ConnectWise®

Advanced Cybersecurity & Threat Protection

ConnectWise eBook Series

Intruder Alert:

Secure Your Remote Access Tools From Cyberattackers

Contents

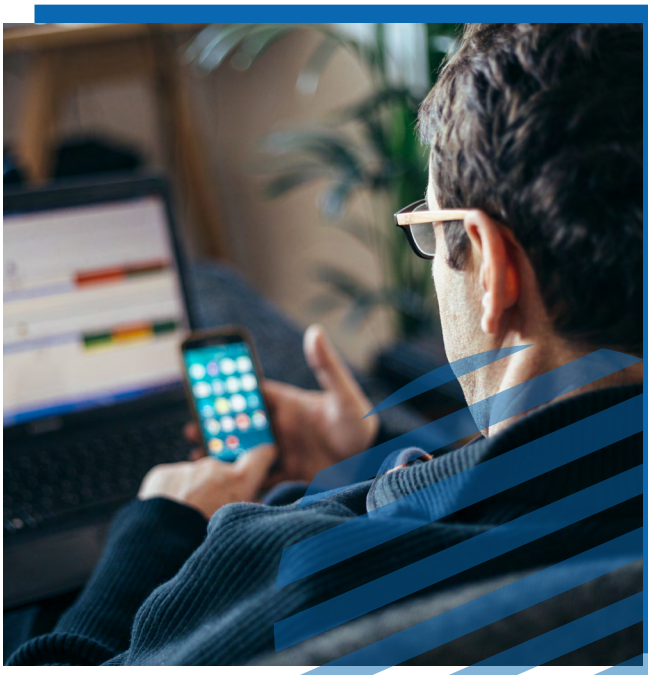
Introduction

Recent large-scale hacks (like those on LinkedIn and Yahoo) have raised awareness about the risks of using insecure passwords. As a managed services provider (MSP) and trusted advisor to your customers, it's more important than ever to consider the security options of the remote access tools you use to support your clients every day.

Vanson Bourne recently surveyed **850 global organizations** with sizes ranging from 10 to 1,000 employees and **64% of respondents have reported that their organization has suffered a cyberattack**.*

Not a big company? You and your clients are still at risk.

Just because you're an SMB doesn't mean you're not a target for cybercrime. The truth is, cybercriminals love MSPs. That's because once they infiltrate your business, they can infiltrate your clients' businesses too—all in one fell swoop.SMBs are an ideal ransomware target. Without the time and resources of a larger organization, they're more likely to simply pay the ransom to get back up and running. Cybercrime affects businesses of all sizes. So, how do you protect your business against these attacks?



Here Are Seven Essential Security Precautions Every MSP Needs to Know

* Underserved and Unprepared: The State of SMB Cybersecurity in 2019
A Vanson Bourne study commissioned by Continuum, a ConnectWise company.

Accessing Your Software

One way to make sure your network environments are kept safe is to simply **be mindful of how you access mission-critical applications**.

For instance, if you're onboarding a new client and you haven't implemented proper malware or antivirus scans against their network, don't log into your remote access tools: wait until you know the network is secure.

The same holds true for deploying agents. Rather than pull them down from machines that aren't secured, consider using a thumb drive—or another alternative that allows you to roll out agents without having to log into your applications.

Knowing the right time to access software and limiting the number of times you jump into a remote session will help reduce your chances of accidently opening up environments to attack.

Role-Based Security

Role-based security defines permissions according to the role that a user performs, and can also specify which machines, or group of machines, can be accessed by users.

The basic idea behind role-based security is that you give your technicians access to **only the features they need to do their job—and nothing else**. This way, you reduce the damage a bad actor can do if they get one of your technician's credentials. By doing this, if a hacker gains access to one user's credentials, they can't wreak havoc in the same way they could if every user was a system-wide admin.

Set up individual user accounts for every one of your technicians. Specify permission around machine access, locations, device types, and so on. **Let your technicians know that this isn't to put roadblocks in the way of them doing their jobs, but is an effort to keep their environment more secure from bad actors.**

Password Complexity

You'd think by now that coming up with a strong password would be a pretty straightforward task. But those pesky cybercriminals are always upping their game.

The National Institute of Standards and Technology (NIST) recommends using long, unique passwords—**ideally about eight characters long**. You can add symbols, uppercase letters, and numbers to make them even more unique.

We know that managing long, unique passwords for all the applications you use on a daily basis can be difficult to keep up with. A password manager makes that a lot easier to maintain these complex passwords, and also saves your technicians time during their workday.

Finally, make sure your applications have appropriate lockouts built-in. Lockouts help prevent brute-force attacks by enforcing a rest period after 8-10 failed lockouts. This extends the time it would take for a hacker to brute-force break into your account.

