Sage Nonprofit Solutions

Demystifying Remote Access:

Terms and tips for evaluating your options

By Grant Howe

Contents

Introduction

Making mission critical business applications (software solutions) available remotely is a hot topic these days. Remote access allows staff to work from any location without being tied to a specific physical location. With the amount of consolidation, decentralization of offices, and home or travel-based positions, being able to offer solid remote access technology to your employees is critical for your success.

Figuring out what to do, or even where to start, can be a significant quandary. Not only must you take into account the architecture of the application you want to access remotely, but you must also consider bandwidth limitations (on both sides of the solution), your data security and compliance needs, and your IT management and administration strategy.

This executive brief will introduce you to the terminology and concepts of remote access and provide a platform for you to begin your evaluation. First, we will look at different remote technology options and the various software architectures for which they are appropriate. Then, we'll give you tips on how to best evaluate your current internal resources and potential vendor partners to create the best solution for your needs.

Types of Applications

In order to create the appropriate remote access scenario, it's important to understand the architecture of the application that you want to access remotely. This is the first step, as some technology choices may not be feasible, based on the application architecture. If you don't know which of these architectures you are using, simply contact your IT professional, business partner, or vendor for guidance.

Standalone (Client/Database)

The client/database architecture is when a larger, dedicated application is installed on each user's desktop. This is sometimes called a "fat client." It connects directly to a database, which may be either on the same machine as the client or over the network. This solution is usually used when only a small number of users need access to the application.

Client/Server

The Client/Server architecture is similar to the Client/Database model. It also consists of a larger footprint[1] application installed on each user's desktop, but this "fat client" connects to a version of the software installed on the server. The server application then applies business logic before interacting directly with the database. An example of an application set up in this fashion is an e-mail client, such as Microsoft Outlook®. The client software must be installed on the workstation and must be configured to connect to a server to get data.

Web-based

A Web-based architecture uses a Web browser as the client and requires minimal software to be installed on the user's computer. This architecture doesn't require a large-footprint application to access the database as it uses a standard Web browser instead. The Web browser works with a Web server to deliver a browser-based user interface (UI) to the end user. The Web server may interact with other application servers to run business logic and return results to the user by way of the browser UI. The database is usually installed on a different server than the Web server. Web-based e-mail is perhaps the most ubiquitous example of Web-based computing today.

[1] The term "footprint" is often used to describe the memory and hard drive recommendations for the application.

Remote Technology Options

There are a number of technology options for gaining remote access to applications, each with various bandwidth requirements and security considerations. We will explore some of the more popular ones and discuss the pros and cons of each.

Tunnel in: Virtual Private Network (VPN)

A VPN is a secure tunnel between a remote user and your internal network. The user creates a session with your VPN server or firewall appliance and then is allowed to pass data directly into your network. It is just like the user is plugged into a wall jack at the office, except for one very important difference: the bandwidth that the user can use is limited by lesser of their and your available bandwidth to the Internet. In other words, the maximum size of the "pipe" is determined by whichever end passes the smallest amount of data.

Most offices have 100 megabit connectivity internally and significantly less out to the Internet (1.5 mb perhaps). Most homes have even less—even with a broadband connection. Your users' experience may be sluggish with your application or the connection may be too unstable for the application to maintain a connection to the server. This makes VPN a challenging option for solutions that use a large-footprint application installed on the local machine. However, VPN does work well for Web-based applications if additional security is desired, since having users log on through the firewall provides another layer of security protection for your Web server.

A Virtual Window: Remote Desktop Connection (RDC)

Remote desktop services allow you to host an application on a remote server and transfer what amounts to screen shots back to the client. Keyboard and mouse inputs are forwarded to the server and the results are shown on the subsequent screen shots that come back. Think of it like using your computer as virtual window into the server where the application is installed.

> *"[With RDC] the user can click on an icon in the start menu, start the application and use it like it was installed on the local machine, except that it is actually running on a remote server."*

This technology allows you to offer a traditionally locally installed software solution to users remotely without needing to boost their bandwidth for the application to communicate with the server effectively. The "screen shots" are compressed so the RDC uses a constant, but small amount of bandwidth.

