, central auditing and logging and remote control if possible. Secure Remote Worker includes all of those features including real-time reporting to ensure the agent’s computer, OS and security software are kept up to date at all times.

c. Network Bandwidth and Device Readiness

This should be handled during the hiring phase in order to allow for scalability. Agents’ machines and internet service quality and reliability must be tested at this stage in order to avoid costly delays during the onboarding phase. Device readiness testing can be very time-consuming unless an automated self-service model is used.

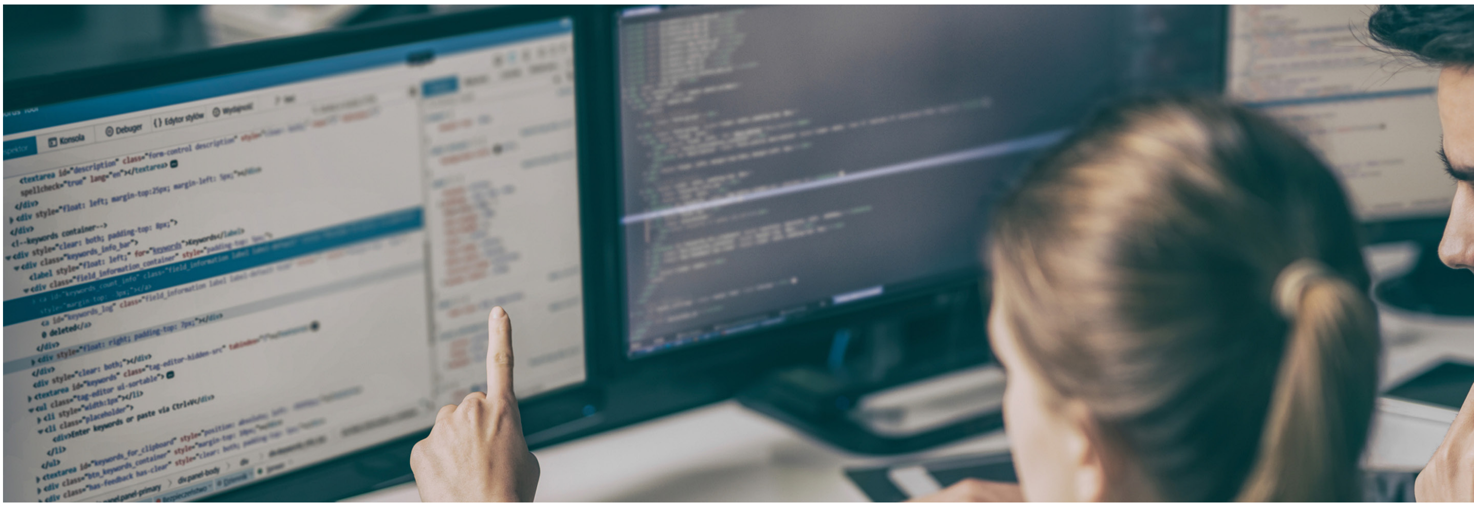
This support challenge is a is a key barrier to the success of work at home programs, so it is critically important to get it right. If it takes four hours to get each agent up and running a work at home program becomes unfeasible. Organizations should aim for a set-up time of less than ten minutes per agent. Any automated device readiness solution should meet that standard.

Equally importantly, the validation tool should offer simple self-service solutions to potential agents where problems are detected. This will not only ensure that good candidates are not screened out due to a simple hardware or OS issue but also offer ongoing support once the agent is hired thereby reducing the support burden in the longer term.

d. Software

The key choice is whether to use VDI, DaaS, web based, local software or a mix. A mix is recommended. The use of local apps for softphones is a good example. Some others will require a VDI while web-based apps are the end game.

Applications need to be evaluated to establish if they should be local, virtual or cloud based. This varies from company to company. For example, a lot of BPOs deliver softphones locally in order to ensure high quality calls. This sits alongside their VDI client software and VPNs.



