NTR support

NTRsupport Security Fact Sheet

NTRglobal delivers remote support solutions that incorporate the most advanced security technologies. NTRsupport uses multilevel security measures to ensure the absolute protection of customer and support representative data in every support session. Some of the many mechanisms that we employ to safe guard your remote support sessions are:

HIPAA Compliance

NTRsupport meets the HIPAA privacy and security regulations for storage and transmission of PHI through state of the art security measures, including 256-bit AES end-to-end encryption and hashing of personal data such as logins and e-mail addresses.

TRUSTe Compliance

NTRglobal is a TRUSTe licensee and complies with TRUSTe's stringent privacy policies, which prohibit unauthorized disclosure of personal or corporate information to any third party. TRUSTe is an independent, nonprofit organization whose mission is to build user trust and confidence in the Internet by promoting the use of fair information practices.

State of the Art Encryption

For maximum security, NTRglobal uses 256-bit AES (Advanced Encryption Standard) end-to-end data encryption as well as industry standard protocols like SSL to ensure that your data is protected. All live session transactions, including text chat, images, audio, video, desktop sharing and file transfer are completely secure.

Login and Password Security

NTRsupport uses strong password authentication and limits access to all of its applications through logins and passwords. Passwords are hashed and encrypted and never travel across the internet. The login process utilizes a “three strike” rule to temporarily block an ID when an incorrect password has been entered three times in a row. In addition, you may limit logins to specific IP ranges either on an individual or group basis, thereby restricting Operator and Administrator access to NTRsupport. To comply with internal password policies you may also define the strength of a password and the frequency with which it must be changed.

NTRsupport features can only be accessed according to the permissions assigned by the Administrator to each Operator. For example, an Administrator can decide which Operators have access to features like co-surfing or remote control, and can further limit the available control modes to allow observer or demonstration mode (where one user can see yet not interact with another desktop).

Administrators can also require that Operator and end-user sessions use an SSL connection regardless of the browser mode selected by the user, thereby ensuring that transport layer encryption is utilized for all transmissions.

Safe Connectivity

NTRsupport utilizes TCP packets and standard ports and is compatible with firewalls and proxy servers that perform network address translation (NAT). Connections can be established through a local area network (LAN) or any other Internet connection. This means that an Operator may be working outside the organization or from another country without a VPN connection and still connect to the company's NTRsupport service via a browser to provide remote support to any other Internet-connected PC or Mac.

Chat features are 100% Web-based, using only JavaScript and HTTP protocols over standard Web ports 80 or 443. Remote control sessions can be established using peer-to-peer connections within the same network or via the NTR bridge server over standard ports. NTRsupport Administrators can also to assign a specific port to an Operator.

Automatic Footprint Removal

At the end of each remote control session, all active components of the remote control session are automatically removed from the end-user's machine, thereby preventing any unauthorized future access.

Authorization and Access Control for Remote Support

Remote control sessions are always encoded with 256-bit AES end-to-end encryption standards. NTRsupport always prompts customer approval before initiating any on-demand remote support or monitoring session. Once permission has been granted by the customer, support professionals can view a customer's computer as if they were sitting right in front of it.

During a remote support session, the customer can terminate screen sharing or screen viewing, decline downloads or file transfers and regain control of the desktop at any time. This ensures that the customer always has ultimate control of his or her own machine.

Secure Application Selection

Using the Application Selection feature, the user whose desktop is being remotely controlled can select from a list of all applications which are available to be viewed or used. This feature allows both the support representative and the customer to restrict remote control to a specific application or group of applications when either of them is reluctant to allow the other full visibility or control.

Change of Viewing Direction Only After Explicit Permission

You may change the viewing direction or the remote control mode without disconnecting entirely from the customer. However, each mode or direction change requires the customer to grant approval, therefore it is only possible with the customer's explicit permission.

Blocking Users

To protect Operators from harassment or unwanted users, NTRsupport includes a blocking feature that allows Operators to temporarily block, and Administrators to permanently block certain users from accessing Operators. The site Administrator manages this blocking feature and can also identify the unwanted user's IP.

Highly Secured Data Center

NTRsupport servers are housed in state of the art, world class data centers that are totally dedicated to hosting mission critical Internet applications. These facilities apply the strictest measures and best practices to ensure the highest levels of security and availability. Among these are 24 x 7 network monitoring, restricted site access via access cards and biometric devices, fire suppression highly redundant connectivity, power and environmental controls to ensure that servers are continually available and always operating under optimal conditions.