The ultimate guide to remote support for enterprise technology vendors

The ultimate guide to remote support for enterprise technology vendors

CONTENTS

How technology vendors are leaving the door open to enterprise security threats

ARE YOU AT RISK OF A CYBERATTACK?

In the past, the most at-risk industries targeted by cybercriminals were those in mission-critical sectors like healthcare and finance. In today's world, hacking is an equal opportunity threat, with virtually every industry feeling the heat.

From retail and healthcare to local infrastructure and government agencies, so many organizations have reported that they have received an unprecedented number of threats in recent years in the form of cyberattacks, security breaches, and ransomware. Bad actors are looking for any portal to extort, manipulate, and harm their targets. And more and more, they're accessing the data through you, the technology vendor.

Four out of five CEOS report they've been a victim of a cyberattack via a third party.[1]

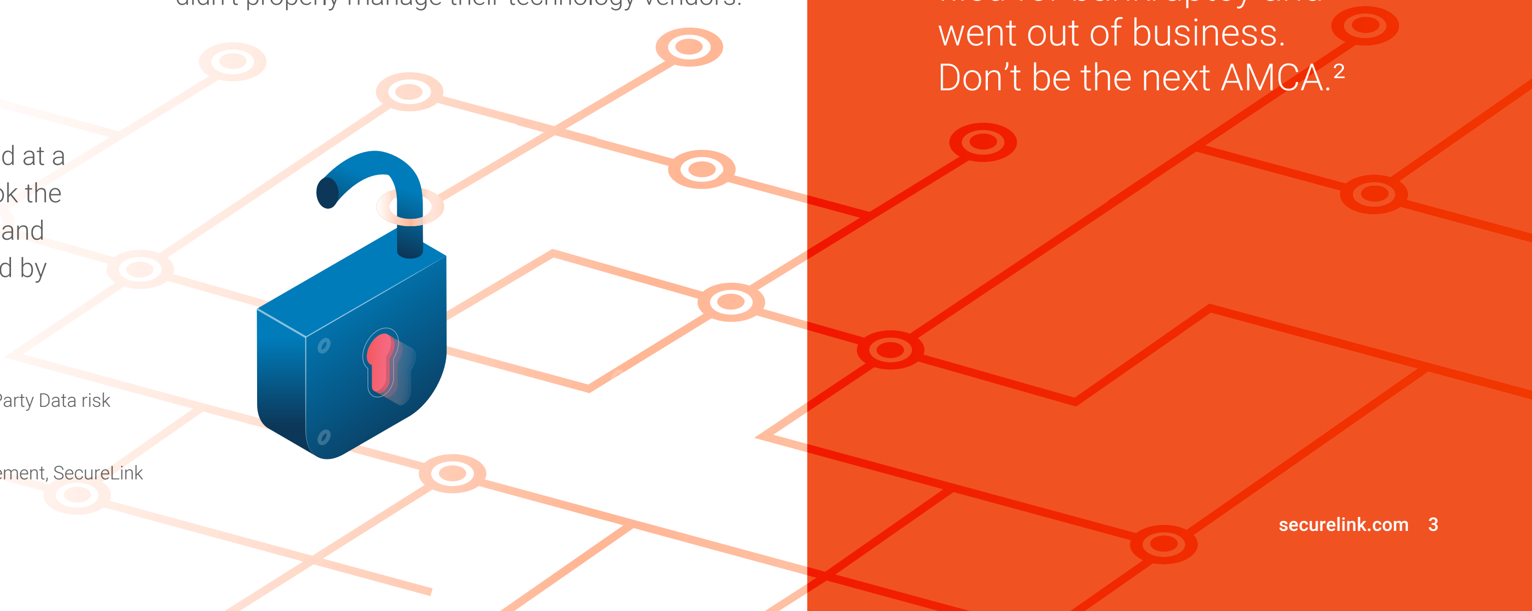
POINTING THE FINGER

Typically, when a major data breach occurred at a company, it was the enterprise itself that took the fall. Think of high-profile breaches at Target and Equifax. The 2014 Target breach was caused by an HVAC vendor, and Equifax blamed its 2017 breach on a flaw in an external software platform it was using. It blamed a malicious download link on its website on yet another vendor.

The public and the media didn't care who was at fault, whether it was Target itself or one of the thousands of technology vendors they have in place. But times are changing, and the vendors responsible for breaches are increasingly in the spotlight. It's no longer just the enterprise affected during a third-party data breach, but the technology vendor associated with the cyberattack.