2. End User Experience

End user experience is extremely important. Simplicity is key. When deploying a solution, it's essential to make it as close as possible to what agents are used to. Set up steps should be kept to a minimum; instructions should be simple; and maximum use should be made of video training.

Plugging in a USB key and booting up Linux to run a specific piece of software is far from being a simple task for the majority of agents. Clicking on a desktop icon and entering log in details replicates the experience with other Windows applications and greatly simplifies the process.

3. Security and Compliance

Remaining secure and compliant is more important than ever with cybersecurity breaches having increased by over 50% in the last four years. The average cost of a data breach according to Security Intelligence, the analysis and insights website, is $3.92 million (Security Intelligence, 2019) while PCI compliance breaches can result in fines of up to $500,000.

Security and compliance solutions involve a mix of people, process and technology. Only a combination of all three can ensure the security and compliance of an environment. In addition, the two core areas to evaluate and secure in work at home deployments are backend infrastructure and the endpoint.

Compliance comes into play at the backend as well as the endpoint. The backend is widely covered with the key players such as Microsoft,

VMWare, Citrix, and Amazon providing excellent guides.

The endpoint can be trickier. Hardware-based endpoints offer the benefit of standardization and the fact that the devices can be tested before being sent to agents to ensure compliance. BYOD/AOD can be more difficult due to many different types of endpoints, OS, software, and so on.

This is where the nature of the implementation comes into play.

Deploying a software-based endpoint addresses the compliance issues while using Windows based software deals with the other complexities. Dizzion, the first PCI compliant DaaS provider, is a widely acknowledged expert in compliance. The company has produced 'Understanding PCI Compliant Desktops' which highlights the risks and provides a very good overview of what needs to be considered in order to ensure compliance. The document also includes a checklist of the specific controls an organization needs to consider putting in place[21]. Microsoft, VMWare, Citrix and AWS also offer guidance on meeting compliance standards.

These vendors largely focus on the backend infrastructure. From an endpoint perspective, ThinScale offers guidance on how to ensure endpoints are compliant and secure. Through our partnership with global cybersecurity firm Coalfire Systems, which works on compliance and security with all of the main vendors, we have developed in-depth expertise on ensuring endpoint compliance.

We have also created a number of documents and white papers covering this crucial area including PCI, HIPAA and GDPR compliance white papers highlighting the relevant endpoint compliance controls.
These documents focus mainly on BYOD solutions, but the same points

should be considered when deploying hardware-based solutions.

The people and process aspects of compliance initiatives are also important and will come up for discussion with auditors and security teams. Some things simply cannot be dealt with by technology. For example, should somebody wish to take a picture of a screen using a smartphone it is impossible to stop them through technology. This has to be dealt with through human resources. Amy Anger, Client Partner - On-Demand Work and Gig Economy Expert with Fulcrum Workforce Solutions, says the way to solve this is through self-certification and the creation of trust between employer and employee.

There can be a mistaken belief among employers that once they do not own the hardware, they are not responsible for the data stored on it. This is incorrect and HR-only solutions are not sufficient to deal with the issue. This is another area where the software-as-the-endpoint solution comes into its own as all data, sensitive or otherwise, is stored on servers or cloud storage controlled directly by the employer and never resides on the agent's computer.

4. Remote Communication and Collaboration

Feelings of isolation and disadvantage among remote workers can impair productivity. A HBR survey of 1,100 employees asked employees to 'describe a manager who is especially good at managing remote teams'.

From this they identified the following best practices: check in frequently and consistently, use face-to-face or voice-to-voice contact, demonstrate exemplary communication skills, make expectations explicit, be available, demonstrate familiarity and comfort with technology and prioritize relationships.
Technical innovations introduced in recent years have provided solutions to these challenges. Of key importance are those which address internal communications and chat, external communications and virtual training.

Microsoft Teams, Slack and similar solutions have been game changers for effective internal communication and chat. Many remote workers feel they do not have enough information to do their jobs, so it is important to work with human resources to ensure the correct solution is implemented. Regular video calls between agents and team leads are essential for building relationships, making remote employees feel secure in their environment, assisting with ongoing compliance.

