
THE ULTIMATE GUIDE
TO THIRD-PARTY REMOTE ACCESS
SECURELINK

Could Third-Party Remote Access Be a Network Security Threat?

At Risk of a Network Attack

It used to be that industries were only at a risk of being targeted by hackers, or data thieves, if they were in the financial sector, or if they could be exploited in order to seize financial or credit data (e.g. credit card, social security numbers, or bank account information). This is no longer the case and has not been for some time. No industry or sector is safe, from banks or retail stores, healthcare providers and hospitals, to local infrastructure or government services and every sector or entity in between. Malicious attackers are looking for any outlet to infiltrate, extort, manipulate, and harm their targets. More and more, the weakest attack surface is a third-party vendor's remote access.

What is a Third Party?

A third party is any entity external to a company, typically referred to as a vendor, partner, or business associate. In their annual report, the Ponemon Institute speaks of a third-party ecosystem. They define this ecosystem "…as the many direct and indirect relationships companies have with third parties..." Most businesses, no matter the size, use third-parties for essential business-critical solutions. In short, a third party are any external business-critical service provider retained by an enterprise or institution.

Third-Party Remote Access is Essential

Third-party remote access solves problems for both vendors and companies needing access to networks or services. Most day-to-day business as we know it would cease to function without some level of third-party remote access, such as remote desktop access. However, it is risky for an enterprise or institution to allow full or unlimited access permissions to a network, especially, as indicated by the Ponemon study, data breaches caused by unsecured third-party access not only on the rise, but at an all-time high.

No company operates alone.
Third-parties are essential.
Third-parties are a risk.

Third-Party Remote Access Challenges

The Ponemon Institute's 2017 annual report acknowledged that third-party relationships are necessary to fulfill business obligations and critical-functions. However, their research underscores that both vendors and enterprises have difficulties preparing and maintaining security measures that would otherwise prevent data breaches and other malicious attacks. The study revealed that at least 56 percent of the respondents experienced a third-party data breach—a seven percent increase from 2016. Malicious attackers will almost always use the path of least resistance. This is all too often a third party's VPN account or privileged remote access.

Enterprises

A third party's need for access varies. Perhaps they require access to your servers to monitor a network-active heating or cooling solution? Maybe they need to sign in to help an individual user install software on a personal workstation? A third party could even be a partner office in a vast healthcare network that needs access to a patient's records. Whatever the need is, the necessity to allow a third party access is undeniable. Because of this, it is imperative that you understand the risks.

Vendors

Vendors are often targets of attacks because they often serve many industries. Vendors must consider their methods of access because they are often subjected to guidelines: Be it a healthcare business associate's HIPAA guidelines, a retail vendor's PCI guidelines, or a government contractor's FISMA guidelines, compliance always matters.

If a bad actor is lucky enough to successfully infiltrate a vendor's network, then they may gain access to all of the organizations the vendor serves. As data breaches continue to rise, third-party vendors find themselves requiring more stringent security protocols. When providing remote services for any number of clients, it is best to ensure your technicians do not leave an opening for unwanted activity.

Mitigate Risk

The concept of having someone remotely jumping into an application in order to make a quick upgrade during odd hours or without complex chain-of-command checks, is tempting due to its convenience. However, it opens up a world of risk. The only solution here is rigorous protection. These protections should be implemented and managed in protective software that allows for scheduling and auditing.

For Enterprise

1. **Understand** the growing business perception of third-party remote access. Impress potential clients and outperform competitors by demonstrating proactive security measures.
2. **Define** the attack surface of your application. Know all the entry points into the system, as well as when and where data can be extracted.
3. **Adopt** a realistic security information plan. Know who is connecting to the network and how they are connecting. Educate all employees and vendors of your new plan and enforce adoption. Use two-factor authentication.
4. **Control** the access to your network. Use least-privilege access, give third-party vendors only the access to the resources they need to perform.
5. **Audit** the actions of users on your network. This solution should track granular actions of any authorized users on a server.

