The 2019 remote access security checklist
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>✓ Find a vendor that is transparent about security</td>
<td>2</td>
</tr>
<tr>
<td>✓ Choose a solution with multi-factor authentication</td>
<td>4</td>
</tr>
<tr>
<td>✓ Make sure you can restrict access rights</td>
<td>7</td>
</tr>
<tr>
<td>✓ Ensure your remote access sessions are encrypted</td>
<td>8</td>
</tr>
<tr>
<td>✓ Understand your connectivity requirements</td>
<td>10</td>
</tr>
<tr>
<td>✓ Choose a solution that supports compliance</td>
<td>13</td>
</tr>
<tr>
<td>Conclusions</td>
<td>16</td>
</tr>
</tbody>
</table>
Cybersecurity has been a major news trend throughout 2018, with frequent media reports of network outages, social engineering attacks and data breaches. To counter cyberthreats, businesses are spending billions of dollars every year deploying technology to protect themselves from risk. Every software product used within your organization presents a potential security risk, and remote access is no exception.

Because remote access software enables control of devices at different physical locations, security is probably the single most important consideration in your overall IT strategy. You must prevent unauthorized individuals with fraudulent or destructive intentions from gaining control of your corporate systems and resources.

With so many remote access solutions on the market, choosing a trustworthy product that meets your security requirements in full can be complicated and confusing. In this guide, we'll break down everything you need to consider before choosing your next remote access solution.
To choose the remote access solution that best meets your needs, it’s essential that you understand the security philosophy of the vendor. A good way to start is by investigating the vendor’s online profile to see what steps they are taking to make sure the product is as secure as possible. It’s also important to get a complete overview of the security architecture of the product to ensure it aligns with your own technical priorities.

Security should be the very highest priority for any vendor of remote access software, so reputable providers will be transparent and make their security information readily available. If you can’t find all the information you need to make an informed decision on their website, ask to speak directly to a staff member.

Some businesses may need to adopt multiple remote access solutions depending on their specific needs but, if you can, it is always best to keep the number to a minimum. Fewer products mean fewer attack vectors for cybercriminals, and easier audit and strategy management. Remote access consolidation not only brings obvious security benefits, but of course also saves you time and money.
Most vendors will offer a free trial so you can try the software before committing to a subscription. While the pressures of work mean it’s easy to download software and then forget about it until the trial is about to expire, try to road-test the product thoroughly, and get any questions you have - especially security questions - answered.

Reputable vendors will make it easy for you to acquire all the information you need by the end of the trial, so you can make an informed purchasing decision. Keep an eye out for emails containing security resources and supporting documentation, and ensure that the vendor’s Support team can be reached easily via either phone or online chat.

**Do**
- Make a list of requirements and essential features
- Make the most of the trial period to road test the product thoroughly

**Don’t**
- Try a product without knowing what you want
- Start the trial and forget to stress-test the security features
Every remote access session must be authenticated before it starts, so you can be sure the user attempting to connect is precisely who they say they are.

Whatever the security architecture of your remote access solution, poor password management can leave your systems vulnerable to cyberattack. While you should always seek to use a remote access product that provides multi-factor authentication, the first step is to ensure your organization adopts a strong password policy.

You should insist that everyone in your organization chooses a password that is memorable, at least 10 characters long and includes letters, numerals and special characters. It’s essential that this password is unique and not shared with other online accounts or services, so that if it is compromised your systems remain safe.

It’s good practice never to use personal information in a password, such as the names of loved ones, pets, or significant dates. The best option is to randomly generate a password that is too long to remember and safely store it using password management software.
Multi-factor authentication

It’s vital to choose a remote access product that offers multi-factor authentication (MFA).

MFA enhances security dramatically by requiring multiple pieces of evidence before access is granted. For example, a connecting user might first be required to supply a user name and password, and then additionally enter an access code generated on a physical device, or plug in a smartcard (or both). While MFA does make things slightly more complex for end users, the security benefits vastly outweigh the costs.

