Choosing a remote access software solution

This document provides an overview of the important technical, operational and financial considerations to address when evaluating remote access software solutions.

November 2016

Contents

Introduction

With so many options on the market, choosing the remote access software solution that offers your organization the best value is an important business decision. But differences in pricing structure and key terminology can make comparing products frustrating, and the wrong selection can result in spending thousands more dollars per year than necessary, or paying a premium for features you will never use.

We've created this guide to help you compare remote access software. In it, we provide an overview of the different pricing structures, feature sets and security guidelines favoured by vendors in the industry. We also introduce and explain key terminology, which can vary from vendor to vendor.

Overview

This document outlines the differences between remote access software solutions in these important categories:

- **Cloud versus direct connectivity** – You can establish a connection from one computer to another either directly (in which case you may need to configure your firewall and router) or automatically using cloud connectivity. This section outlines the advantages and disadvantages of each method.
- **Feature evaluation** – Besides basic screen sharing, remote access software can have dozens of additional features. While many are beneficial, you may be at risk of paying extra for features you will never use. This section addresses the importance of balancing functionality against cost.
- **Security considerations** – Customer security is every vendor's top priority, but you may not be aware what the jargon surrounding this topic actually means. This section introduces important terms, helping you understand how your data is protected by the solution you choose. It also details how transparent a vendor should make their security policies.
- **Pricing models** – Conflicting pricing can make it difficult to compare the cost of one remote access software solution with another. In this section, we outline the information you need in order to make an informed comparison of different products.

Cloud versus direct connectivity

Remote access software can establish a connection between computers in two distinct ways: directly, or using cloud connectivity. This section addresses the difference between each connection method, and discusses why you may choose to use one over the other.

Direct connections

At no point does a direct connection communicate with third-party servers. Instead, the connection is established, and the remote session maintained, between the device you are using to take control (Viewer device) and the computer you are taking control of (Server computer).

This provides a remote connection between computers in the same network, even if that network is private (e.g. a LAN), although you must know the Server computer's local IP address/hostname in order to connect.

Direct connections are completely configurable. For example, if your network environment mandates that all connections remain within a private network, direct connections can be tailored to comply with this.

It is possible to make a direct connection over the Internet, meaning you *can* take control of a computer that is on a different network. This usually requires port forwarding and changes to every firewall that stands between the Server computer and Viewer device, but you can also use a virtual private network. In both cases, additional configuration is necessary.

This extra setup is often trivial to computer experts, and provides precise control over a connection and its route. However, it can be difficult for the average user to configure and administer connections in this way, and impossible even for computer experts if the connection has to pass through equipment they cannot access.

Imagine you are a system administrator and a colleague is in a hotel and connected to its Wi-Fi. No amount of technical expertise will allow you to connect to their laptop, because there is no way for you to make the necessary configurations to the hotel's firewall and router.

Cloud connections

Cloud connections give you control of your computer from anywhere to anywhere, even over the Internet, without needing to configure firewalls and routers or know the Server computer's local IP address/hostname. In the example above of your colleague being connected to hotel Wi-Fi, a cloud connection would be simple.

Once the cloud service has brokered a connection, the remote session itself is often peer-to-peer. This ensures latency remains minimal, as events are sent directly from one computer to another.

Cloud connections can build upon the security offered by direct connections. For example, the cloud service can be used to provide extra protection against man-in-the-middle attacks. When connecting directly, identity checks are usually done manually so are subject to user error or significant infrastructure set-up costs.

To summarise, cloud connections require no administration and do not sacrifice security. For the majority, this ease-of-use is more beneficial than the increased control offered by direct connections.

Our advice

Your own use case is likely to favor one connection method over the other. If you are unsure which, or if your use case is adaptable (e.g. you are part of a LAN at work but need to access colleagues' computers when they are off-site), consider a remote access solution that supports *both* connection methods. This is the easiest and cheapest way to ensure you are covered for any eventuality.

Feature evaluation

It can be tempting to favor whichever remote access software solution has the largest feature set. However, this approach may not give you the best value for money or an ideal user experience. If your remote access software contains too many features you will never use, it can feel bloated and unnecessarily complex. These extra features can also drive up a product's cost.

Understanding which features benefit you

A solid feature set is important, as certain functionality can be the difference between an intuitive user experience and hours of frustration. One example of the former is system authentication. When taking control of a computer, system authentication lets you confirm your identity using the details you usually use to *log in* to that computer.

During your research, you'll come across multiple features that simplify remote access in a similar vein. But you must be careful not to assume that every feature is of equal benefit to every user. A good example of this is remote deployment/policy control, which can greatly increase a product's price despite only being useful to certain high-level users. These features are critically important for system administrators, who 'push' software to their colleagues and prevent them from changing certain settings. However, most users will never use this functionality, even if they pay for it.