The truth is, when it comes to pointing the finger at the guilty party, it's typically the systems that are in place, not the vendor who became the access point, nor the enterprise customer who didn't properly manage their technology vendors.

If you don't believe us, let's think about a recent example with AMCA, the vendor used by a couple of well-known medical organizations like Quest Diagnostics and LapCorp. Today, Quest Diagnostics and LapCorp, the enterprises, are still around and doing business. We, unfortunately, cannot say the same for AMCA. Soon after the breach, AMCA filed for bankruptcy and went out of business. Don't be the next AMCA.[2]



[1] Opus and Ponemon Institute Announce Results of 2018 third-Party Data risk Study, Businesswire

[2] Embracing cybersecurity for better vendor access risk management, SecureLink

The real cost of a breach: It's more than just money

The fallout from the rising security breaches is significant. It can cost the enterprise dearly in terms of customer loss, reputation damage, and regulatory penalties.

A data breach costs a U.S. company over $8 million, more than twice the global average.[3] What's worse, the financial losses to an enterprise are, on average, higher when the breach occurs via a third-party provider.[4] Now customers are changing how they manage their technology vendors, requiring providers to invest in higher liability coverage levels or find a better, more secure platform for remote access. For you, the technology vendor, the impact of a data breach attached to your name can be deadly, leading to fines, reputation damage, and, most critically, the loss of your customers' loyalty. If a bad actor infiltrates your network successfully, they may gain access to all the organizations you serve, which has even led some technology vendors to file for bankruptcy.

Remember AMCA? In 2019, Retrieval-Masters Creditors Bureau, the parent company of AMCA, filed for Chapter 11 protection after an eight-month system hack breached the personal, financial, and health data of up to 20 million Quest Diagnostics, LabCorp, and BioReference patients.[5] Do we have your attention yet?

[3] Cost of the average U.S. data breach is $8 million, Axios

[4] Cost of a Data Breach Report 2020, IBM Security

[5] AMCA Files Chapter 11 After Data Breach IMpacting Quest, LabCorp

THIRD-PARTY REMOTE ACCESS IS ESSENTIAL

As a technology vendor, you are indispensable to your customer. The fact is, most day-to-day businesses could not exist without some level of third-party remote access.

What does this mean for you, the technology provider? As a vendor, you probably work off-site and require remote access into a network to support an enterprise technology. You may have dramatically scaled up your VPN connections to support your remote technicians and prevent disruption to client services. However, you have dozens, if not hundreds, of customers to support, requiring you to use multiple remote access solutions to meet your customers' needs.

THE TROUBLE WITH VPNS AND DESKTOP SHARING ALTERNATIVES

Hackers exploit known vulnerabilities in VPNs and other remote access platforms, including desktop sharing tools and consumer video conferencing apps. If you don't securely manage this network access, your vulnerable surface area grows.

In addition to the vulnerability of VPNs, they are cumbersome and challenging for the end-user to manage. Without a standardized remote access tool in place, you and your team are reliant on a customer-provided solution. With hundreds of customers and support representatives to manage, each with their own login and credentials, this system is arduous, at best. Gaining initial access and setup from your customer can be lengthy, and it depends on the customer's IT team's availability to create an account.

The result?

1. Precious time lost for resolving issues.

2. Your reps, eager to complete the mission at hand, are more likely to share passwords amongst themselves than wait for customers to grant access.

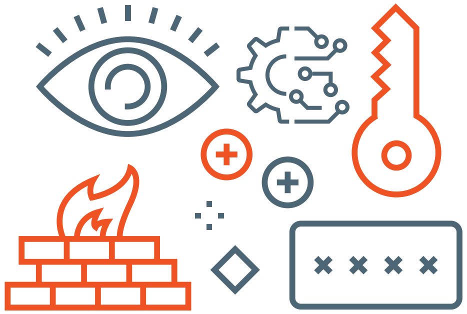
3. While your people are waiting for that customer to coordinate attended access, you may end up paying your technicians overtime.

The Ponemon Institute Cyber Risk Report found that misuse or unauthorized sharing of confidential data by third parties was the second -biggest security worry for 2019 among IT professionals, with 64% of the tally.[6]

MITIGATING RISKS: THE SOLUTION FOR VENDORS IS RIGOROUS CONTROLS

Relationships between vendors and enterprise organizations are growing exponentially, even as high-stakes breaches make headlines weekly. To prevent a data breach, every organization, from the enterprise to the technology provider, must take the necessary steps to protect themselves, their customers, their data, and their reputation. The answer: adopt a protective remote access platform that allows for scheduling and auditing.

