N-ABLE™

Take Control:

Built for secure remote access

eBook

Table of Contents

Intro

Imagine that someone could tunnel into one of your customer's computers and access every file, every app, and every driver on the system. They could make all the changes they wanted in seconds. They could upload malicious scripts, change user credentials, or download ransomware to the machine.

Making matters worse—they could do this because you left the doors wide open for them to enter.

Unfortunately, this happens with a lot of remote access systems and protocols. Remote connections are often done via remote desktop protocol (RDP). When this is enabled, it leaves open a listening port on the end machine. It allows for convenient access to everything on your customers' computers, but also can leave them vulnerable to cyberattacks. This isn't hypothetical. The FBI posted an alert in late 2018 claiming, "remote administration tools, such as Remote Desktop Protocol (RDP), as an attack vector has been on the rise since mid-late 2016."[1]

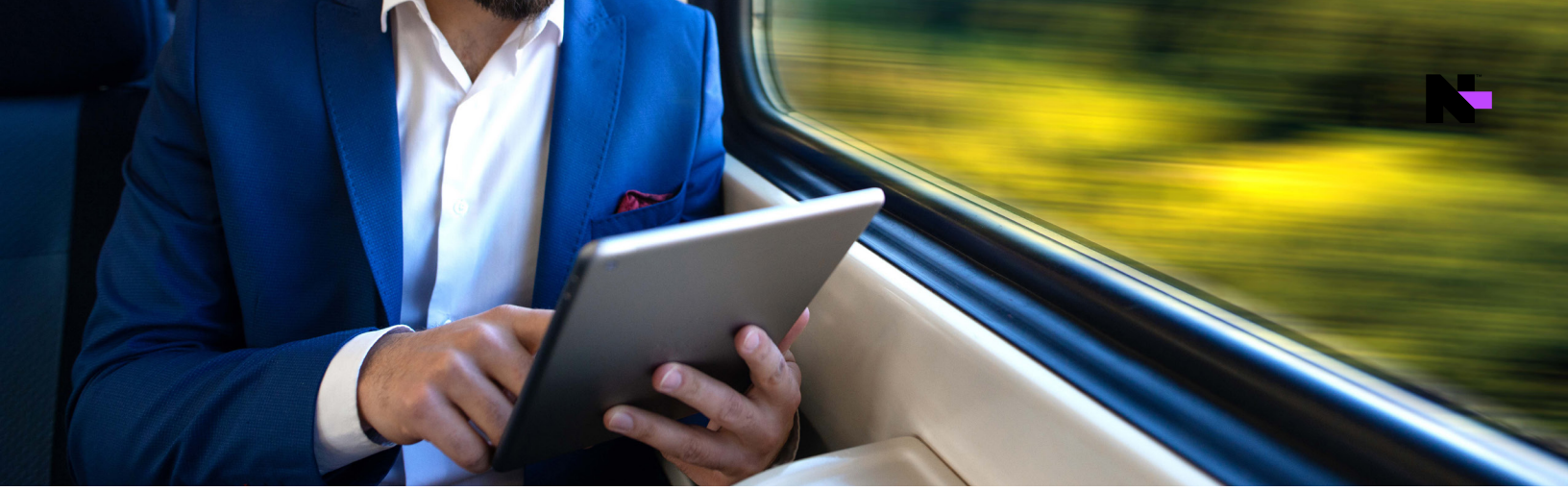
If you're serious about your customers' cybersecurity—and you absolutely should be if you want to keep their business—then it makes sense to find a remote support solution that takes security just as seriously.

N-able™ Take Control was built with security in mind from day one. It contains multiple safeguards designed to keep both you and your customers safe. Before we get into that, however, it helps to understand the risks posed by using insecure remote support.

THE CONSEQUENCES OF INSECURE REMOTE SUPPORT

Let's say you use an RDP-based solution. If attackers manage to break into an RDP port either because it was left open or the user had a weak password, they pretty much have free reign on that machine. They could use it to install malicious software like ransomware (which happened to LabCorp in a 2018 attack[2]), keyloggers, financial trojans, or cryptominers. If they compromise one machine, they could use that as a launching-off-point for attacks against the rest of the network. Or they could use PowerShell® scripts or commands to do a lot of other damage on the machine. Making matters worse, since these attacks often use built-in Microsoft® Windows® tools, these attacks can be hard to detect with traditional antivirus programs or prevent by blocking the applications. Instead, it helps to choose remote access technology that doesn't rely on simple RDP connections.

However, RDP vulnerabilities aren't the only things you have to worry about. Despite your due diligence during the hiring process, insider threats happen. Some are malicious, some are accidental, but either way they can do serious damage. According to a study from Ponemon Institute, the average cost of an insider incident for companies with fewer than 500 employees was $1.8 million.[3] Any remote support solution you choose should help reduce your risk of these potentially catastrophic insider threats.



Secure access

With the challenges of traditional remote access and protocols like RDP, the question arises: What does it take to make it more secure? N-able Take Control was built from day one to sidestep these vulnerabilities and help you remain secure in even harsh environments.

First off, you want to prevent unauthorized access to the end-user machine. As mentioned before, if you use a traditional RDP-based solution you're leaving the doors unlocked for motivated hackers. Take Control uses a separate viewer and agent for remote connections. Instead of a direct connection between two machines, this routes traffic through an intermediary that's much harder for hackers to penetrate.

Second, N-able Take Control offers the ability to tightly control user permissions. The "principle of least privilege" applies here. For example, if you have assigned techs to specific accounts, then there's no reason for them to have access to other accounts. This can help you reduce your risk of an insider attack—and mitigate some of the damage if one occurs. The last thing you want is a disgruntled employee making off with customer data or trashing your systems and workstations. Take Control is designed to help prevent that.