From a technology perspective, external communication refers to conference calls and softphones. Among the most common solutions deployed for conference calls include Zoom, Webex, and Teams. Standalone softphones are mainly from RingCentral, 8x8, Cisco, and Avaya. Some contact centre platforms including InContact, Talkdesk, Genesys and Five9 include this in their offering.

The most advanced and successful work at home employers create regular opportunities for people to chat and communicate online both through portals to facilitate informal communication and through more structured virtual meetings.

Best practice for such meetings is to ensure that no team member is at an advantage, perceived or otherwise, to another. Therefore, all team members, regardless of whether they are home or office based, will log in to the meeting in the same way. Such meetings have to be planned proactively by the host or team leader. One senior BPO executive even goes so far as to rearrange objects behind him for each meeting so that they can be used as props in the conversation. These objects can include recently won awards and so on.

The size of the team is also important. Office based teams can be quite large as the team leader has multiple opportunities to meet members and get to know them. This is not the case with work at home teams which should be limited in size to six or eight people in order to facilitate relationship building.

Communication does not stop with the office-based team leader or supervisor. The role of the IT department is to provide the necessary software to enable management, supervisors, trainers and support teams to work effectively with remote agents. It’s also essential that IT, HR and operations collaborate and communicate effectively and have service level agreements in place to ensure each department does its part.

5. Virtual Training

The approach to virtual training generally depends on current training practice. Where physical training rooms are used more than online methods it is recommended to continue this practice initially or move to a blended approach which limits the need to attend on site but doesn't change things too much. This will allow for an orderly transition to a virtual training model over time.

This may lead to higher costs during the initial deployment but a move to a virtual model is required in order to scale.

> "When implementing a work at home or flexible working program it's important to consider the following:
>
> **1.** When introducing new technology think of all users – on premise, home, travelling, etc.
> **2.** Technology MUST be reliable
> **3.** Ensure the IT helpdesk are specifically trained for these new types of workers"
>
> *Amy Freshman, Senior Director ~ Global HR Workplace Enablement ~ HR Strategy and Planning, ADP*

6. Recruitment and Onboarding

One of the biggest challenges for clients when implementing work at home is recruitment and onboarding.

The priority in recruitment is not so much finding candidates but maintaining candidate interest and managing onboarding times and controlling the IT support burden. Vicki Brackett, COO of work at home BPO Sinuosia and a consultant in contact center turnarounds with 25 years' experience, says it's common to see 14,000 candidates apply for positions with just 125 making it to day one.

The challenge is maintaining interest and controlling the burden being put on the recruitment, training and IT support teams. It is therefore important to automate at least some aspects of initial candidate identification and contact to ensure recruitment resources do not become overwhelmed.

With onboarding, the primary focus is managing onboarding times and ensuring simplicity. The introduction of any unnecessary complexity leads to difficulties due to agents being remote, inexperienced and not very technical.

> "A key focus area for us is to ensure all of our associates who work remotely get the equipment they need to get started right away on day 1. With proper SLAs in place and a partnership between HR and IT, we are able to deliver on the proper timing and allow for a positive associate experience beginning their first day."
>
> *Amy Freshman, Senior Director ~ Global HR Workplace Enablement ~ HR Strategy and Planning, ADP*

The key technical pieces to be concerned about are bandwidth and, depending on endpoint choice, device readiness, network compatibility and peripherals. The industry standard is to include bandwidth checks in the hiring process to ensure an applicant can't be hired if they do not have good enough bandwidth.

On the device front, as mentioned earlier, it depends on the endpoints chosen:

- Hardware endpoints including laptops, thin clients, and USBs, as mentioned earlier, present challenges at scale including cost, support, and technical difficulties for agents.
- Secure BYOD (Secure Remote Worker) eliminates the challenges associated with company owned hardware endpoints as the employee is using their own computer. It is also the lowest cost option with the employer not only saving on hardware costs but also on Windows licenses.