A password is the first line of defense against an attack. Increasing the complexity of your passwords can be the thing that keeps an attacker busy enough for you to deploy the tools to stop them in their tracks.

Multi-Factor Authentication

Multi-factor authentication requires a user to present more than one form of identity validation before granting system access. It might be a combination of something you know (like a password) with something you own (like a cell phone or debit card). In essence, it's about blending knowledge with possessions to more securely validate someone's identity.

One popular method for multi-factor authentication is **email authentication**. This way, even if a cybercriminal cracks your password with brute force or credential stuffing, they would still need to validate their identity via your email address to access your account.

Another popular method for MFA is the use of authentication apps. Authentication apps generate security codes (time-based one-time passwords) that can be used when you log in to your remote access tools.

Sometimes MSPs resist multi-factor authentication because they're concerned the extra step will frustrate their technicians. But the truth is, it just takes a few seconds—and in the grand scheme of security, it makes a world of difference in protecting you, your environment, and your users.

Logging & Auditing

Logging and auditing are about tracking who is connected to which machine, when they connected, where they connected from, and what they did while connected.

Capturing, saving, and periodically reviewing this information enables you to flag suspicious activity in your environment. This is valuable because, by the time you receive a ransomware threat from a malicious actor, they may have already been poking around in your system for weeks—even months—performing activities too innocuous to set off any alarm bells.

By reviewing your audit log regularly, you can catch some of those anomalies early. Case in point: If you notice someone connecting to your environment or sending commands at 3:00am, you'll know something's up—and you can respond quickly before the issue escalates.

Require Consent

As an MSP, it's also your responsibility to make sure your end users are doing their part to keep their environment secure—which really comes down to educating clients.

Because the average end user doesn't know how to recognize, say, a phishing attack, you need to walk your clients through what these different attacks entail, and explain to them how you protect against them.

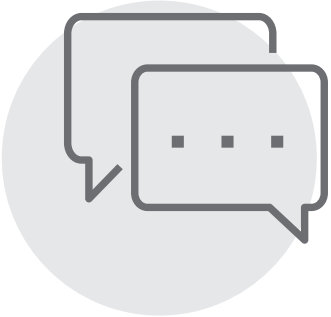
'Guest consent,' for instance, is one precaution that has saved a couple of our clients. When you have 'guest consent' enabled, your end user can say whether or not someone can connect to their machine. **If something seems fishy or they have questions, they can deny access and reach out to you.** It's a simple, powerful way to make sure that if your credentials are compromised and someone gets into your application, you have another layer of protection.

Inform the User

We've all seen the "If you see something, say something," signs in airports and train stations. The same principle holds true for your end users in their environments.

If they notice something suspicious, sense their machines are running slow, or see weird programs opening up—they need to send you tickets informing you of the issue.

But they won't know to do that unless you're reminding them to do so and helping them to recognize when something that looks innocent may actually be a threat.



It makes you more valuable, and your end users will appreciate you for it.

Other Considerations

Now that we've covered the seven security must-haves, what are additional things you should consider in the security of your remote access tools?

1. **STUDY** different cybersecurity frameworks, like the NIST Cybersecurity Framework, which is quickly becoming the industry standard. It's a framework that outlines how to be more secure in your environment—and how to make security a priority.

2. **SIGN UP** for the US Department of Homeland alerts. The department sends regular email newsletters that alert you to new threats and other information to help you stay secure.

3. **CREATE** an incident response plan. Even if you follow all the rules, bad things can still happen. Maybe you're protected against outside hackers, but what if an internal employee loses their cool one day and does something disastrous? Think through all the possible scenarios and people involved—in-house employees, clients, past contractors, and even mistakes you yourself might make—and document your response plan.

4. **ENCRYPT** your data properly. Cloud solutions transmit data which must be protected between the user's browser and the cloud servers. Protection like HTTPS/SSL (Secure Socket Layers) encrypts the data being passed between the user's browser and the web server. When web applications use desktop tools to communicate to the web server, it's paramount to have vetted, strong encryption and cryptographic modules in place, such as AES-256 and Microsoft® FIPS 104-2.

5. **REVIEW** your security procedures regularly. Does everyone have multi-factor authentication? Do all users have long, unique passwords? Are your permissions role-specific? Take time every so often to review your procedures, evaluate your environment, and ensure your software is up to date with the latest security features.

6. **COMPLETELY** offboard employees. When an employee is leaving your company, this is a moment when you'll definitely want to make sure you take appropriate security precautions. Keep a checklist of all the applications they have access to—and make sure you delete their accounts or make them inactive.

Conclusion

Cloud-based remote solutions and resources are going to be a mainstay in our computing lives from here on out.

Making sure they're secure is absolutely essential. Follow the principles in this guide to stay one step ahead of the next cyberattack—and one step closer to providing your clients with expertise and experience that is second to none.