Third, you need to protect logins like they're prized possessions. Any solution worth its salt must include two-factor authentication (2FA). Additionally, N-able Take Control offers authentication apps for 2FA including Google® Authenticator, Duo® Mobile, Authy®, and Microsoft® Authenticator. These apps increase security by helping prevent SMS message interception from cybercriminals or from those who gain access to email accounts.

Finally, you want to make sure to keep passwords for your customers' systems under tight lock and key. You don't want technicians using their own individual password managers (or paper) to handle authentication across accounts. Take Control includes an integrated password manager that injects credentials into a system without the technician ever seeing them. You simply put credentials in once, then the vault is locked with a recovery code and master password. Additionally, the integrated password manager records every action taken—vault creation, use, and deletion—so you can review and audit every touchpoint in case you suspect anything fishy.

Secure infrastructure

Any solution you choose needs to be powered by strong technology and secure processes. N-able Take Control helps keep things safe via:

- Key agreements: Take Control changes the normal process of remote connections. Instead of opening a listening port, both the technician's machine and the end user's machine get session keys from one of our intermediary cloud servers.
- Resiliency and redundancy: Beyond the security element, our cloud server architecture is designed to promote maximum uptime via redundant servers. If network traffic can't go through one server for whatever reason, our systems will route the traffic to another. Additionally, traffic remains encrypted end- to-end, making it difficult (if not impossible) to snoop in on communications.

In short, we include multiple safeguards in our infrastructure to help keep you and your users secure while using Take Control.

Secure encryption and keys

Next, you need to consider the security of the data you'll work with. Encryption is an absolute must—both in transit and at rest.

N-able Take Control offers several features meant to keep data safe:

- Elliptic- Curve Diffie–Hellman (ECDH): The ECDH protocol creates cryptographic keys between two parties. This public/private key exchange allows the viewer and the agent to connect securely each time a session gets created (which is a vast improvement over leaving a port open like in an RDP-based solution). Additionally, ECDH protocols offer performance improvements over other encryption schemes. The ECDH algorithm uses shorter keys than most cryptographic protocols yet retains the strength of longer keys. This is part of how Take Control retains high performance and speed without compromising security.
- Advanced Encryption Standards (AES) 256 Encryption: We also use a maximum-security implementation of AES 256-bit encryption on data to help keep data secure both in transit and at rest. However, we add more layers to this as well. To decrypt data used in storage, the system uses both the AES 256 algorithm and your password. This adds another layer of security to protect your data and that of your customers.
- FIPS (140-2) OpenSSL®: We also use FIPS 140-2 certified OpenSSL modules to help keep sessions safe from prying eyes via advanced cryptographic protocols and packet signing techniques.

Secure sessions

Each individual session requires its own security mechanisms be built in. N-able Take Control has you covered here, too.

For starters, you can set the system to automatically delete clipboards used by technicians after each session. If they've stored sensitive data like passwords or configuration information, the system will automatically wipe this information so no one can exfiltrate it after the fact. Additionally, PINs automatically expire after each session, which can help with insider threats. You can most likely trust your employees, but it's always better to err on the side of caution. Plus, this can provide a little extra comfort to your customers.

Additionally, you can set timeout controls for idle sessions. However, even if you don't enable this feature and leave a session open, cybercriminals would still have a hard time listening in. With the ECDH protocol mentioned in the previous session, cybercriminals would have an extremely difficult time decrypting the network traffic.

Finally, it's worth noting that only authorized users can open remote support sessions (and as we mentioned in section one, we have several safeguards in place to help keep system access secure). Plus, each attended support session—or a session where both the technician and the end user are involved—requires its own unique PIN. This helps prevent people from reopening sessions.

N-ABLE TAKE CONTROL: BUILT FOR SECURE REMOTE ACCESS

Remotely connecting to a computer is one of the most invasive operations a technician could perform. You gain access to a computer's inner workings. You can tunnel into the computer, gain access to all their files, drivers, apps, and all their data. You can send scripts that make deep changes to the system without them even knowing. That's a lot of power for one person (or multiple technicians) to have.

As businesses increasingly expect their service providers to keep them secure, MSPs must make sure the tools they use are up to the challenge. N-able Take Control is built to help you keep your customers secure—and allow you to provide them peace of mind in the process.

Learn more about Take Control by visiting n-able.com.

About N-able

N-able empowers managed services providers (MSPs) to help small and medium enterprises navigate the digital evolution. With a flexible technology platform and powerful integrations, we make it easy for MSPs to monitor, manage, and protect their end customer systems, data, and networks. Our growing portfolio of security, automation, and backup and recovery solutions is built for IT services management professionals. N-able simplifies complex ecosystems and enables customers to solve their most pressing challenges. We provide extensive, proactive support—through enriching partner programs, hands-on training, and growth resources—to help MSPs deliver exceptional value and achieve success at scale.

n-able.com

[1] "Cyber Actors Increasingly Exploit the Remote Desktop Protocol to Conduct Malicious Activity," Federal Bureau of Investigation Internet Crime Complaint Center (IC3). ic3.gov/media/2018/180927.aspx (Accessed April 2019).

[2] "Samsam Infected Thousands of LabCorp Systems via Brute Force RDP," CSO. csoonline.com/ article/3291617/samsam-infected-thousands-of-labcorp-systems-via-brute-force-rdp.html (Accessed April 2019).

[3] "2018 Cost of Insider Threats: Global," Ponemon Institute. observeit.com/cost-of-insider-threat/ (Accessed April 2019).