Top 5 benefits of standarizing remote support

Companies of all sizes rely on technology vendors for additional business support of all kinds — from performing routine maintenance to specialized tasks. While vendors and contractors offer unique capabilities and flexibility, they can also expand the threat landscape for the client.

As a vendor, it's up to you to ensure all of your support reps can securely access client systems not only to minimize your exposure, but to build client trust and preserve your reputation.

Here are the five key benefits of using a standardized remote support tool to establish a secure, efficient, and cost-effective way of doing business.

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

Roughly 50-60% of data breaches can be attributed to a third party such as vendors, business associates, and contractors. [1] Many of these connectivity solutions are targeted and frequently breached by hackers who gain entry to client systems without the vendor discovering the breach until after the damage has been done.

To ensure more secure access, your remote support platform should:

- Ensure multi-factor authentication through any time-based one-time password (TOTP) mobile authenticator application, email verification, and SMS two-factor authentication.
- Grant granular least privileged access to the user, tied to specific hosts and application ports.
- Include a defined time period users will be enabled before access is granted.

02 Meet compliance requirements you and your clients are subjected to

Compliance with industry standards is essential for vendors to ensure their clients don't face fines or other consequences while ensuring you're both trusted and reputable. Plus, demonstrating you take protecting your customers' data seriously can lead to higher customer retention and future revenue
.

To simplify compliance, your remote support platform should:

- Generate detailed audit records that include who accessed the system, actions and keystrokes they performed and which files were accessed, and time logged on and off.
- Enable administrators to assign, mask, and pass credentials for users connecting to a system.
- View credentials in detailed audit reports generated through the platform.

03 Increase efficiencies with quicker time to resolution

With nearly half of all vendors relying on multiple platforms to access multiple client networks, management can quickly get out of hand. [2] This causes increased time toresolution and lowers customer satisfaction. Now's the time to 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 on a single platform that offers a consistent user experience on both the vendor and client sides.
- Eliminate disruptive patching and upgrade cycles for multiple remote access tools.

04 Lower IT support costs

IT can spend more time on maintenance tasks such as updating credential requirements, installing security upgrades on multiple solutions, and more. With a single platform, all changes can be deployed automatically, which allows admins to spend time on more valuable client services.

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 they're needed.
- Automate routine maintenance and monitoring tasks.

05 Protect your reputation and your customer's revenue

Data breaches not only erode client trust, but they can 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 minimize complexity, your remote support platform should:

- Assign users role-based access that provides least privileged access with granular permission controls.
- Prevent breaches by employing FIPS-validated cryptographic modules that use, at minimum, AES 128-bit ciphers for all.
- Encrypt audit data at rest at 256-bit AES.

1. Third-party breaches are a threat — and many companies aren't ready
2. Third-Party Remote Access: Challenges for Enterprises and Technology Vendors

imprivata

Imprivata is the digital identity company for mission- and life-critical industries, redefining how organizations solve complex workflow, security, and compliance challenges with solutions that protect critical data and applications without workflow disruption. Its platform of interoperable identity, authentication, and access management solutions enables organizations in over 45 countries to fully manage and secure all enterprise and third-party digital identities by establishing trust between people, technology, and information.

For more information, please contact us at 1 781 674 2700
or visit us online at www.imprivata.com

CPAM-infographic-top-5-benefits-remote-support-0124