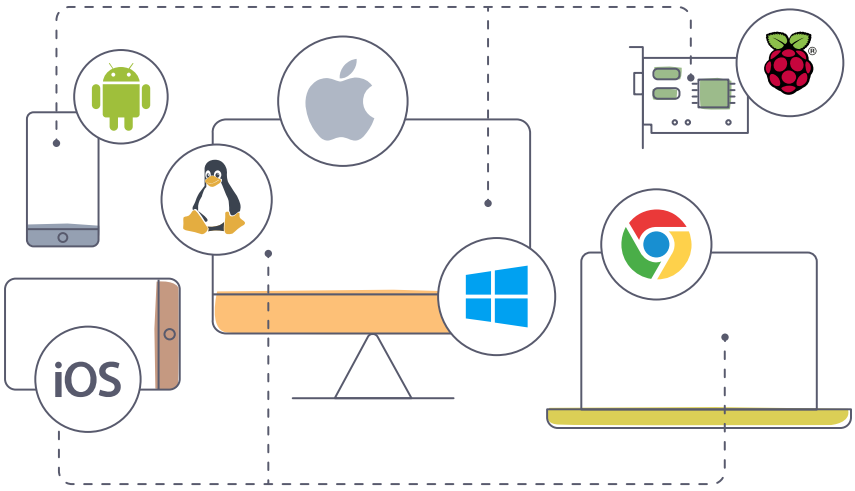
REALVNC

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

Version 1.4



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. However, 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 won't 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 connections to remote computers either directly (in which case you may need to reconfigure intermediate firewalls and routers) or via a cloud service (in which case the connection is brokered for you via the Internet). This section outlines the advantages and disadvantages of each.

Installed versus on-demand access – Remote computers you want to control must be running an 'agent'; that is, a small software program that shares the screen and injects control events. You can either install this program and have permanent access, or provision the remote computer 'just in time', removing it afterwards. This section helps you choose the right method, or methods, for your use cases.

Feature evaluation – Besides basic screen sharing, remote access products typically offer dozens of additional features. 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 suggests how transparent we consider a vendor should make their security policies.

Pricing models – Conflicting pricing and terminology 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 to make an informed comparison of different products.

CLOUD VERSUS DIRECT CONNECTIVITY

Cloud versus direct connectivity

Remote access software can establish connections in two distinct ways: directly, or via a cloud service. This section explains the differences between these connection methods, and discusses why you may choose one over the other.

Direct connections

With a direct connection, endpoints never communicate with third-party servers. Instead, the connection is established, and the remote session maintained, entirely between the device you are using to take control (Viewer device) and the remote computer you want to control (Server computer). Note the connecting user must know the remote computer's current IP address or hostname at the moment they want to connect (IP addresses may change without warning).

Direct connections are completely configurable. For example, if your network environment mandates that all communications remain within a private network (ie. a LAN), direct connections can comply with this.

It is possible to make a direct connection over the Internet, meaning you can access a computer on a different network. This usually requires port forwarding and changes to every firewall 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 standard practice for computer experts, and provides precise control over a connection and its route. However, it can be difficult for the average user to reconfigure network equipment, and impossible even for computer experts if the connection has to pass through equipment they do not own.

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

Cloud connections

You can establish a cloud connection to a remote computer wherever it is in the world, without reconfiguring intermediate firewalls and routers, or knowing the target IP address or hostname. Providing both endpoints are connected to the Internet, the vendor's cloud service brokers the connection seamlessly. In the example above of an employee using hotel Wi-Fi, a cloud connection would be effective.

Once the vendor's cloud service has brokered the connection, the remote session itself is often established peer-to- peer. This ensures latency remains minimal, since packets are transmitted directly between endpoints, and session data itself is not sent via the vendor's servers.

Over the Internet, cloud connections are typically more secure than direct connections. For example, the cloud service may provide extra protection against man-in-the-middle attacks. When connecting directly, identity checks are usually performed manually, so are subject to user error or significant infrastructure set-up costs.

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

Our advice

Your own use case will likely favor one connection method over the other. If you are unsure which, or if your use case is adaptable (e.g. you have a LAN at work but need to access employees' computers on the road), 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.

INSTALLED VERSUS ON-DEMAND ACCESS

Installed versus on-demand access

You can either install remote access software on computers you want to control, or connect 'just in time' using a disposable, zero-footprint app. Some use cases mandate that you must use one of these methods; for others, it's possible to use either.

Installed access

If it's feasible to install remote access software in advance, then a wide range of use cases become possible. You can connect repeatedly, at any time, either to your own computers when you're out and about, or to those of employees or friends, whether attended or unattended. Typically, it also means you can establish concurrent connections; that is, many Viewer users can connect to a Server computer at the same time, perhaps to collaborate or watch a demonstration.

The caveat is that pre-configuration is required. You must have access and permissions to install and license software on all the computers you want to control in advance.

On-demand access

If you don't own or manage the computers you want to control, then it may not be possible to install remote access software in advance.

For example, if you're supporting customers, or employees in a BYOD environment, then you cannot deploy the software yourself, nor reasonably talk the end user through the complex, privileged installation process. In these scenarios, you need to provision remote computers 'just in time' – at the precise moment support is required – and then remove the software afterwards, leaving no footprint.

Products that only support on-demand access excel at a single use case: the IT technician offering technical support to colleagues or customers during office hours. But there are limitations; unattended access and direct connectivity are typically not possible.

Our advice

As with cloud versus direct connectivity, it's important to weigh the benefits of each method. If you have more than one use case, look for a product that supports both methods in a single tool. This prevents your IT team needing to purchase and maintain separate products for different purposes.