Everything is set up as needed as it's the agent's personal device. The challenge is device readiness. Devices are not standardized and for security reasons the employer needs to be sure Windows is updated, and Security Center is reporting good health, among other checks to ensure no malware is running, correct firewall rules are applied, agents aren't running in a virtual machine, keyloggers aren't running and that mass storage devices are plugged in and data can't be downloaded.

Device readiness checks, such as that offered as part of ThinScale's SRW solution, can be included in the hiring process in the same way as the bandwidth check. The solution comes with automated tools to turn this into a self-serve process carried out by the agent thus removing the burden from the employer while providing a report on which candidates passed and failed the test. Automating device readiness checks and including them in the hiring process allows the secure BYOD/AOD solution to be rolled out at scale.

7. Supporting Agents

For IT, it is important to consider how hundreds and thousands of agents can be supported when they are fully distributed, especially as technical issues are seen as one of the key challenges faced by work at home employees. Opinions differ when it comes to supporting remote agents, but a consensus holds that, where possible, all employees regardless of location should receive the same standards of support.

> “Create a baseline and then remove redundancy based on type – on premise, remote, travelling, and so on.
>
> *Amy A. Anger Client Partner - On-Demand Work and Gig Economy Expert, Fulcrum Workforce Solutions*

Those on the front lines go even further. Support engineers and helpdesk agents say the answer is to make location irrelevant. Whether agents are on site or at home, how they are supported should not change. Desk visits should be eliminated by implementing a central management and remote support solution. Support and communication should be standardized through the use of tools like Teams or Zoom. In other words, just because an employee is physically closer to the support engineer, the service they receive will not differ.

This parity of support only addresses simple and quite straightforward issues. Where hands-on attention from an engineer is required, work at home becomes very costly to support with devices having to be shipped to and from the agent’s home and the downtime that entails further ramping up the bill. Worse still, standardization can actually be detrimental in some instances as it increases the likelihood of problems being replicated across multiple agents.

This is the principal reason why variations in hardware, networks, locations, and so on can, somewhat surprisingly, lead to a simplification of support. According to the lead support engineer for a top 20 global

BPO, where an issue arises with an agent it's likely to be an individual problem. This minimizes the risk of hundreds of agents being affected by the same problem with support being overwhelmed as a consequence.

Software-based endpoints reduce IT support costs still further. The software is directly controlled, supported and maintained by the BPO with all support being carried out centrally. This allows the support team to create a virtual environment utilizing its own nomenclature for agents' devices and so on while the agents themselves experience no difference to their personal work environment.

The use of Windows PCs by work at home agents in a BYOD/AOD environment delivers a high level of hardware and OS standardization in any event and the majority of support issues should be capable of being dealt with on a self-service basis by the agent with online tools and tutorials made available to assist them. More difficult issues are dealt with by the agent with their own hardware vendor.

The BYOD/AOD solution does introduce some new challenges though. Getting audio to work with different hardware can be a challenge for the same reasons that non-laptop hardware endpoints cause support challenges. Missing drivers, third party software, and router issues are among the problems faced. One solution is to standardize headsets to ensure quality audio. SRW resolves this as its Windows based and compatible with most hardware available on the market today.

Overall, when organized correctly, work at home should not entail an increased burden on support. The nature of that support will change, however, and new issues will arise while others are eliminated.

Summary and Conclusions:

The benefits of work at home for BPOs are compelling – increased productivity, improved employee satisfaction, significantly enhanced recruitment and retention metrics, and considerable savings on real estate and other overheads. The only real question up until now for the majority of larger BPOs has been how to realize those benefits at any scale.

The Benefits:

- Productivity increases of up to 55%
- Annual real estate savings per employee of up to $11,000
- Overall cost reductions per employee of up to 40%
- Employee savings on annual commuting and other costs of up to $7,000
- Reduced staff turnover of up to 50%
- Access to a wider labor pool in rural areas and among those who normally find it difficult to access paid employment including military spouses and people with disabilities

The Challenges:

BPOs implementing work at home programs face a variety of technical challenges which must be resolved before the benefits can be realized. These issues range from hardware costs through security and compliance to difficulties providing support to many hundreds of remote agents who are potentially using a diverse range of devices and operating systems.

