Sage Construction and Real Estate

Demystifying Remote Access

Terms and tips for evaluating your options

By Grant Howe

sage

Table of Contents

Introduction

Your construction or real estate company balances back-office functions—billing, paying invoices, running financial reports, payroll, planning logistics—with the physical presence needed on the job site or in a client's office. Having constant access to information from the back office, no matter where you are, can help inform supervisors out in the field and assist them as they manage construction projects in any location. Today's technological solutions must be able to serve users like you in both work settings.

As a result, making mission-critical business applications and software solutions available remotely is a growing trend in the construction industry. Remote access allows staff to work from almost anywhere, without being tied to a specific physical location. 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, 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. We will look at different remote technology options and the various software architectures for which they are appropriate. We'll also give you tips on how to best evaluate your current internal resources and potential vendor partners to create the best solution for your needs based on four key aspects:

- Architecture
- Bandwidth
- Security
- IT impact

Partnering options: colocation, hosting, and managed services

Before starting the discussion, it is important to understand what you are being offered versus what you really need. Equally important is to understand what is typically covered in each scenario, and what remains your responsibility. Each of the following options increases in price and also in value.

	Complexity	Cost Impact	Architecture	Bandwidth	Security	IT Impact
Colocation	High	Up front and ongoing	You own it	Covered	Managed	High
Hosting	Medium	Ongoing plus s/w	Covered	Covered	Covered	Medium
Managed Services	Low	Regular ongoing fees	Covered	Covered	Covered	Low

Colocation means that you purchase servers and equipment colocated in a secured data center. The vendor provides network access, power, and sometimes firewall configuration. You are responsible for managing the servers, software, and so forth, on those boxes. Colocation is for companies that have an established and experienced IT staff but do not have a secure data center, 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)

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.

Architecture

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 typically 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 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 email 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 email is perhaps the most ubiquitous example of web-based computing today.

Bandwidth

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 the 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 smaller 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 required, 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 resides.

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 midsized 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 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

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, antivirus 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.

Networking and security

Firewalls, antivirus, 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.

IT impact

Whether 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.

Operating systems and administration

Most remote application offerings use a 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.

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 the vendor 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 t aking 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 it wants to sell you.

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 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.

About Sage

Sage is a leading global supplier of business management software and services for small and midsized businesses. The Sage Group plc, formed in 1981, was floated on the London Stock Exchange in 1989 and now employs more than 13,500 people and supports more than 6 million customers worldwide. For more information about Sage in North America, please visit the company website at NA.Sage.com. Follow Sage North America on Facebook, Facebook.com/SageNorthAmerica, and Twitter, Twitter.com/SageNAmerica.

About Sage Construction Anywhere

Sage Construction Anywhere is a cloud-based collaborative solution that connects people, documents, and data securely together in one, easy-to use, online project hub—designed specifically for the construction industry. It is a subscription-based cloud service that combines both application and platform hosting services. It also includes a proprietary Connector that initiates and handles all communications between the cloud and the customer's back-office financial and operations software that are on-premises, providing security protection for company information. Sage Construction Anywhere is developed upon the industry-leading cloud services hosted platform Microsoft® Windows Azure. With Azure, customers are provided with the highest available levels of data integrity, availability, and confidentiality.

Built and distributed by Sage, Sage Construction Anywhere offers your business the only integrated, cloud solution on the market tailored specifically to accompany and evolve hand-in-hand with your Sage 300 Construction and Real Estate (formerly Sage Timberline Office) financial and operations software. It strengthens communication between the field and the office and integrates with your back-office operations to simplify job costing and payroll processes. Sage Construction Anywhere keeps projects moving forward by providing project teams access to common, accurate, and timely project information anytime, anywhere.

About the Author

Grant Howe, VP of research and development, has more than 17 years of technology industry expertise. Before joining Sage, he served as executive vice president of engineering and chief technology officer (CTO) for Houston-based CareFlash.com, a Web 2.0 company. He holds a master's degree in software engineering from Syracuse University in Syracuse, N.Y., and a bachelor's degree in computer science from the State University of New York (SUNY) College at Oswego. Grant is on Twitter as @geekbyte.

Sage

15195 NW Greenbrier Pkwy

Beaverton, OR 97006-5701

800-628-6583

www.SageCRE.com