Given the rising level of intensive online criminal activity, relying solely on user names and passwords to grant access to business services constitutes an extremely high security risk.
Identity verification

As an additional security precaution, some remote access solutions require users to confirm their identity each time they link a new device to their account. In this scenario, a user receives an email to the address used to register the account every time they attempt to sign in on a new device.

Authenticating both the user and the device represents an alternative two-factor authentication method that helps keep your system safe in case passwords are stolen or guessed.

When you are assessing remote access software, always ask questions about the authentication process. Remember that while it’s important to educate your team about password management best practices, the priority should be to ensure that the remote access solution itself provides multiple layers of authentication.
Make sure you can restrict access rights

You don’t have to give every user the same level of remote access.

To maintain the highest level of security, organizations should grant different levels of remote access to their employees, so that a person only has sufficient permissions to perform a particular task, and no more.

You should make sure your remote access software provides granular access control. For example, some products allow you to restrict the list of available computers that users are able to discover in the first place. Some may additionally allow you to configure session permissions, so that for example you can grant Administrative users full keyboard and mouse control, but limit standard users to watching sessions ‘view only’. Others might restrict the use of in-session features such as file transfer, printing or chat.
During a remote access session, screen data, files and keystrokes are transmitted between the two devices, potentially over the open Internet. It's essential that this data stream is encrypted end-to-end so that cybercriminals cannot intercept and decrypt it, to steal valuable business and personal information.

Vendors often refer to different levels of encryption in their promotional materials, such as 128-bit or 256-bit AES. This reflects the name of the algorithm used to protect the data (AES) and how hard it is for an attacker to break the code (128-bit or 256-bit).

To crack 128-bit encryption, it would take a network of super computers an average of 100 billion years. The universe has only been around for 13.8.

Solutions that employ encryption generally use 128-bit or 256-bit AES. Both are highly secure, but it's worth noting that higher encryption levels can negatively affect performance, due to the additional processing overhead required.
Open source remote access software typically provides no encryption. Using unencrypted remote access software within a business environment is very dangerous, as it allows anyone to intercept and decrypt session communications, without any indication that it is occurring.

While 128-bit AES encryption is currently virtually impossible to crack and provides a very high level of security, 256-bit AES encryption is the gold standard for future proofing against technology that has yet to be developed fully, such as quantum computers.

256-bit encryption is 340 billion-billion-billion-billion times harder to crack than 128-bit encryption.

Because it takes more processing power to encrypt and decrypt data, you may only want to deploy 256-bit encryption to comply with a particular regulatory compliance regime.

While some software vendors may offer 512-bit encryption, it adds more delay for less genuine benefit, so there is no real reason to adopt it. You should choose between 128-bit and 256-bit AES encryption according to the needs of your business and the regulatory requirements defined by your industry.
As the name suggests, direct connections are established between two devices without the involvement of third party servers. Direct connectivity in remote access software has been around for decades and continues to be used successfully by thousands of organizations.

Direct connections are typically made within a closed network that has no Internet access, such as a LAN or VPN. They are entirely configurable, enabling you to comply with your network environment or security policies.

It’s possible for a direct connection to be made over the open Internet, but you must be able to configure every firewall that stands between the two devices. Therefore, direct connectivity often makes sense for providing IT support to office workers, but is not really a feasible option for supporting travelling employees or those working from home.
Cloud connections

Cloud connections are established via a cloud service provided by your remote access vendor. They are extremely convenient when you need to access devices outside your corporate network, for example when providing service to customers, or IT support to travelling employees or those working from home.

There are two types of cloud connections. In the first type, the cloud service itself acts as the relay mechanism for the entire remote access session, passing session data through the cloud servers. However, this can degrade performance and does introduce another link in the security chain, creating a potential attack vector.

In the second type, the remote access software establishes what is called a “cloud-brokered” connection. The connection between the two devices is negotiated by the cloud service but, once the connection is established, the cloud service steps back, allowing the two devices to communicate peer-to-peer. In this scenario, your remote access vendor doesn't relay session data via their cloud servers, which may be required in order to comply with a particular regulatory compliance regime.