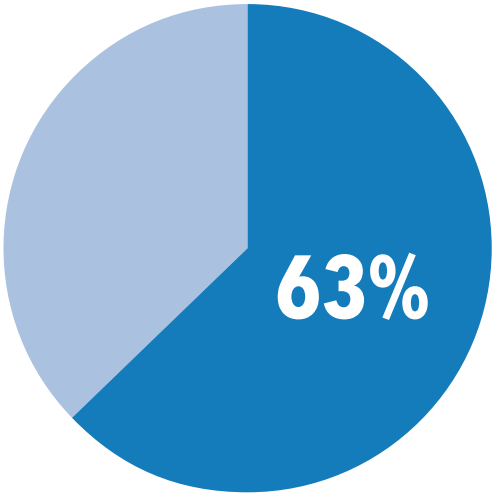
A defender must never fail.
An attacker need only succeed once.

For Vendors

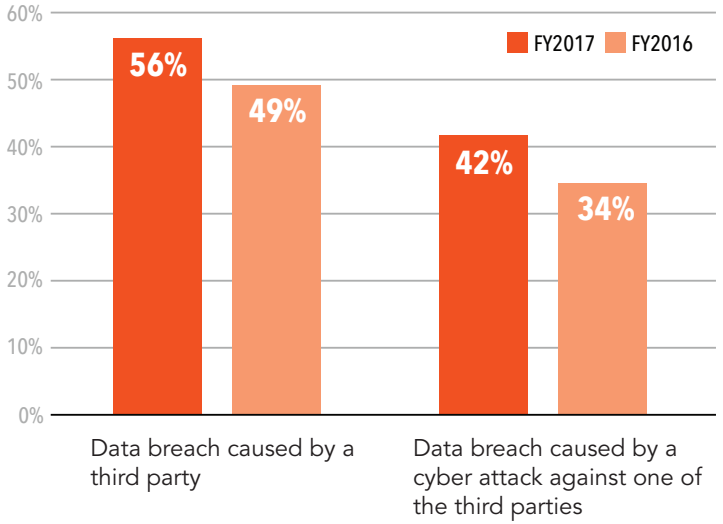
1. **Regulate** your access and stay in compliance with whatever guidelines your industry is held to: e.g. HIPAA, FISMA, PCI. All have strict standards that would be affected if your access is compromised.
2. **Consider** using a standardized and secure remote access platform to satisfy security requirements for all of your clients and substantially reduce the risk to your clients' networks.
3. **Eliminate** risk. More and more, in highly regulated industries, the liability for data breaches is being pushed to vendors and business associates. Remain compliant. Reduce your liability.
4. **Deliver** fast services and improve customer acceptance. Strive to be secure, efficient, and scalable. The more standard your security, the less time to deploy.
5. **Authenticate.** Managing login credentials for your employees demonstrates a commitment to security. Set a protocol in place that uses a confidential, unique, and multi-factored method for authentication that ensures your assigned technicians–and only your technicians–have remote access to your clients' networks.

The only difference between being hacked and third-party remote access is permission.

Data breaches caused by third party failures[1]



Data breach or cyber attack caused by a third party[1]



Mind Your Guest List When it Comes to Third Parties

If you work with a third party who needs to connect to your network from an external location, some type of third-party remote access service is necessary. The trick is to ensure that the third party that shows up isn't a party-crasher. Any visitor to your network needs to be an invited guest there to perform a critical task who leaves after they've completed their work. This means they should be identified, governed, and only granted the access necessary to perform the role listed on their invitation. Moreover, seek out a service with an auditable trail, containing a record of all of the third-party user's actions while they were within your network.

Third parties are not employees so it is important to implement a third-party remote access solution that does not provide the same level of access as your employees. Avoid adding third-party vendors or contractors to internal access databases like AD or LDAP and providing VPN access.

VPN is the key to the stable, the armory, the vault, the castle, and the kingdom. It is not recommended for third-party remote access. Why give access to the kingdom to those who only need access to the armory?

