How to Improve Secure Remote Access - and Keep IT and User Happy

-A SOLITON WHITE PAPER-

Soliton®

CONTENTS

You're probably wondering if you're really going to learn anything new about remote access solutions in this guide? You know remote working is here to stay, and you need solutions to keep users happy, without compromising security. What else is there to learn?

We get it. There's already a lot of information out there. But trust us: we're here to share something a bit different, which may help you solve the challenges and issues common in many remote access solutions.

But before we get into the details, here's a real-life example.
The world's largest automotive manufacturer has 53 overseas manufacturing facilities in 28 different countries. It directly employs over 25,000 people and works with an additional 25,000 contractors, consultants and partners.

With COVID-19 lockdown restrictions, management decided all employees had to work from home, which meant over 12,000 additional users required remote access to the company's internal systems.

Upscaling the existing remote access solution wasn't a viable option, as it required infrastructure changes and additional load balancers to add more users and getting remote access for the 12,000 employees would take too long, given the very immediate need.

Using a VPN connection for remote access was also not an option. Aside from the risks associated with VPNs, the company needed a solution to cater for approximately 6000 AutoCAD users; high library call volumes and large data downloads meant these users would put too much burden on the VPN, making it unacceptably slow.

Today, the car maker's employees and contractors can work from home securely and with simplified everyday operations. Both the remote device and the internal office device connect outbound to a Secure-Desktop service, and the service connects the two together. Users and devices are strongly authenticated on both ends, using digital certificates to provide an added security layer.

The outbound connections mean it's unlikely that changes to the firewall are necessary, saving the IT department time and reducing implementation costs. As well, the office desktop computers can take any route to the internet that is available, which prevents a single point of congestion and improves performance.

The IT department can immediately upscale users, without having to modify the IT infrastructure, and users can simply download the application to their home device to access an office PC. The streaming technology compresses and transfers only the information on the PC screen to the remote device to ensure a stable connection — even with low bandwidth internet lines.

Employees can get started without any training, making the roll-out to over 12,000 people smooth and efficient. Fast connection and HD image quality mean it renders a highly synchronised remote screen to ensure efficient remote operations, which is highly valued by AutoCAD users.

SecureDesktop meant the company could leverage personal PCs and Macs, to get people working from home, without compromising sensitive data or security.

Curious to find out more? Let's get started!

WHY THE TIME FOR ACTION IS NOW

It's obvious that companies require some form of remote access solution — modern working practices mean it non-negotiable. But sticking to "what we've always done" is not necessarily fit for purpose anymore. Many companies are starting to wonder whether the solutions they have in place are future-proofed, especially if they already see some cracks begin to appear.

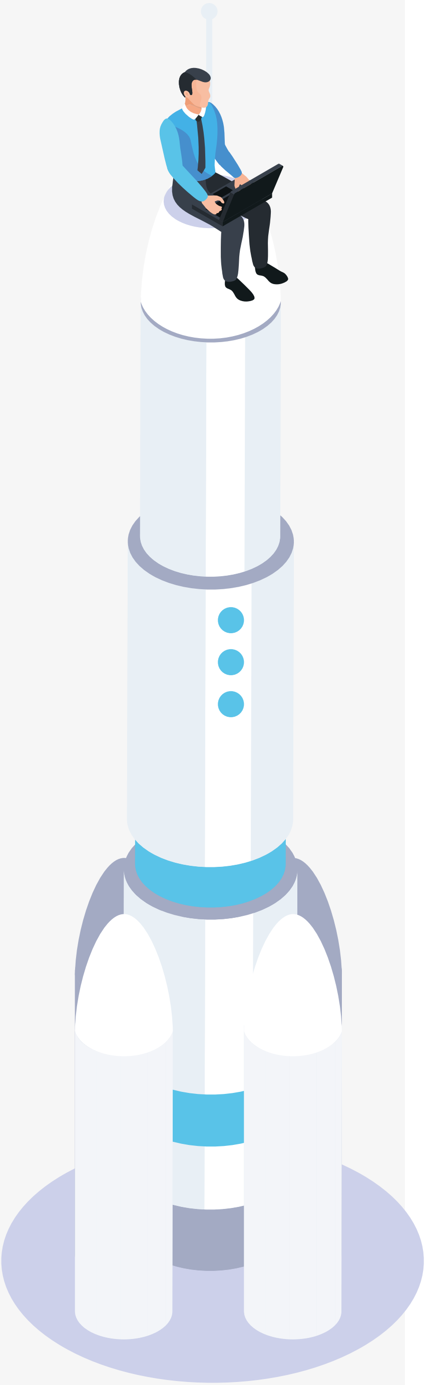
So the question is, why now? What changes are happening, that means companies are rethinking their approach to secure remote access. We've identified four key challenges that IT teams need to address.

#1 The elephant in the room: COVID-19

We can't write about remote working without mentioning COVID-19. Plenty of articles already exist about the explosion of home working and the likely long-term changes to working habits. But from a remote access perspective, COVID caused a very sudden, almost overnight, need for many more people to work away from the office. IT teams had to work very fast to scale remote access — sometimes at the expense of making the solution secure.