Security

Security is absolutely critical in the BPO world with compliance requirements ranging from PCI, HIPAA, GDPR and numerous financial regulations. Work at home requires policies to be put in place for a whole range of eventualities not normally considered in the workplace, particularly in relation to credit card and other sensitive data. Every point in a credit card transaction must be secure and comply with PCI and other regulations. Additional risks in the home environment include data leaking from employee devices, malware running on a computer, employees taking pictures of screens, and so on. Failure is not an option.

A single data breach can cost up to $4 million under current regulation and instances have increased by 50% in the last four years. This is too great a risk to take for any organization regardless of scale.

Recruitment and onboarding

Finding staff with the skillsets and the broadband service required for an agent's role can present difficulties, as can finding those with suitable hardware to work in a BYOD/AOD environment. Where large number of agents are required the time taken to validate broadband and hardware must be reduced to less than 10 minutes and this can only be achieved through an automated self-serve process.

Maintenance, operation and support

Ongoing maintenance of infrastructure, software, endpoints and so on can be a challenge when agents are distributed. Managing, maintaining and supporting a widely distributed estate of company owned hardware becomes virtually impossible when the number of agents rises to above 100 or so.

The Solution

The solution that addresses these challenges whilst simultaneously maximizing the benefits is secure BYOD/AOD. This avoids the costs associated with providing hardware to agents, greatly reduces and simplifies the level of support required, and deals with the security issue by retaining all data on servers or cloud storage directly owned controlled by the company.

ThinScale's Secure Remote Worker (SRW) product offers all these features and more. It is a simple Windows application that creates a secure workspace on a Windows personal computer. Onboarding of personal devices is reduced to a less than 10-minute process due to a mix of self-service tools for agents to update Windows and so on as well as built in deployment automation.

Agents launch SRW, get logged out and logged back into the secure mode. The application automatically carries out security checks in the background and can even stop the execution of any services or applications chosen by the employer.

In essence, the agent no longer uses their own device when they are working; SRW takes them to a secure, cloud-based environment controlled by the employer. All data, sensitive and otherwise, resides in that environment and never resides on the agent's computer. The software therefore becomes the endpoint thereby delivering complete security and peace of mind.

Conclusion

Work at home at scale is a genuine option for BPOs for the first time thanks to Secure Remote Worker from ThinScale. It brings the productivity improvements, cost savings, and recruitment and retention gains within reach with almost none of the resource and logistical challenges associated with traditional solutions. This will have far reaching implications not only for the BPO sector but for the environment as well as a result of the transport and real estate savings achieved.