Older versions of this technology presented an entire desktop for the user to use as essentially a remote workstation. The current 2008 server version of Microsoft's Terminal Services now allows for the publishing of applications only, if you so choose. The end result is that the user can click on an icon in the start menu, start the application and use it like it was installed on the local machine, except that it is actually running on a remote server.

Citrix XenApp is Citrix's version of Terminal Services and allows publishing of applications the same way. XenApp may allow for nicer administration of the applications and a better user experience and depending on your configuration, it may also offer you the ability to work with mobile devices. However, licensing and implementation costs are typically higher than with Terminal Server. Either solution (and RDC in general) is a good choice for remote access of applications that utilize a large-footprint user interface.

Application hosting

RDC can be managed internally by your own IT staff, but many small- to mid-sized organizations choose to partner with specialized technology and hosting providers. While level of service varies with cost, hosting relieves considerable and possibly all IT burden from your staff. For example, an Application Service Provider (ASP) takes an application, puts it into a hosting infrastructure, and sells the use of the software directly to customers. The application is typically one built to be installed directly on a client machines, but the ASP uses Terminal Services, Citrix XenApp or another technology to take the administrative burden off of the end consumer. Later, we'll discuss how to evaluate the right partner for your needs.

Web-based applications

A Web-based application does not need RDC to be set up on a client machine. Data passes over the Internet as encrypted Web traffic. Often, it is specifically built as a SaaS (Software-as-a-Service) offering and requires no IT department interaction to sign up for it and begin using right away. Normally only the software vendor can offer SaaS to customers.

Security Considerations and Compliance

No evaluation like this would be complete without a discussion of security and compliance. There would be no quicker way to draw a halt to your campaign, traumatize your constituents, and give your organization a black eye than to have a security breech resulting in a loss of personal information. If your organization has neither the knowledge nor the skill set to build and execute a solid security plan, then seek outside help from a professional.

General Security Best Practices

Security best practices involve the use of a properly configured firewall, anti-virus protection, automated patching of operating systems, and security policies and procedures. Other areas to consider are intrusion detection and prevention measures, vulnerability assessment, and employee security training. The scope of these methods is too large to be included in this brief, but there is ample information about these practices on the Web. Look for the term “defense in depth” in your research.

Another best practice is to set up servers that perform only one service and lock down or “harden” them against breaches. For example, a Web server can be hardened and allowed only to serve Web pages, and a database can be hardened to only perform database functions. When you mix a Web server and a database server together on one box, a hacker has the opportunity to breach your database server by hacking through the Web server’s vulnerabilities.

“If your organization has neither the knowledge nor the skill set to build and execute a solid security plan, then seek outside help from a professional.”

Sarbanes-Oxley

Few compliance regulations have gotten the attention that SOX, or SarBox, has received in the industry. A congressional regulation passed in 2002 as a result of the massive collapse of Enron, the bill requires that subjected companies place auditable controls on key points in their process that might affect the accuracy of their financial reporting. It also provides a key deterrent for executives who knowingly provide data that is negligently false or inaccurate: jail time.

Currently SOX is required only for public companies. Even though it does not apply to nonprofit organizations at the moment, it is important to note, since many nonprofit organizations are preemptively adopting some of the practices and new regulations may be passed in future years for the sector.

Read the Sarbanes-Oxley act.

PCI Compliance

PCI compliance refers to the Payment Card Industry Data Security Standard published in 2004. Organizations that accept and/or store credit card data are required, by their processors, to be PCI compliant. To be compliant you must patch your systems regularly, conduct vulnerability scans, and perform an official audit at least annually.

More information on PCI.

HIPAA Compliance

The Health Insurance Portability and Accountability Act was enacted in 1996. There are many sections in the act, but the two most important to this discussion are the “Privacy Rule” and “Security Rule” added in 2003.

The “Privacy Rule” states that individuals have a right to access their “personal health information,” a right to have that information kept confidential, and the right to request an audit of its use.

The “Security Rule” complements the privacy rule as it lays out standards for control and administration of individuals “personal health information.” Safeguards are identified in the areas of Administration, Physical and Technical. You must put policies and procedures in place and audit their use to be in compliance.