> Despite the high risk of a breach through a supplier, 77% of respondents said they had limited visibility into those vendors.[6]



[6] Supply chain attacks show why you should be wary of third-party providers

Four best practices to reduce your exposure to a data breach

FOR VENDORS AND ENTERPRISES

The Enterprise

Only 17% of enterprises rate their effectiveness in mitigating third-party risk as highly effective.[7]

DEFINE THE ATTACK SURFACE OF YOUR REMOTE ACCESS APPLICATION

Know all the entry points into the system, including when and where data can be extracted.

PERFORM DUE DILIGENCE

Before choosing your technology vendor, be sure to research and understand their security policies and protocols. Without clear visibility into remote networks and third-party systems, it can be hard to know if a current or potential vendor may be vulnerable or compromised. Routinely review your vendors' protocols, monthly or quarterly. This task can be difficult for complex organizations that have thousands of vendors to manage without a standardized platform.

MAINTAIN COMPLETE ACCESS CONTROL

Employ the same role-based permissions to your technology vendors as you do internally. You hired the vendor, but not each of their reps—you need complete control, all the way down to the individual. Employ a remote access solution that limits each user's access to ONLY the systems they need to perform their job.

AUDIT ALL USER ACTIVITY ON YOUR NETWORK

Your remote access platform should track access of any authorized users on a server on a granular scale.

For Vendors

The number of third parties with access to confidential or sensitive information has increased by 25% since 2016.[7]

REGULATE YOUR REMOTE ACCESS

And, what's even better, is that you will be compliant with your customers' mandates no matter the industry.

USE A STANDARDIZED REMOTE ACCESS TOOL

This will satisfy security requirements for all of your clients and substantially reduce the risk to your clients' networks.

DELIVER FAST SERVICES AND IMPROVE CUSTOMER ACCEPTANCE

The more standardized your security, the less time it will take your customer to respond.

AUTHENTICATE

Managing login credentials for your employees demonstrates a commitment to security. Use a confidential, unique, and multi-factored authentication method that ensures your assigned technicians have remote access to your clients' network.

[7] Data Risk in the Third-Party Ecosystem, Second Annual Study, Ponemon Institute

The challenges of current remote access methodologies

- **Inefficient and time-consuming remote access to provide support**
- **Increasing security demands from enterprise customers and compliance requirements**
- **Greater exposure due to unlimited customer access and increasing cyberattacks**

INEFFICIENT AND TIME-CONSUMING REMOTE ACCESS TO PROVIDE SUPPORT

Without a standardized remote access solution, a vendor is dependent on customer-provided solutions. Managing these disparate platforms for hundreds or even thousands of customers, each with unique logins and credentialing, is untenable and difficult.

- This decreases the efficiency of access and increases the time to resolve large and small issues.
- If your tech reps are accessing systems via attended access (TeamViewer, LogMeIn, etc.), they may need to coordinate with customer schedules, which increases the time to resolve an issue and requires you to pay them overtime pay.

Vendors that use SecureLink typically see a 65% reduction in time spent managing and supporting remote access.[8]

[8] ROI Calculator for technology vendors, SecureLink

INCREASING SECURITY DEMANDS FROM ENTERPRISE CUSTOMERS AND COMPLIANCE REQUIREMENTS

Customers want to know what steps their technology vendors are taking to protect their information and networks. Many of these customers are now requiring vendors to complete questionnaires and risk assessments around how they handle remote support. Imagine completing a form or two for each of your hundreds of customers.

Compliance doesn't apply solely to the enterprise. Increasingly, business associates are subject to the same compliance with industry regulations that the enterprise is. This includes HIPAA, CJIS, SOC2, and many others. Current remote access solutions make it difficult to demonstrate and ensure compliance. You need proof of access in the form of an audit trail.

GREATER EXPOSURE DUE TO UNLIMITED CUSTOMER ACCESS AND INCREASING CYBERATTACKS

If something goes wrong within a customer environment, it can be challenging to prove that the technology vendor didn't cause it. Without granular tracking and auditing of all access, the provider may be held accountable for something that wasn't their fault.

Role-based access is a critical issue for technology providers who are using traditional remote access methods. If your reps have access to more than they need to do their jobs, you are further exposed to the threat of cyberattack.