If users are sharing credentials or using less secure means to obtain access they are effectively hacking your network.

[1] Data Risk in the Third-Party Ecosystem, Ponemon Report, 2017.

Pay Attention to Your Network and Application Access

Surely you've heard the horror story where the police tell a scared babysitter that they've traced the terrifying phone call and "the call is coming from inside the house!" Well your network is the house and third parties may be handing the menace the phone.

Understanding Unrestricted Access

Never let anyone onto your network when all they need is application access.

Let's say your smartphone needs an update but you don't have the time or energy to complete the update. So you hire a technician to install the update, but synchronizing updates proves difficult so you agree to leave the location of your spare house-key with this technician so that they can gain access the phone you left at home. This way the technician can gain access to the phone without you having to take the time to be there. Sure the technician is trustworthy, but what if he is scatterbrained? So this technician jots down the location of your spare key so that he doesn't forget. But then he leaves this information out for anyone to discover.

Ultimately there's no way for you to know this has happened until it is too late, you obtained service and have moved on to the next project. Until several months pass and now maybe you notice leftovers have gone missing from the fridge? A few weeks later you discover a priceless heirloom is missing, and before you know it the house has been emptied and you're asked to pay a ransom to regain your property.

> Never let anyone onto your network when all they need is application access

If that seems dramatic, be assured that it is not. In January of 2018, a ransomware attack against Hancock Health Center was reported and eventually traced back to unauthorized access due to poor third-party remote access security, not before Hancock Health had to pay around 47,000[2] using bitcoin.

According to news reports[3], the hackers gained access to the system by using the hospital's remote-access portal and logged in with a third-party vendor's username and password.

[2]http://www.healthcareitnews.com/news/hancock-health-pays-47000-ransom-unlock-patient-data
[3]http://www.healthcareitnews.com/news/ransomware-attack-hancock-health-drives-providers-pen-and-paper

Perceptions about Third-Party Access[4]

EXPECT MORE BREACHES

While 62% of respondents didn't believe their organization was vulnerable to an attack from third parties, 79% expect their competitors have or will suffer a serious data breach in the future.

LOTS OF MOVING PARTS

75% agree they have to touch 5 to 14 network and application components when adding new external user groups.

WHO'S ACCOUNTABLE?

But only 8% thought they might lose their job if a data breach occurred during their watch.

A majority thinks their competition is vulnerable, and that same majority feel that they are not. This is a very risky coin toss.

[4]Data Risk in the Third-Party Ecosystem, Ponemon Report, 2017.

Managed Access

Because most security protocols and methods of access have been designed for employees, or internal privileged remote access, the only solution here is rigorous protection. These protections should be implemented and managed in protective software that allows for scheduling and auditing. Grant application access rather than network access to better ensure the safety and security. If you hold true to the lessons above, your security teams can minimize the potential of a security attack stemming from an untrusted remote user.

Have a realistic authentication policy and plan ahead.

Ultimately you will want to ensure that all of your third-party access is controlled by a consistent formula for reliable identification, up-to-date credentialing, and multi-factor authentication. Consider time as well. Managing AD permissions and access for a vast network of, sometimes temporary, third-party users requires valuable IT time that can be better served elsewhere. Find a solution that does not overwhelm your internal resources.

Segmenting provides the right amount of access where you need it. Third-party vendors are not typical users and should be treated accordingly. Third-parties should have just enough access to perform their designated responsibilities and nothing more. Through great policies and segmented access, you ensure that vendor access is focused on the job at hand. This prevents you from violating strict requirements found in regulatory compliance guides (e.g. HIPAA or PCI).

Set up specific access for each third-party vendor. It is always a best practice to ring-fence third-party access, restricting permissions to only the application that they need to be connected to rather than your entire network.

Policy-based approaches enable networking teams to segment permissions by access to internal applications instead of having to allow access to network segments by IP address or access control lists. Ring-fencing using unique credentials allows a layer of control not found in many other access methods. For instance, if the employee leaves the company, simply removing their unique credential from the system triggers all policy controls and revokes permissions and access to the applications on the network. To increase security measures further, add two-factor or multi-factor authentication to each login and ensure that when a unique user signs on they are exactly who they say they are.