More information on HIPAA.

SAS 70 (Type I and II)

Statement on Auditing Standards #70 is an auditing standard issued by the American Institute of Certified Public Accountants. SAS 70 standards are usually applied to external service providers to ensure that their operational policies, procedures and controls protect the controls and integrity of the services they host.

Type I SAS 70 compliance is an auditor’s assessment of the effectiveness of the design of the operational policies, procedures, and controls that the entity has put in place. Type II includes the same evaluation as Type I and adds an audit of whether the policies, procedures, and controls were in use at the time of the audit and whether they were effective.

More information on SAS 70.

> *“Be sure that your security professional is certified by a recognized entity.”*

Personnel and Skill Set Requirements

Regardless, if you are providing remote access from your internal systems or looking at a third-party partner, there are some definite skill sets necessary in any of the technology choices. Carefully assess if these skill sets available from your staff or an outside partner. If not, seek to close the gap.

Networking and Security

Firewalls, anti-virus, intrusion prevention, compliance controls, and policies and procedures need to be configured properly, maintained and, if appropriate, rolled out to users. An improperly configured firewall is a leading cause of security breaches from external attackers.

Generally these are specialized skills not found with sufficient aptitude in an IT generalist. If you plan to manage your remote access solution internally, it is strongly recommended that you seek the services of a professional security analyst. There are organizations that offer certification for analysts—be sure that your security professional is certified by a recognized entity.

Operating Systems and Administration

Most remote application offerings are based on the Microsoft Operating system. Besides needing the skill set to install and configure servers, someone must be tasked with applying security patches issued by Microsoft on a monthly basis. Failure to apply important security patches to servers is another leading cause of security breaches.

Administration of Services and Access

Besides knowledge of the operating system, you must have expertise in the installation, configuration and maintenance of the chosen remote application hosting technology. This knowledge is not the same as knowledge of the operating system, therefore the need for an additional specialized skill set, or finding the rare person who has both, is critical.

Application-specific Administration

Additionally, expertise in installing, configuring, and maintaining the application you are making available for remote access is necessary. Make sure to check with the software vendor and ask with which technologies the application has been successfully accessed remotely, and if the vendor supports that configuration. If the vendor says it works but doesn't support it, this should be a big red flag for you. Maintenance headaches are almost a guarantee.

Evaluating Remote Application Access Options

Do It Yourself or Partner?

Many organizations have been successful in offering remote access to internal applications with internal resources. If you already have a solid IT department with the skill sets outlined earlier and have an application whose vendor supports some sort of remote-access technology, you may be in business. However, you still need to consider the significant effort and the opportunity costs of other projects on which your IT staff could focus. Or, you may be considering ways to reduce your IT expenses, since outsourcing such projects is often more cost effective.

Vendor Selection

With every business relationship, you are looking for not just a vendor, but some sort of partnership. This is even more imperative when you need to depend on them for the continuity of your business operations. Before making your initial contact of inquiry, gather the following information to help narrow down your options:

- Length of time in business (avoid new entrants to the market regardless of cost)
- Proper accreditation (look for SAS 70 type I and PCI at a minimum)
- Customer support reputation (look for a vendor who strives to make you successful)
- Avoid lowest bidder or low cost providers (you will usually get what you pay for)
- Avoid vendors on the cutting edge of technology (success in IT is not gained from taking high risk with new technology)
- Look for staff with architect level titles and certifications on technology (MCSE, Cisco, SAIC)
- Look for a company that first strives to understand your needs rather than prescribes a solution that they want to sell you.

Partnering Options: Co-Location, Hosting, and Managed Services

It's important to understand what you are being offered versus what you really need. Each of the following options increases in price and also in value.

Co-location means that you purchase servers and equipment co-located in a secured datacenter. The vendor provides network access, power, and sometimes firewall configuration. You are responsible for managing the servers, software, and so forth, on those boxes. Co-location is for companies that have an established and experienced IT staff, but do not have a secure datacenter, reliable power, or enough internet bandwidth to host internally.