An easy-to-implement standardized remote access tool will change your business for the better.

The right remote access solution will deliver a standardized platform with increased visibility for both the customer and the vendor. And it will help you surpass your customers' demands and expectations.

A STANDARDIZED PLATFORM

One of the biggest struggles for technology vendors is that they use multiple products per customer, and keeping track of them all can be daunting. Standardization allows you to use one platform to connect to all customers which decreases time spent connecting and having to remember what tool is used for what client.

INCREASED VISIBILITY

As a vendor, you shouldn't be responsible for your customer's network credentials. With the ability to connect by literally clicking a button, you gain confidence in knowing you could not be the reason for a privileged credential- related breach. Role-based access enables you to provide all the access your reps need without the struggle, and credential storage is secure, so you don't need to know passwords.

EXCEEDING CUSTOMER DEMANDS AND EXPECTATIONS

Because the number of vendor breaches continues to rise, highlighting only the enterprise's missteps, customers today expect a new level of security and accountability. The way to accomplish this is to provide an audit trail. Audit trails can make all the difference when it comes to retaining current customers and winning new ones.

Compliance is mission-critical

The importance of maintaining compliance requirements for your customers and your own business concern cannot be overstated. Regardless of industry, noncompliance can cause your customers to pay fines and lose their own clients. Enterprises are increasingly seeking visibility into the vendors' activities and access.

COMPLIANCE CAN BE COMPLICATED AND EXPENSIVE

Requirements by regulatory agencies have never been broader and more stringent than they are today. The EU's General Data Protection Regulation (GDPR) has been described as a "261-page beast," and the California Consumer Privacy Act (CCPA) is packed with requirements — some more extensive than the GDPR — for ensuring that consumers have control of their own data: specifically, what data a company has collected from them, and how it's being used.

> The average compliance cost for organizations across all industries worldwide is $5.47 million.[9]

GDPR compliance applies to all companies that collect personal information from European citizens, not just those based in the EU. GDPR fines are up to 4% of total global revenues.[10]

Most industries have dozens, if not hundreds, of disparate regulatory rules and requirements that businesses must deal with, with some CISOs reportedly spending 30% or more of their time dealing with compliance issues.[11]

Despite the intensive staff-hours and tens of millions of dollars spent on compliance, over 90% of businesses have systemic IT weaknesses that leave them vulnerable and potentially noncompliant.[12]

Regulations like GDPR and CCPA have prompted companies to get much more serious about privacy and better understand where their data "lives"—how it is processed, stored, and used. As companies have become more reliant on a network of collaborators to get things done, the attack surface for cyber intruders has grown. Increasingly, security breaches reveal trails that lead back to the technology vendor. Regulators are focusing more and more on how companies manage outsourcing in general; as regulatory agencies train a sharp eye on companies' compliance, companies are sharpening their focus on their vendors.

[9] The True Cost of Compliance, Corporate Compliance Insights

[10] General Data Protection Regulation (GDPR): What you need to know to stay compliant, CSO

[11] Awash In Regulations, Companies Struggle With Compliance, Forbes

[11] Despite spending more on compliance, businesses still have basic IT weaknesses, Help Net Security

CREATE AND MAINTAIN A CULTURE OF COMPLIANCE

To show customers you take security and compliance seriously, it's essential to create a “culture of compliance” among your own employees and team members. The ability to provide your customers with compliance records can go a long way toward gaining loyalty and market share within your target industry.

AUDITING: FOR PEACE OF MIND AND OVERSIGHT

A truly secure remote access solution will track the granular actions of any authorized users on a server via an audit trail. An audit trail is a journal of every action taken with your data, including creation, modification, and deletion of records, and a sequence of automated system actions.

Effective auditing gathers detailed log files about each sign-on event, delivering priceless valuable forensic and diagnostic benefits — and peace of mind — for your customer. With greater control and security via masked credentials, plus a comprehensive audit trail, your customer is more likely to approve access and respond to communications quickly. Most importantly, this level of detailed documentation limits your liability and provides definitive documentation of work done, complete with keystroke logs. Beyond the obvious benefit of an audit trail— success and business continuity — having an audit trail helps ensure you adhere to compliance requirements.

CONVENIENCE, WITH CONTROL

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

THE JOURNEY OF A SHARED LOGIN:

You or a member of your team request access: typically VPN, WebEX, or another form of remote access designed for use by off-site employees.