With non-unique credentials, there is no way to prevent third-party vendors from sharing a single username and password amongst an indeterminate amount of users. If you cannot hold a third-party user accountable, then they are likely to take the easiest path to access. This is the path that will be exploited when hackers attack your network. A password is only as secure as the sticky-note it is scribbled on.

It is recommended administrators insist that third-party users are assigned logins associated with their unique email address. That way if a user stops working at the vendor company, their work email can be deactivated and their access revoked.

The solution of a unique business email-based login is often a preferred solution for third-parties as well, as emails are easily authenticated among their local AD or LDAP services.

According to the 2017 Ponemon Report "Data Risk in the Third-Party Ecosystem."

Less than half of all respondents surveyed said managing third party risks were a priority.

IT IS RECOMMENDED ADMINISTRATORS INSIST ON UNIQUE LOGIN CREDENTIALS, THE BEST OPTION IS TO REQUIRE YOUR THIRD-PARTY USERS USE LOGINS TIED TO THEIR UNIQUE BUSINESS EMAIL ADDRESS.

The average number of third-parties with access to confidential or sensitive information has increased by 25% since 2016.

Only 17% rate their effectiveness in mitigating third party risk as highly effective.

Ensure Visibility: Third-Party Access Management

Imagine a third-party user needs access to your network to perform routine maintenance. If you provide VPN access, or full RDP access, it effectively opens a tunnel to your network. If the provided access credentials were shared, or phished, this unrestricted access can be used by bad actors–as evidenced by the continued uptick in harmful breaches (such as the Jan, 2018 breach of Hancock Health).[5]

It's not if a third-party will be responsible for a network breach... it's when. Take control of your network.

Third-party access management is crucial for complete oversight. Know what happens when, and what was performed by whom. With the proper policies in place you can meticulously schedule access, set access permissions, and control who has access; when coupled with proper auditing you can view all of this activity at any time.

Be convenient, but maintain control

Discuss your secure remote access solution with your vendors. Both vendors and enterprises should avoid the liability of unsecured open access solutions such as a WebEx desktop sharing solution or VPN. These are designed for internal solutions, not third-party remote access. Instead, select a dedicated third-party solution featuring unique email-based authentication, flexible enough to limit access to the necessary services your third-party requires while retaining speed and ease of use.

A password is only as secure as the sticky-note it is scribbled on.

THE JOURNEY OF A SHARED LOGIN:

A third party will typically request access; usually VPN, WebEX, or another form of remote access designed for use by off-site employees.

The vendor technician or technicians are assigned credentials and permissions for access by internal IT. This is generally managed in AD.

A vendor technician services many accounts so they often note their varied credentials in a digital file, on their whiteboard, or on several sticky-notes.

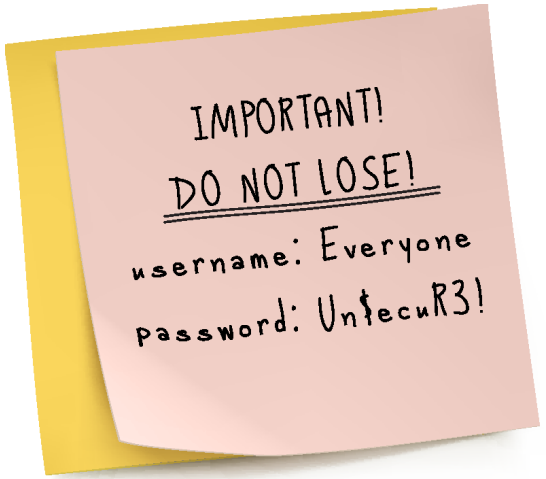
Another technician needs first-time access to the client systems or forgets their credentials.

Rather than request access through their channels, they seek out a peer or co-worker who is known to have credentials.