Finally, be aware you may find it difficult to pin down which products support which features. This is due to conflicting terminology within the industry, and because one vendor may heavily advertise functionality that another vendor sees as a basic necessity. This means you may need to study a product's user guide or FAQs to understand its full capabilities.

Free, Business and Enterprise products

Most remote access software is separated into multiple pricing tiers, each offering different features. A typical pricing structure might look like this:

- **Free** – Non-commercial use only. Essential security and features. Restricted connectivity.
- **Regular** – Commercial use. Full security. More features.
- **Premium/Enterprise** – Commercial use. Full security. Advanced administrative feature set.

Some remote access software is comprised of many different products, or bundled with additional software you may have no use for. Be wary with these solutions, as the lines between each product can become increasingly blurred. This can make it difficult to know which pricing tier suits your needs best.

Our advice

Don't simply settle for the product with the most bullet points in its feature list. Instead, keep your own use case firmly in mind, and choose the software that supports this with the most precision. Otherwise you are at risk of paying for features you will never use, which only serve to make your experience unnecessarily complex.

With remote access software, less can often be more.

Security considerations

Customer security is a top priority for every vendor. However, the jargon surrounding this topic can be difficult to understand, leaving you confused about how exactly your data is protected.

This section provides an overview of the terminology you're likely to come across when researching remote access software security. Afterwards, we outline the security information that reputable vendors should divulge to their users.

Key terminology

An important security measure is **encryption**. Encryption ensures any information passed between your Server computer and Viewer device is unreadable to malicious third parties. This keeps data such as keystrokes and file transfers safe from a potential attacker.

There are many ways to encrypt data, but a robust standard that is commonly used in the industry is **AES encryption**. Data encrypted with AES can be protected with either a 128-bit or 256-bit long secret. The length of this secret is the difference between **128-bit/256-bit encryption**.

Some vendors emphasize the benefits of 256-bit encryption over 128-bit encryption, but both are incredibly secure. 256-bit encryption may be required in order to achieve compliance with a regulatory agency. However, the additional overhead it creates can slow down connections on less powerful computers. This is one reason why some products allow you to choose which level of encryption is used.

The industry standard is for data to be **end-to-end encrypted**. This means even the vendor itself has no way of accessing your data. **Perfect forward secrecy** offers an extra degree of security by providing a unique encryption secret for every connection. This secret cannot be recovered after the connection has ended, ensuring your data is secure now and forever. You should bear in mind that perfect forward secrecy is not yet industry standard.

Your software should support **auditing**, often in the form of logging. By checking connection logs, you can prove that someone from a particular IP address connected to a computer at a specific time. Auditing tools help support compliance obligations by providing **non-repudiation**.

Finally, you must **authenticate** each connection you make. This additional security measure ensures that even if someone gains access to your account, they cannot take control of all your computers. Instead, they need a specific password or pin code for each computer. With **system authentication**, you can enforce that connecting users must enter the details they usually use to *log in* to a given computer. This means you are protected by the computer's existing security measures as well as your remote access software.

Our advice

You should feel completely confident in a vendor's ability to protect your data. But as someone who may not be an expert in computer security, how do you know who to trust?

First and foremost, a vendor should be transparent. This does not mean their entire security process must be explicitly detailed, but you *do* need to know how your data is protected, and whether they follow industry best practices.

The vendor must actively maintain their product and adapt it to the evolving needs of the market. As any security measure can theoretically be compromised, you should choose a vendor who pledges to update their software in response to potential and active threats – preferably without forcing you to pay for these critical security fixes.

Finally, ensure the connection authentication process is as secure as possible. As detailed above, the best form of this is often system authentication, so look for a product that supports this important feature.

Pricing models

A key frustration you'll encounter is that different products use vastly different pricing models. This makes it confusing to compare the annual cost of two different solutions. Although most use an annual, subscription-based pricing model, this may be where the similarities end.

While Product A may be $45 per month and Product B may be $25 per month, Product B isn't necessarily better value. In fact, the two costs may not even be directly comparable. This is because there are two ways for remote access software providers to charge for their software, and it isn't always obvious which one is in use.

Server pricing model

Some products charge per computer you want to *control*, or per Server computer.

With this model, the device you are taking control *from* (Viewer device) does not need to be licensed. This means you can connect to a Server computer using any device, no matter where you are in the world. Server computers are often licensed in bundles of 1, 3, 5, 10, etc.

This is ideal for collaboration, as multiple users can simultaneously connect to a Server computer from wherever they are in the world, without needing to pay an additional fee per user.

Viewer pricing model

Other products charge per device you want to take control *from*, or per Viewer device.