Your tech is assigned credentials and permissions for access by the customer’s internal IT team.

Your technicians service many accounts, so they often note their varied credentials in a digital file, on their whiteboards, or on multiple sticky notes.

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

Rather than request access through their channels, the tech seeks out a peer known to have credentials.

This co-worker then shares the credentials, 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, long after the original authorized user has left the vendor's employ.

No more shared credentials.

Receiving a password from your customer and hoping it isn't shared or accidentally compromised is no longer acceptable. Access between your customer and your team should be restricted to need-to-know access.You should be using a secure remote support platform to access the networks of your customers.

Choosing the right access

Your goal is to resolve customer issues in a timely manner and maintain customer satisfaction. You require a solution that will maintain or increase customer satisfaction by providing support and resolving problems quickly and efficiently. In short, you require a remote access solution that can balance your need for security, efficiency, speed, and cost-effectiveness. A standardized remote support platform will satisfy security requirements for all of your clients' networks.

Before settling on the ideal remote access solution, consider these critical aspects:

- **Security and compliance:** Will it meet internal security, customer security, and compliance requirements? Does it limit exposure and decrease liability?
- **Usability for your support reps:** What is the learning curve? Does it fit into your current processes and allow your reps to provide support quickly and easily?
- **Infrastructure requirements:** Will the solution fit into your current infrastructure? What is the burden of maintenance on the IT team? How much effort is required for implementation?

BE PROACTIVE, NOT REACTIVE

The goal: Be proactive rather than reactive when it comes to data security in relation to third-party risk. Unfortunately, many vendors don't self-police their security protocols or document their responses regularly, leading to significant breaches and steep fines.

As a vendor, vetting yourself will go a long way in establishing your credibility among covered entities. Vendors should have clear procedures in place for protecting sensitive information and identifying and anticipating threats and vulnerabilities. These actions and responses should be documented and ready to demonstrate to covered entities who need your expertise.

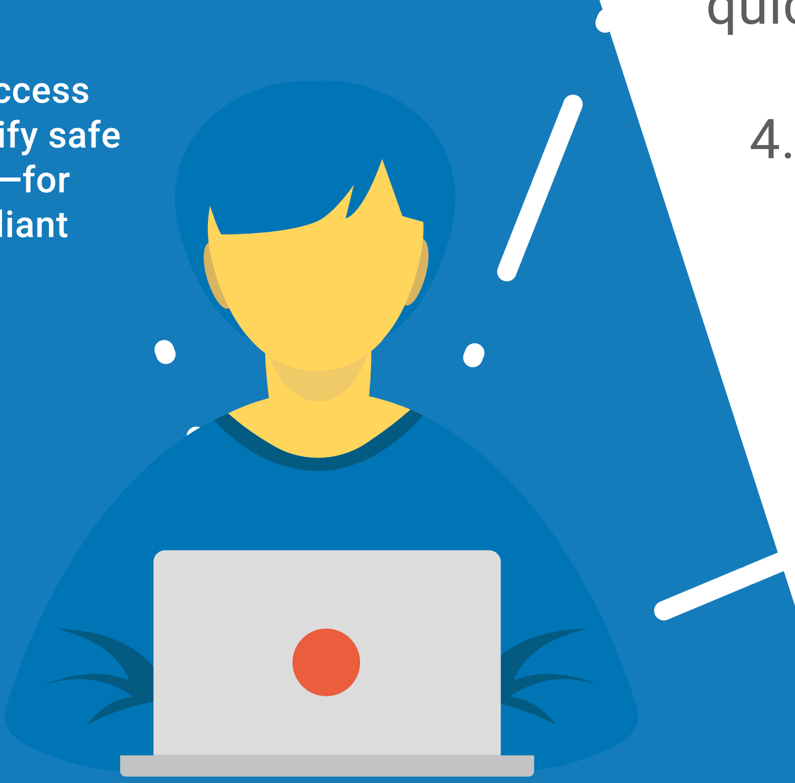
High-risk vendors often lack established or formally documented methodologies to prioritize and address identified risks.[13] The right remote access solution is a single, standardized platform that allows for both attended and unattended support, securely and efficiently. With greater control and security via masked credentials, your customers will have greater peace of mind and willingness to approve access. Best of all, you, the vendor, will have a single point to access your customers.

> Vendors that use SecureLink typically see a 75% reduction in time spent establishing remote connections with customers.[8]

[13] Third-Party Vendors Behind 20% of Healthcare Data Breaches in 2018, Health IT Security

Top 5 benefits of standardizing remote support.