This co-worker then shares the credentials, often jotting them down on a sticky-note so that their peers have them at the ready whenever they need access.

The credentials are then passed around indefinitely. Even after the original authorized user has long left the vendor's employ.

[6] https://usat.ly/2DsqAhe



No More Shared Credentials

Access should be restricted to need-to-know access. It is not a good practice to simply provide a third-party vendor with a password and hope it isn't shared or accidentally compromised. Sharing usernames and passwords, or allowing any level of internal access (such as VPN), should absolutely never occur. Instead, use a secure remote access service to grant access to third parties.

As a vendor manager your technicians may be sharing credentials and exposing you to liability without you ever realizing it. Technicians need to get work done quickly, and often will circumvent the long process of AD authorization or access request procedures in order to quickly complete a task. Ensure that credentials are never shared and that you remain compliant with all regulations.

Auditing: For Peace of Mind, and Oversight

A truly secure third-party remote access solution should track the granular actions of any authorized users on a server. Great auditing gathers detailed log files about each sign on event, and for GUI interactions (like remote desktop sign ins), a video log should be added to the audit parameters. These files provide valuable forensic and diagnostic benefits. It is easier to discover bad-actors or unauthorized access when you have comprehensive logs.

An audit should also contain access notifications which alert administrators when sign-on activity is taking place without the need to install additional agents or software.

Choosing the Right Access

There are many ways to access a network or allow access to your network. Your organization likely identifies you and your access permissions by using a variety of identity management tools. Oftentimes third parties are allowed the same authentication methods as employees. This is not a good business practice. Sharing tools such as remote desktop, VPN, and WebEx are ideal solutions for internal employees, but poor for third-party access.

Most remote access solutions will use authentication based on username and password log-in method Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP). It is possible, and recommended, to employ additional compliance and risk reduction methods including Two-Factor Authentication (2FA), and Multi-Factor Authentication (MFA) to improve the security of many remote access methods.

A brief overview of many of the more common terms typically used in the conversation around remote access may better help you in your search for a secure remote access solution.

Internal Access (IA)
Typical enterprise network access solution. Think about the way most employees interact with your internal network.

Virtual Private Networks (VPN)
Initially developed to behave similarly to IA, the goal was a solution that allowed remote employees access as if they were on site. Typically, VPNs require secure remote authentication.

Active Directory (AD)
Active Directory most often simply just AD, was developed by Microsoft for Windows Server. AD is often thought of as a scalable, more secure, network resource management solution. Active directory requires "forest-based" database maintenance which requires an administrator. User access permissions are regulated within this database.

Lightweight Directory Access Protocols (LDAP)
LDAP is a directory access protocol. It is a mechanism used to connect with, search, and modify Internet directories. You may ask yourself what the difference is between LDAP and AD. Think of it this way AD is a database, and LDAP is a means of communicating with it.

Remote Access Dial-In User Service (RADIUS)
RADIUS is a ubiquitous technology often used by internet companies to manage access. Many gateways that allow internet or network access have some sort of RADIUS server running to manage authentication.

Remote Desktop Protocol (RDP)
The most common remote access method, RDP was developed by Microsoft as a proprietary graphical interface to allow connections to another computer. In order to take advantage of this both the client and server must have RDP protocol deployed. Clients exist for most GUI operating systems (e.g. Windows, or Mac OS). Additionally, there are RDP server clients for Unix and OS X Server. This connection is akin to having direct access to the computer you are connected to as if you were sitting right in front of it.

About SecureLink

SecureLink is a pioneer and leader in third-party remote access. For highly-regulated enterprise organizations, SecureLink Enterprise is the only purpose-built secure remote access platform to identify, control, and audit third-party vendors. For technology vendors, SecureLink for vendors is the gold standard remote access platform because it is easy, efficient, and helps reduce liability when supporting customers. For both enterprise and vendors, a SecureLink solution is the most secure option for third-party remote access.

securelink.com - 888.897.4498 - contact@securelink.com