Now, many companies are starting to reflect on their approach to remote working and consider how to future-proof the way they've scaled remote working capabilities. People are now beginning to think, 'we've put a solution in place, but it's complicated or insecure. What can we do to improve?'

What this means for you:
After the rush to get people working from home earlier this year, now is the time to reflect and consider. Is your solution secure? What could you do now to make it faster, more reliable and more efficient?



#2 Users expect to be able to work anytime, anywhere

People used to go to the office to do work. They'd start in the morning, work through the day, before heading home in the evening. Not anymore. Today, people expect to be able to work anywhere and anytime they like.

At home, they're used to quickly accessing services. If they want to watch a film on Netflix or check their personal inbox, they know they'll have instant access. This same expectation applies to work; it's now the status quo.

Improving support for anytime, anywhere working isn't just about reducing complaints to IT about slow services and poor connection — though, of course, it's an added perk. The real business driver is ensuring people can do their jobs, effectively and productively, wherever they are.

What this means for you:

Users expect you to provide seamless access to work systems; for them, technology should be an enabler, not a blocker. As we said in the introduction, you know remote working is here to stay. This requires remote access solutions that help users get their work done.

#3 Purchasing and managing devices for each user is expensive

When companies issue users with devices, IT typically retains control over the device. But this approach is expensive for the business. You have to pay for the device. You have to buy software to manage it. You have to control it. You have to think about and mitigate all the risks in all the places.

And, if demand for devices spikes, it can be impossible to get hold of enough devices — even if you have the budget available.

For the user, using company-owned devices also has downsides. The device is a business PC. If they want to use it for personal reasons, it probably isn't allowed. And if they change jobs, the computer likely will need returning, meaning if they have used the device for personal use, they might lose personal data or IT management could lock them out.

What this means for you:

Purchasing devices for users is difficult to scale, especially when demand outweighs supply. Relying on this approach means you're left stuck if availability - or budget constraints - mean you can't buy enough devices.

#4 Infrastructure changes are hard to scale quickly

Some remote access solutions rely on infrastructure changes. If a company wants to give access to internal resources, they often install security gateways. In theory, it's a good practice. Security gateways check a remote users identity, secure the connection and endpoint, and allow the user access to the resource. Gateways also ensure there is a central point where all remote access can be monitored, logged and controlled.

But it has downsides. Implementing gateways means making changes to the network infrastructure, which can be complicated and time-consuming. Additionally, all traffic going back and forth to internal computers now has to go through the gateways. This scenario creates congestion — and can significantly slow down the speed of the connection.

What this means for you:
If the demand for remote access increases suddenly, it's challenging to make the necessary infrastructure changes in-line with business demand. Even if infrastructure changes are feasible, congestion through the gateways can make connection speeds unacceptably slow for users.

A NEW APPROACH TO REMOTE ACCESS: THE ANSWER TO YOUR CHALLENGES

Whether you work in construction, education, transportation, or an entirely different sector, you've likely come across one or more of the remote access challenges outlined above. But what can you do? How can you improve secure remote access, maintain security and support employees working away from the office?

It needs a different approach to remote access, one that is fast, secure and easy to get started.

Picture this scene: An employee is finishing off their morning coffee at 8:30 am. Work is supposed to start at 9 am, and it takes 45 minutes to get to the office. But they're not running late. They're already at their desk. They're using their home computer — and able to access everything they need, just like they're in the office.

How is this possible? Using Soliton SecureDesktop, a remote desktop solution.

In the past, helping employees work from home was hard. Solutions are often time-consuming and expensive to set up, with complex infrastructure changes needed. And, if set up incorrectly, can create security issues.

Soliton SecureDesktop changes this by providing employees with remote access to their internal office desktop. It securely connects an internal office PC or Mac to a remote device, without having to open up the firewall or make complex infrastructure changes.

So just what is it about SecureDesktop that helps answer the common remote access challenges?

#1 Outbound connections

SecureDesktop is a cloud service that connects an internal resource to a remote device, without having to open up the firewall. Both the remote device and the internal device connect outbound to the service, and the service connects the two together. The result of this connection is that the remote device and the internal computer are talking directly to each other over a secured channel. As the connections are outbound, it's unlikely any firewall changes are necessary.

Using outbound connections, the internal desktop computer can take any available route to the internet. This prevents a single point of congestion, which improves performance and keeps the service fast.

#2 Digital certificates

Creating access rules without proper authentication doesn't make a lot of sense. Both users and target devices need authentication. Otherwise, how do you know who's really on the other side?

The answer is digital certificates, which validate users and devices to ensure they're allowed access. If a PC or phone doesn't have the right certificate to make a connection, that trust isn't in place, and access is denied. Sounds good, right?

SecureDesktop uses digital certificates to provide an additional security layer, with users and devices strongly authenticated on both ends. Even if the employee loses their home device, revoking the digital certificate prevents unauthorised access.