Bibliography

1. https://cdn.thepennyhoarder.com/wp-content/uploads/2017/06/30140000/State_Of_Telecommuting_U.S._Employee_Workforce.pdf, Flexjobs, 2017
2. Scott Mautz, 'A 2-year Standford Study Shows the Astonishing Productivity Boost of Working From Home', in INC. (2018), https://www.inc.com/scott-mautz/a-2-year-stanford-study-shows-astonishing-productivity-boost-of-working-from-home.html
3. Global Workplace Analytics, 'Telecommuting Trend Data', (2019), https://globalworkplaceanalytics.com/telecommuting-statistics
4. 4 Global Workplace Analytics, 2019
5. Contact Babel, 'The UK Contact Center Decision-Maker's Guide 2016', 14th edn, (2016), http://www.contactbabel.com/pdfs/july16/The-2016-UK-Contact-Centre-Decision-Makers-Guide-Executive-Summary.pdf
6. Raja Simhan, 'Attrition is a major problem for all BPOs'', (2018), https://www.thehindubusinessline.com/info-tech/attrition-is-a-major-problem-for-all-bpos/article9026856.ece#
7. David G. Allen, 'Retaining Talent: A Guide to Analyzing and Managing Employee Turnover', in SHRM, https://www.shrm.org/hr-today/trends-and-forecasting/special-reports-and-expert-views/Documents/Retaining-Talent.pdf
8. Scott Mautz, 2018
9. Global Workplace Analytics, 2019
10. Everest, 2019
11. Global Workplace Analytics, 'Advantages of Agile Work Strategies For Companies', (2019), https://globalworkplaceanalytics.com/resources/costs-benefits
12. Berkeley, 'Case Study: Telecommuting', (n.d.), https://inst.eecs.berkeley.edu/~eecsba1/sp97/reports/eecsba1d/report/telecommute.html
13. Carmen Nobel, 'Working From Home Cuts Costs, Helps Planet', (2010), https://www.thestreet.com/investing/working-from-home-cuts-costs-helps-planet-10766582
14. Jeff Rimburg, 'The Metrics of Contact Center Productivity', (2019), https://www.icmi.com/resources/2019/the-metrics-of-contact-center-productivity
15. Prithwiraj Choudhury, Barbara Z. Larson and Cirrus Foroughi, 'Is It Time to Let Employees Work from Anywhere?', (2019), https://hbr.org/2019/08/is-it-time-to-let-employees-work-from-anywhere
16. Global Workplace Analytics, 'Measuring Results', (2019), https://globalworkplaceanalytics.com/measuring-results
17. Wharton University of Pennsylvania, 2018
18. Global Workplace Analytics, 2019

19. Risk Based Security, ‘Cyber Risk Analytics, 2019 MidYear QuickView Data Breach Report’, 2019, https://pages.riskbasedsecurity.com/hubfs/Reports/2019/2019%20MidYear%20Data%20Breach%20QuickView%20Report.pdf?utm_campaign=Data%20Breach%20QuickView%20Reportandutm_source=hs_automationandutm_medium=emailandutm_content=75543609and_hsenc=p2ANqtz--D7t-IllS7wLtmQ2mG-dNyT4HGnAN_9DfSQBKSB5dYwsmRUmjuGN13pj_GcxYZzwc0zXsdPwMq0_QKvxyHz61E2BGP3Aand_hsmi=75543609
20. https://www.ibm.com/security/data-breach?p1=Search&p4=p50370570822&p5=b&cm_mmc=Search_Google-_-1S_1S-_-WW_NA-_-%2Bcost%20of%20a%20%2Bsecurity%20%2Bbreach_b&cm_mmca7=71700000061027912&cm_mmca8=aud-382859943522:kwd-417449383088&cm_mmca9=Cj0KCQiAsbrxBRDpARIsAAnnz_Nu2nu6nyjs7uvf3Sm8CuIh-OCFHw2BcvMxMiFT5LwC_7OgHFb9JykaAkkIEALw_wcB&cm_mmca10=405839889732&cm_mmca11=b&gclid=Cj0KCQiAsbrxBRDpARIsAAnnz_Nu2nu6nyjs7uvf3Sm8CuIh-OCFHw2BcvMxMiFT5LwC_7OgHFb9JykaAkkIEALw_wcB&gclsrc=aw.ds
21. Dizzion, ‘Understanding PCI Compliant Desktops’, 2019, https://www.dizzion.com/wp-content/uploads/2017/09/Understanding-PCI-Compliant-Desktops.pdf
22. Joseph Grenny and David Maxfield, ‘A Study of 1100 Employees Found That Remote Workers Feel Shunned and Left Out’, 2017, https://hbr.org/2017/11/a-study-of-1100-employees-found-that-remote-workers-feel-shunned-and-left-out
23. Joseph Grenny and David Maxfield, 2017
24. Redefining Communications, ‘Remotely Interested? What remote workers really want from internal communication teams’, 2019, https://remotelyinterested.work/RemotelyInterested_digitalreport.pdf

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

+353 1906 9250
hello@thinscale.com