Hosting means that your vendor rents you all of the equipment, power, and bandwidth for a monthly or yearly fee. You do not own the hardware your applications run on. The vendor also provides the operating systems and manages them for you. Generally the vendor is responsible for keeping your servers up and running and adhering to a service level agreement. The vendor generally does not support any software that sits on top of your operating system. Examples of software that vendors do not directly support are database, Web server, remote access, Active Directory, Exchange, and third-party software (such as accounting or fundraising software). Hosting is a good opportunity to take a load off your IT staff and possibly reduce costs.

Managed services providers take hosting to the next level. They do everything a hosting provider would do, plus manage common software like the ones named above. They generally would not manage the business application for which you are setting remote access, but they manage everything else including the remote-access technology itself (such as Terminal Services). Managed services is an ideal choice for those who have few or inexperienced IT staff or are looking to reduce IT costs. However, even with managed services some IT staffing is required to run your application.

Application Service Providers (ASP)

ASPs pick up where managed service providers leave off. An ASP offers you remote access to popular applications along with hundreds of other customers. They generally charge you a monthly fee for access and possibly a licensing fee. Typically they use established applications and fit them into a remote-access technology infrastructure and are seldom the developer of the applications to which they are providing access.

The ASP model generally eliminates all need to have IT staffing for the particular application you wish to use, making it an extremely attractive option for those with little or no IT staff. The drawback is that you have to find an ASP that offers the application you want. For niche software this could be an issue.

One possible drawback is the ASP owns your data. Since it's a commercially available application, you could get your data from the ASP and move to another hosting model at a later time.

Software as a Service (SaaS)

"The ASP model generally eliminates all need to have IT staffing for the particular application you wish to use, making it an extremely attractive option for those with little or no IT staff."

Software as a service further picks up where ASPs leave off. SaaS is generally offered to customers by the software developer. The application is specifically tailored and built for SaaS use. SaaS applications are almost always Web browser based and have subscription pricing for access but no license fee since you don't own the software. Generally, the user is not required to install any additional software to sign up, pay, and begin using a SaaS product.

SaaS products constantly evolve and often add new features on a quarterly basis. Since the software is written specifically for a SaaS model, the developer can listen carefully to its customers and tune the software frequently and quickly to meet their collective needs.

Like the ASP model, the SaaS model eliminates the need to have IT staff allocated to this application.

The most significant drawback of SaaS is that the vendor owns your data exclusively and switching to another hosting model will have high switch costs. While you could get an export of your data, since the software you are using is only available in SaaS form, you can't buy it and run it yourself. You would have to transform the data and import it into another package.

It is widely believed in the industry that the trend is for most software to eventually end up as SaaS model.

Summary

There are lots of variables and choices in putting a successful remote application access strategy in place. The bottom line recommendation is that you really shouldn't try to go it alone in unless you already have very knowledgeable IT staff in house with available time to support the effort. If this is not the case, a good partner who is interested in your success is the best bet.

Reference

Read the Sarbanes-Oxley act

http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h3763enr.tst.pdf

More information on PCI

https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

More information on HIPAA

http://www.cms.hhs.gov/HIPAAGenInfo

More information on SAS 70

http://infotech.aicpa.org/Resources/Systems+Audit+and+Internal+Control/IT+Systems+Audit/Standards+and+Regulations/SAS+No.+70+Service+Organizations.htm

About Sage (North America)

Sage North America is part of The Sage Group plc, a leading global supplier of business management software and services. At Sage, we live and breathe business every day. We are passionate about helping our customers achieve their ambitions. Our range of business software and services is continually evolving as we innovate to answer our customers' needs. Our solutions support accounting, operations, customer relationship management, human resources, time tracking, merchant services, and the specialized needs of the construction, distribution, healthcare, manufacturing, nonprofit, and real estate industries. Sage North America employs more than 5,000 people and supports nearly 2.9 million small and medium size business customers. The Sage Group plc, formed in 1981, was floated on the London Stock Exchange in 1989 and now employs 14,800 people and supports 5.7 million customers worldwide. For more information on Sage Nonprofit Solutions, please visit the Web site at **www.sagenonprofit.com** or call **866-831-0615**.

Sage North America

12301 Research Blvd.
Building IV, Suite 350
Austin, TX 78759

866-831-0615
www.sagenonprofit.com