Tecan Remote – how to protect your organization and its data.

REMOTE

CONNECT. CORRECT. CONTINUE.

THINKING CAPS ON

Remote support enables rapid resolution of system or software issues, with real-time, expert assistance to minimize workflow disruptions and related costs. For lab operators, reducing – or even preventing – instrument downtime means they can efficiently continue their work. For IT departments, remote support can cut the degree of assistance they need to provide to equipment operators, and helps to ensure that complex instrumentation continues to function as it should. However, remotely accessing your system comes with a certain degree of risk, and this white paper discusses how these challenges can be alleviated, enabling a safer way to efficiently, effectively and securely support customers.

ACKNOWLEDGE THE ISSUES...

Compared to other industries, life sciences has been slow to fully adopt this service, partly due to the sensitive information produced in the lab. Data is vital to every scientist, and allowing access into a private network opens up a point of entry for data infiltration, or other criminal activities such as ransomware. But, with technology becoming more and more complicated – including intricate automation systems – traditional channels for IT professionals to diagnose and resolve issues are not always viable; remote support from specially trained professionals is needed. Any technology provider must therefore balance and reduce the risks to provide this now invaluable support to customers.

... TO MITIGATE THE RISKS

As secure as possible, as open as necessary

Tecan is known for setting industry standards in quality and regulation, which is why we partnered with TeamViewer – a global leader in remote access – that possesses the best state-of-the-art security solutions. All TeamViewer traffic is secured via RSA public/private key exchange and AES (256 bit) session encryption. Communication works through firewalls and proxy servers, allowing HTTPS protocols on port 443 to pass through. If an organization uses a proxy server, Tecan Remote must be configured with settings and authentication for the proxy.

TeamViewer requires no installation, and clients simply download the QuickSupport module – an executable file – which will then establish a connection. As soon as the program is closed, access ends and connection to the client's computer is no longer possible. This way, a client doesn't need to install an application that permanently lives on their computer and can potentially be exploited, giving a transient element to this approach.

IMPLEMENT SECURITY METHODICALLY

TeamViewer is an industry-accepted solution with well-defined security parameters, but it is vital to properly operate the platform to ensure these benefits aren't eroded away. Tecan Remote is built according to the three 'A's of identity and access management, which should form the core structure of any IT security strategy:

- **Authentication – "I am who I say I am"**
- **Authorization – "I am allowed to do what I've said I will do"**
- **Auditability – "You can see what I did and when"**

What does this mean? To begin with, Tecan employees have undergone training to understand data and privacy guidelines, and they must initiate each session with a unique username and password to prevent unauthorized connections. Following successful authentication, users need to manually approve any screen view, remote control or file transfer request, giving total control to the client. And all sessions are logged both locally, and on TeamViewer secure servers, for full traceability and audit purposes.

SECURITY IS A TWO-WAY STREET

There are certain pragmatic steps that can be taken to help minimize the security risk, starting with a concept called the 'zero trust security model'. This ensures that in any interaction that takes place

– software-to-software or human-to-software – both parties must authenticate to prove their integrity. This expands on the first 'A' of identity and access management, rescinds any status an employee may feel exempts them from security detail, and helps to complete the audit trail of every interaction.

We also advice to create an AppLocker configuration for secure connectivity, which restricts the activity of QuickSupport. It guarantees that the correct file and version of QuickSupport is downloaded – and not hijacked by an untrusted source – verifies the integrity of the app, and makes sure it hasn't been tampered with en route. Once the correct file is downloaded, this whitelisting technology tightly restricts what QuickSupport is allowed to do, so that when it runs, it can only speak to the TeamViewer server in the cloud, and not connect elsewhere.

Additionally, network access of TeamViewer QuickSupport should be limited to outgoing TCP connections over port 443 to *.teamviewer.com domains, where Tecan Remote exclusively establishes connections. These suggestions can help boost the security of something that is already best-in-class for secure remote access.

FUTURE STRATEGIES TO ENHANCE SECURITY

Security is an evolving process that continues to transpire as innovations arise and partnerships grow. That's why Tecan is working on improving its platform with solutions that further heighten security measures. On the horizon is a warning system that ensures TeamViewer is being used for its intended purpose and, if something is awry – a suspicious login or if QuickSupport is used for a session other than with Tecan – then red flags are raised.

Tecan Remote uses secure data and program encryption, with every possible measure taken to allow Tecan service and support specialists to provide remote technical assistance in the safest possible way. Of course, remote access is not without risk, but using industry-leading technologies with heightened precautionary measures helps to mitigate them to the utmost degree. Tecan will, as always, continue to search for ways to amplify security and stay ahead of the game to alleviate the concerns of IT consultants and lab personnel.