A standardized remote access tool will simplify and fortify safe access to your customer—for fast, effective, and compliant productivity.



1. Shore up the gaps in VPNs and VPN alternatives to increase security.
2. Meet compliance requirements for you and your clients.
3. Increase efficiencies with quicker time to resolution.
4. Lower IT support costs.
5. Protect your reputation and your customer's revenue.

1

Shore up the gaps in VPNs and other remote support tools to increase security.

Nearly half of all data breaches can be attributed to a third party.[14] With a standard remote access solution, you can:

Ensure multi-factor authentication with a time-based one-time password (TOTP) mobile authentication application, email verification, and SMS two-factor authentication.

Grant granular least-privileged access to the user, tied to specific hosts and application port.

Set a specific window of time in which a user can receive access.

2

Meet compliance requirements for your customer — and your own operation.

Compliance with industry standards is essential for vendors: it ensures your customers don't incur penalties, and it guards both your reputation and theirs. Demonstrating that you take protecting your customers' data seriously can lead to higher customer retention and future revenue. A standardized remote access tool will:

Generate detailed audit records that document who accessed the system, actions and keystrokes they performed, specific files accessed, and time logged on and off.

Enable admins to assign, mask, and pass credentials for uses connecting to a system.

View credentials in detailed audit reports generated through the platform.

3

Increase efficiencies with shortened time to resolution.

With nearly half of all vendors relying on multiple platforms to access individual client networks, management can quickly get out of hand. This increases time to resolution and lowers customer satisfaction. Choose a single, integrated platform to support all of your clients. To minimize complexity, your remote support platform should:

Support easy access to client networks for all authorized employees and contractors wherever they work.

Gain client trust by standardizing your remote support in a single platform that offers a consistent user experience for both the vendor and client.

Eliminate disruptive patching and upgrade cycles for multiple remote access tools.

[14] Nearly half of firms suffer data breahces at hands of vendors, Help Net Security

4

Lower IT support costs

With a single platform, all changes can be deployed automatically, which allows IT to spend time on more valuable client services, like updating credentials requirements and installing security upgrades on multiple solutions. To help lower support costs, your remote support platform should:

Eliminate the manual collection of system logs and utilization data.

Efficiently provide remote support by enabling technicians to securely connect, control, and collaborate precisely where and when needed.

Automate routine maintenance and monitoring tasks.

5

Protect your reputation and your customer's revenue.

Data breaches not only erode client trust; they create endless work for your internal teams who need to contain the damage, prevent it from happening in the future, and rebuild the client relationship (if possible). To help prevent breaches that can expose client data, the SecureLink remote support platform will:

Assign users role-based access that provides the least-privileged with granular permission controls.

Prevent breaches by employing FIPS-validated cryptographic modules that use, at a minimum, AES 128-bit ciphers for all.

Encrypt audit data at rest at 256-bit AES.

*Vendors that use SecureLink see a 1% increase in revenue on average through improved customer service and visibility into service levels.[8]

The bottom line about remote support

Standardized operations practices result in more efficient access, quicker time to resolution, and increased customer satisfaction. Standardization of all remote access into a single view for each vendor rep saves time and increases efficiency. Shorter resolution time results in higher customer satisfaction.

- Vendors are being held accountable for data breaches more often—don't allow your access to be the reason your customer gets hacked.
- Make your job easier: A standardized remote support platform can save you hours, plus your sanity.
- Enjoy the peace of mind that comes with having an accurate audit trail for meeting compliance requirements.
- Close more cases in less time than with desktop sharing alternatives.

CONTINUED EDUCATION.

As a vendor who needs to service customers remotely, the tool you use to access customer networks can either introduce high-risk complexities or provide a streamlined solution that promotes inter-departmental efficiency and success. Download our remote support checklist to see how the right remote support tool can meet your client's needs, increase efficiency, and create more growth opportunities for you and your business.

About SecureLink

Headquartered in Austin, Texas, SecureLink is the leader in third-party security, providing secure third-party remote access for both highly regulated enterprise organizations and technology vendors. SecureLink solves and secures the greatest point of risk in the third-party lifecycle for more than 30,000 organizations worldwide, providing companies across multiple industries, including healthcare, manufacturing, government, legal, and gaming, with secure remote access with identity management, access controls, audit, and compliance assurance.

Securelink.com| 888.897.4498| contact@securelink.com