FEATURE EVALUATION

Feature evaluation

It can be tempting to favor the remote access software solution that 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 will also drive up the 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 same credentials you usually use to log in to that computer. You don't have to remember yet another password.

During your research, you'll come across multiple features that simplify remote access in a similar way. But be careful not to assume that every feature is of equal benefit. A good example of this is remote deployment/group policy, which can greatly increase a product's price despite being tailored for large enterprises. These features are critically important for system administrators, who 'push' software to their colleagues and prevent them from changing certain settings. But small businesses may not be set up to take advantage, but still end up paying for it.

Finally, be aware you may find it difficult to pin down which product supports 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 has 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.

Business – Commercial use. Essential security. More features.

Premium/Enterprise – Commercial use. Advanced security. Advanced administrative feature set.

Some vendors provide different modules, or bundle additional software for which you may have no use. Be wary of these solutions, as it becomes difficult to know what you are actually paying for.

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 best supports this. Otherwise, you risk paying for features you will never use, and risk making the user experience unnecessarily complex.

With remote access software, less can often be more.

SECURITY CONSIDERATIONS

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 systems and data are 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 industry standard is AES encryption. Data encrypted with AES can be protected with either a 128-bit or 256-bit secret. The length of this secret is the difference between 128-bit and 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 in the future. You should bear in mind that perfect forward secrecy is not yet industry-standard.

Your software should support auditing, perhaps in the form of session logs. By reviewing these, 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 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 credentials they usually use to log in to a given computer. And the vendor should offer multi-factor authentication, so you can layer additional authentication mechanisms on top, perhaps using smartcards, digital certificates, or email, SMS or push notifications to mobile devices.

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 authentication process is as secure as possible, preferably using multi-factor authentication.

PRICING MODELS

Pricing models

A key frustration you'll encounter is that competing products use different pricing models. This makes it confusing to compare the annual cost of two different solutions. Although most vendors 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 different ways for remote access software vendors to charge for usage, and it isn't always obvious which one is on offer.

Server computer pricing model

Some products charge per remote computer you want to control (Server computer), often in bundles of 1, 3, 5, 10 and so on.

With this model, the devices you are using to take control (Viewer devices) are not licensed. This means any number of people can connect in, from any number of machines. This is cost-effective in a training scenario; multiple users can connect simultaneously to an expert's Server computer, without needing to pay an additional fee per connecting user.

Viewer user pricing model

Other products charge per person taking control (Viewer user).

With this model, the remote computers you want to control are not licensed. This means you can support any number of remote users, without calculating demand in advance. This is the most cost-effective model for the IT helpdesk; the size of your IT team is a known quantity, but the number of users requiring support is unlikely to be.

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 most effective. However, for the IT helpdesk, Viewer-based licensing may be preferable.

You may not find these different models explained clearly on a vendor's web site, so we recommend studying each product carefully. 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

Summary

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

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

Cloud versus direct connectivity – Be aware which connection method you need, and choose a product that supports this. If your use case is adaptable, consider a remote access software solution that supports both.

Installed versus on demand access – There are pros and cons to each method, so consider a product that supports both. Otherwise, your IT team may need to manage and maintain separate tools for different use cases.

Feature evaluation – Never assume that the product with the most features will offer the best value. Instead, search for a product with a feature set that enriches your experience without feeling bloated.

Security considerations – Although every vendor takes security seriously, don't trust a product blindly. Take the time to study how different vendors keep your data safe. If you're not sure, choose a vendor that provides adequate information about their security measures and support policies.

Pricing model – Remember that pricing is split into two key models: paying per Server computer, and paying per Viewer user. 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 a purchase.

Appendix: The RealVNC offering

At RealVNC, we understand how difficult it can be to compare one remote access software solution with another. So we've tried to make VNC Connect as simple and as flexible as possible.

Cloud versus direct connectivity

VNC Connect supports both cloud and direct connectivity, and is one of the only products on the market to do so. Millions of our existing customers still rely on us for traditional direct connectivity, but you can now connect via our cloud service too. By supporting both connection methods with our Enterprise subscription, we offer customers the greatest possible flexibility.

Installed versus on demand access

VNC Connect is unique in the marketplace in that it has both device access and instant support capabilities built-in. There's only one product to purchase, deploy, manage and secure. While instant support enables IT technicians to connect to computers that do not, or cannot, have remote access software installed, device access lets you provision remote computers in advance and benefit from regular, direct, concurrent and unattended access. With VNC Connect, you don't need to purchase and maintain separate tools for different remote access use cases.

Feature evaluation

We want our customers to feel in complete control, so our feature set provides essential functionality without ever feeling bloated or complex. That said, we're always working on new features that we hope will enrich the experience. For simplicity, there are only two paid VNC Connect subscriptions – Professional and Enterprise. The differences between each are clearly defined on our website, so you always know exactly what you're paying for. You can try either free for 30 days.

Security considerations

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 system authentication and multi-factor authentication, you're additionally protected by the security measures you've already invested in. We're upfront about our security, and we'll update our software as and when necessary.

Pricing model

Our pricing model is the most flexible on the market. Instead of forcing customers to choose between Server-based and Viewer-based licensing, we offer both in a single, simple subscription. This means you don't need to buy separate tools for different remote access use cases, reducing your costs as well as attack surface and maintenance overhead. When you come to purchase, simply choose between a Professional and an Enterprise subscription, and then select a remote computer tier for device access, a number of technicians for instant support, or both.

If you have any further questions, 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