WHITEPAPER

Working from home, now and in the long-term.

Perhaps both can be achieved at the same time–a fast implementation fit for the long term.

As more and more employees work from home due to the current pandemic, IT professionals have several challenges to face. Do they roll out a "quick and dirty" solution to satisfy the immediate need? Should they consider the long term, understanding that the use of home offices has become a de facto standard, and a professional solution is required?

No two companies have the same needs in this area. This paper will focus on small and medium-sized businesses (SMBs), where three likely scenarios exist in their IT structures.

1. **PCs & Servers:** The company works within a traditional environment where most applications run locally on PCs or laptops, and some SaaS applications are accessible via a web browser. Data is available locally and on servers.
2. **Terminal services:** The company has moved most or all applications to the server backend and access them with PCs, typically via Microsoft RDS. A mix of locally run applications and Terminal services is possible so long as the end-users are on Windows PCs.
3. **Virtual Desktop Infrastructure (VDI):** The company has moved entirely to a Desktop virtualisation solution such as the platforms offered by Citrix, VMware, or Microsoft. All applications are running in the datacenter or are accessible as SaaS.

Desktop virtualisation (#3 above) remains the best-case scenario for home office use as it offers security, central management, data consistency, and a backup strategy. However, these VDI solutions can be cost-prohibitive and to complex for many SMBs. For companies utilizing legacy scenarios such as 1 or 2 with local PCs, staying with them opens the door to security risks, data corruption, and inconsistencies. Some SMBs have moved to a thin client solution. Here a terminal device works by connecting remotely to a server-based computing environment. Most applications and all sensitive data are stored on the server(s) to deliver secure work from home environments.

For SMBs that still use scenarios 1 or 2, the easiest way to virtualise applications is likely a move to a Terminal Service solution like Microsoft RDS. These services are part of well known and understood Microsoft Servers with a straightforward learning curve for IT.

Depending on the workload and number of home office users, existing server hardware might be sufficient to handle the additional load. A more significant number of users will require investment in the server backend unless the company is willing to move quickly into a cloud-based infrastructure like Azure or AWS.

Moving into cloud services has the advantage of being quickly adopted and scalable for future needs. However, data protection and long-term system costs will outpace the CAPEX required for in-house server infrastructure.

Terminal services are a great way of virtualising applications or even desktops where users are using a similar set of applications. If users have different requirements and use various applications, a more robust desktop experience is required. A true VDI environment through the likes of Citrix or VMware would make more sense.

These companies offer very powerful VDI as well as app virtualisation solutions for large numbers of users (into the thousands) with enterprise-class management and remote access technologies. Unless these are already in place, they do take time to deploy with a much longer learning curve.

Once a decision has been made to virtualise the environment, finding a secure way of connecting home offices to the data centers becomes the priority.

Several questions should arise:

1. Is central management of the devices used at home desirable?
2. How knowledgeable are the home users at setting up VPNs and devices?
3. Is a mix of personal and office use, and therefore a combination of private and company data allowed?
4. What kind of credential management already exists, and what is desirable?
5. How important is the use of multimedia through the corporate network?

For most companies, question number 3 will be a definite 'no', meaning additional hardware in the form of a dedicated work PC, laptop, or thin client is necessary. Though laptops might be considered the logical choice, don't overlook their disadvantages. First of all, they are full PCs requiring IT personal attention. They are prone to malware attacks and have more computing power than is necessary for a virtualised environment. Also, their form-factor makes them challenging to use for extended periods unless augmented with a larger screen, external keyboard, and mouse, making this a rather expensive proposition.

Using thin clients instead has several advantages, including minimum interaction for IT personnel, significantly less susceptibility to malware attacks, and a guaranteed separation of personal and company-owned data and applications. Thin clients come in many different forms, but there are only two relevant architectures:

1. **x86:** Based on the PC x86 architecture, these thin clients carry the same cost structure as a full PC, sometimes being more expensive.
2. **ARM:** Based on platforms like the Raspberry Pi, these offer much lower hardware costs while providing similar performance and capabilities. They have a small form factor and are easier to incorporate into a home or remote work location. In some cases, ARM-based clients may not have specific device drivers to support all possible peripherals properly. However, this is unusual in a home office environment.

Thin clients deploy pre-configured by your IT team, requiring no on-site set-up and management knowledge by the end-user above plugging it in. If chosen right, they can be managed and supported remotely as well.

Connection of clients to the in-house or cloud data center can be securely done via built-in VPN clients or using the gateways provided by all major vendors like Citrix, VMware, and Microsoft.

In summary, a relatively quick, easy way of deploying SMB home office workspaces built for the future is:

- Move all relevant applications to application virtualisation solutions like Microsoft RDS, either locally or cloud-based.
- Set up client management software as a virtual application to allow remote management.
- Choose credential management (e.g., yubikey).
- Choose the best value thin client that allows for a simple roll-out.

If done correctly, the result is a safe, easy-to-use, standardized home office solution that opens the door to a more flexible, scalable, and future proof IT infrastructure.

About the author:

Jochen Polster is an industry veteran having spent more than 25 years in system and semiconductor sales and marketing in Europe, the US, and Asia. At *NComputing*, he serves as the Vice President for Sales and Marketing in Europe

About NComputing:

NComputing is a leading desktop virtualisation solution provider serving more than 70,000 companies across 140 countries. *NComputing* specializes in providing affordable, easy-to-deploy, centrally managed, and high-performing Raspberry Pi-based thin client computing solutions. The RX-RDP thin client is a cloud-ready thin client designed and optimized specifically for Microsoft RDS, powered by Raspberry Pi3. The RX-RDP provides a rich PC-like experience in an affordable, energy-saving device with a small footprint. The new RX420(RDP) thin client brings premium performance and native dual display, powered by the latest Raspberry Pi4. Both thin client solutions deliver full-screen, full-motion HD multimedia playback with support for Microsoft RemoteFX and *NComputing* vCAST Streaming, WiFi connectivity, and built-in transparent USB redirection achieving unparalleled peripheral support.