Ideally, your vendor should provide both direct and cloud connectivity, and explain how you stay secure.
Which connectivity type meets your needs?

The following table explains key differences between direct and cloud connections, and between cloud connections that are relayed via a vendor’s cloud servers, and those that are brokered (peer-to-peer).

<table>
<thead>
<tr>
<th></th>
<th>DIRECT CONNECTION</th>
<th>CLOUD-RELAYED</th>
<th>CLOUD-BROKERED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connectivity to computers outside corporate network</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Connectivity in offline network environments (no Internet access)</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Seamless connectivity without specialized configuration</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Zero reliance on third party cloud infrastructure</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Session data never routed via third party servers</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Highly performant and responsive sessions for end users</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
</tr>
</tbody>
</table>
Choose a solution that supports compliance

Security and regulatory compliance are closely related, so much so that the line between them easily becomes blurred. To comply with a particular set of regulations, you must typically address multiple security, privacy and transparency concerns.

Regulatory compliance defines best practice and technical standards for a particular industry. Some of the best known are HIPAA for the US healthcare industry, PCI DSS for the financial services industry, and GDPR for the data protection of EU citizens.

In most cases, regulations will define encryption levels and access control standards, such as compulsory multi-factor authentication. When choosing remote access software, you need to be sure that your vendor is aware of typical regulatory standards and able to explain clearly how their software enables you to meet them.

4% of firms' revenue is spent on compliance

72% of senior executives see compliance as one of the most important challenges in their company

70% of firms are expecting to see new regulations within the next year
Common compliance regulations

**GDPR**

**GDPR: EU General Data Protection Regulation**

Requires businesses to protect the personal data and privacy of all EU citizens effective May 2018.

**HIPAA: Health Insurance Portability and Accountability Act**

US law that defines privacy standards aimed to protect medical records of patients and medical data provided to healthcare services.

**PCI-DSS: Payment Card Industry Data Security Standard**

Policies and procedures that optimize the security of card transactions and protect cardholders against the misuse of personal information.
Here are some of the security and privacy features typically demanded by regulatory compliance regimes:

**Two-factor authentication or multi-factor authentication.** You must be able to prove that users are asked for multiple authentication factors before access is granted, such as a user name and password for the first factor and a one-time validation code sent from a device for the second factor.

**Session encryption.** You must be able to demonstrate that all remote access sessions are encrypted end-to-end. The minimum encryption level to look for is 128-bit, although some regimes require 256-bit.

**Audit logging.** You must be able to provide a history of every user who has accessed your network remotely. These records will be often asked for by an investigator if a data breach has occurred.

**Granular access rights.** You must be able to prove that users are only granted the permissions they need to perform their allotted task, and no more.
Conclusion

We have covered six remote access security essentials: vendor reputation, multi-factor authentication, granular access control, session encryption, connectivity methods, and regulatory compliance. While a six-item checklist might not seem very long, each deserves your full attention to ensure that empowering your organization with remote access does not increase your exposure to risks.

Our remote access software, VNC® Connect, will always protect your session data using industry standard end-to-end encryption, in your choice of 128-bit or 256-bit AES. VNC® Connect also provides multi-factor authentication using, a variety of industry-standard mechanisms that you can configure in any way you choose. And we truly believe in being transparent about our security and software architecture; you’ll find every aspect covered in full in our security whitepaper.

For more information, and to download our security whitepaper and other resources, please visit our VNC Connect security and compliance resource page.

Have you ticked all the boxes?

- Reputable vendor
- Multi-factor authentication
- Granular access rights
- Encrypted sessions
- Direct and cloud connectivity
- Compliance support
Every day, millions of people around the world use VNC® Connect to improve the efficiency of their businesses, connecting people and devices wherever they are.

From the original developers of VNC® remote access technology, VNC® Connect is flexible, secure and easy to deploy for all your remote access needs.

Contact
Sales: 0800 888 6410
www.realvnc.com

Address
RealVNC Ltd
Betjeman House
104 Hills Road
Cambridge
CB2 1LQ
United Kingdom