The Viewer device can access any computer with the necessary software installed, sometimes allowing the installation to be done on-demand. As with the Server pricing model, Viewer devices are often licensed in bundles.

This provides remote access to any computer at a moment's notice, allowing a small number of Viewer users to control any number of computers.

One disadvantage is that you are forced to pre-plan your remote connectivity. If you need immediate remote access while away from your Viewer device (e.g. only your work computer is licensed and an emergency occurs while you are off-site), you won't be able to get connected.

Restricting concurrent remote access sessions

Some vendors restrict the number of concurrent sessions you and your team can make. For example, you may license ten Server computers and ten Viewer devices, but still be restricted to three remote sessions at any one time. It is usually possible to pay extra to enable more concurrent sessions.

It can be difficult to compare the cost of a product that imposes these session controls with one that doesn't.

Our advice

You may find that one pricing model complements your use case more than the other. For example, if you want to access your office computer from multiple devices, the Server pricing model is probably appropriate.

With this in mind, your first step should be to clarify how each product is priced. Due to the conflicting terminology within the industry, this can only be done by studying each product carefully. Disregarding remote access software solutions that don't suit your needs is then far more simple.

Struggling to compare the price of one remote access software solution to another can be extremely frustrating. If a product's website is unclear, or if they hide their pricing until you contact their sales team, consider a solution that offers more transparency.

Summary

Discovering the remote access software solution that suits your needs best can be a frustrating process. This is due to the fundamental differences between each product on the market. You can combat this by thoroughly researching each product, while always keeping your own use case in mind.

Consider how each product suits your needs in the four key categories outlined in this document:

- **Cloud versus direct connections** – Be aware which connection type you need, and choose a product that supports this. If your use case is adaptable, consider a remote access software solution that supports both.
- **Features** – Never assume that the product with the most features will offer the best value or the simplest user experience. Instead, search for a product with a feature set that enriches your experience without feeling bloated.
- **Security** – Every vendor takes security incredibly seriously. However, this doesn't mean you should trust a product blindly. Take the time to study how different vendors keep your data safe. If you are unsure, choose a vendor that provides adequate information about their security measures and support policies.
- **Pricing** – Remember that pricing is split into two key models: paying per Server computer, and paying per Viewer device. Try to establish which of these models suits your use case best. If you find a product's pricing confusing, choose a solution that offers more clarity.

Whichever remote access software solution you choose, ensure you have your own use case clearly defined. You should understand exactly how a product meets your needs before committing to any purchase.

Appendix: The RealVNC offering

At RealVNC, we understand how difficult it can be to compare one remote access software solution to another. This is due to fundamental differences in the key areas outlined in this guide. We empathize with how frustrating this must be, so VNC Connect is designed to have clarity, simplicity and adaptability at its core.

We feel this approach has helped us create a product that gives our customers complete confidence in their remote access software.

Cloud versus direct connectivity

Most business users have an adaptable use case, and we feel remote access software should reflect this need for flexibility. This is why VNC Connect users can make both cloud *and* direct connections.

Millions of our existing customers still rely on us for traditional direct connectivity. By supporting both connection methods with our Enterprise subscription, we offer our customers the greatest possible flexibility.

VNC Connect is one of the only products on the market with full support for both cloud and direct connections.

Features

We want our users to feel in complete control of our software, so our feature set provides essential functionality without ever feeling bloated or difficult to navigate. That said, we're always working on new features that we feel will enrich our customers' experience.

For simplicity, there are only two paid flavors of VNC Connect – Professional and Enterprise. The differences between each are clearly defined on our website, so you always know exactly what you're paying for.

Security

VNC Connect protects your data using industry standard end-to-end AES encryption (up to 256-bit). Unlike most, we also provide perfect forward secrecy, so your data remains safe forever. With optional system authentication, you're additionally protected by the security measures already on your computer.

We're upfront about our security, and we'll update our software as and when necessary.

Pricing

Our pricing structure is simple. We charge per the number of Server computers you need to control, and provide discounts depending on the volume or the length of your subscription. We *never* restrict the number of concurrent connections you can make, and our updates are included in the cost of our subscription.

In a market that can be extremely difficult to navigate, we strive to be as transparent with our pricing as possible.

If you have any questions about the topics raised in this business paper, please contact us at enquiries@realvnc.com, or visit realvnc.com/connect.

RealVNC's remote access and management software is used by hundreds of millions of people worldwide in every sector of industry, government and education. Our software helps organizations cut costs and improve the quality of supporting remote computers and applications. RealVNC is the original developer of VNC remote access software and supports an unrivalled mix of desktop and mobile platforms. Using our software SDKs, third-party technology companies also embed remote access technology direct into their products through OEM agreements.

www.realvnc.com