But digital certificates have a reputation for being complex. If something goes wrong with the certificate, it isn't trusted, and authentication fails.

SecureDesktop removes this complexity from device and user authentication, making it simple and secure. It's all managed as part of the service, so you don't have to worry.

#3 No network infrastructure changes

When companies need to scale up remote working capabilities, they often don't have time to make complex infrastructure changes. The business-critical need to get people working from outside the office means delays are too expensive.

Whether the requirement comes from an existing solution not working, or because more people need to work away from the office, a solution that doesn't rely on infrastructure changes is essential to move fast.

SecureDesktop is installed with just two clicks and establishes secure and reliable connections.

With SecureDesktop, the internal system can be Windows-based or macOS-based while the clients can run Windows, macOS, iOS, iPadOS or Android. The communication protocol is extremely fast, allowing even the most demanding applications to run smoothly on the endpoints. SecureDesktop is cloud-based, which means organisations can start to scale up their secured remote working capabilities in minutes, rather than weeks (though it's also available on-premise if that worked better for you).

THE BENEFITS - FOR YOU AND YOUR USERS

Now let’s get to the bit you really care about: how does a remote desktop solution make life easier for you and your users? Companies are already utilising services like Soliton SecureDesktop to streamline remote access, without compromising on security. They’re doing this because they recognise the four business benefits that embedding accurate remote access solutions can have for them.

1

Remove complexity from your remote access

We've already covered the downsides of solutions that rely on you making complex infrastructure changes. So it should be no surprise that one of the benefits of SecureDesktop is it's fast to set up. Deployment completed in as little as 1 hour. It doesn't require any modifications to the existing IT infrastructure; no need to install a VPN or RDP.

2

Fast to setup + fast and stable access

You can add users by forwarding an URL, inviting them to connect to the SecureDesktop Service. Employees can launch a remote session to their work computer and work from anywhere that has an Internet connection.

And, once set up, users can get access to their office computer in seconds. The streaming technology used in SecureDesktop compresses and transfers the information on the PC screen for remote operation and ensures a stable connection — even with low bandwidth internet lines.

3

Scale-up (or down) as you need

You can immediately upscale (or downscale) users, without having to modify the IT infrastructure, and users can simply download the application to their home device to access an office PC.

4

Leave no trace of company data on unmanaged devices

SecureDesktop ensures data protection on every device used for remote access. When using the SecureDesktop app, the office-based PC shows a black screen, indicating its remotely controlled. This feature prevents unauthorised people from viewing data - even when the PC under control is in an open-plan office.

It also protects users from accidentally leaking valuable company information, as they cannot copy & paste or transfer files between the office and private PC. And, when they close the app, all data is automatically deleted.

THE BUSINESS SUCCESS FORMULA:

Keep users happy

+

Keep IT happy

=

Happy business outcomes

Enough on the technical details: let's talk about you again. We've shown the importance of having the right solution in place for remote access and explored the benefits of Soliton SecureDesktop. But we're not there yet. It's not just about the technology; it's about who uses it and the business drivers. In other words, we need to consider you, your users and the business reasons you need a remote access solution in the first place. That's why we'd like to introduce you to what we believe is your success formula:

Keep users happy + keep IT happy = happy business outcomes.

To put this formula into place, these are the ultimate ingredients:

1. Friction-free experience for users
2. Security at the core of the solution
3. Experts that understand how to support you and your business challenges

1

Friction-free experience for users

Getting users to adopt tools relies on making life easy for them. They need to be intuitive to get started, with a super-fast, reliable connection, so users can access what they need without delay or disruption. Building a friction-free experience from scratch is one way to do it. The other is to implement a remote access solution with one already built-in.

2

Security at the core of the solution

Even while prioritising ease-of-use, security is non-negotiable. SecureDesktop has multiple enhanced security features. All remote connections and data transfers are secured with TLS (including TLS 1.2) and 256-bit AES encryption. The SecureDesktop consists of several components, including the Client and Streamer that provides user and device authentication using 2FA, and this ensures all unauthorised access is blocked.

3

Experts that understand how to support you and your business challenges

Were you turned off when reading the words “256-bit AES encryption” and “2FA”? No need. IT security is a specialism, meaning specialists that can do the technical parts for you. Whether you have in-house IT security or not, calling in the help of a third party is a good idea when getting started. Sometimes, all you need is a helping hand to put the right solutions in place for you.

ABOUT SOLITON

Soliton Systems has a strong vision to innovate solutions, to fulfil the needs of our customers without adding complexity. Soliton supports companies with their security management challenges, including network security and remote access to internal and cloud applications. Soliton's solutions protect the company's resources from unauthorised access and accidental data leakage.

EMEA office

Soliton Systems Europe N.V.
Barbara Strozzilaan 364, 1083 HN Amsterdam, The Netherlands
+31 (0)20 896 5841 | emea@solitonsystems.com

www.solitonsystems.com