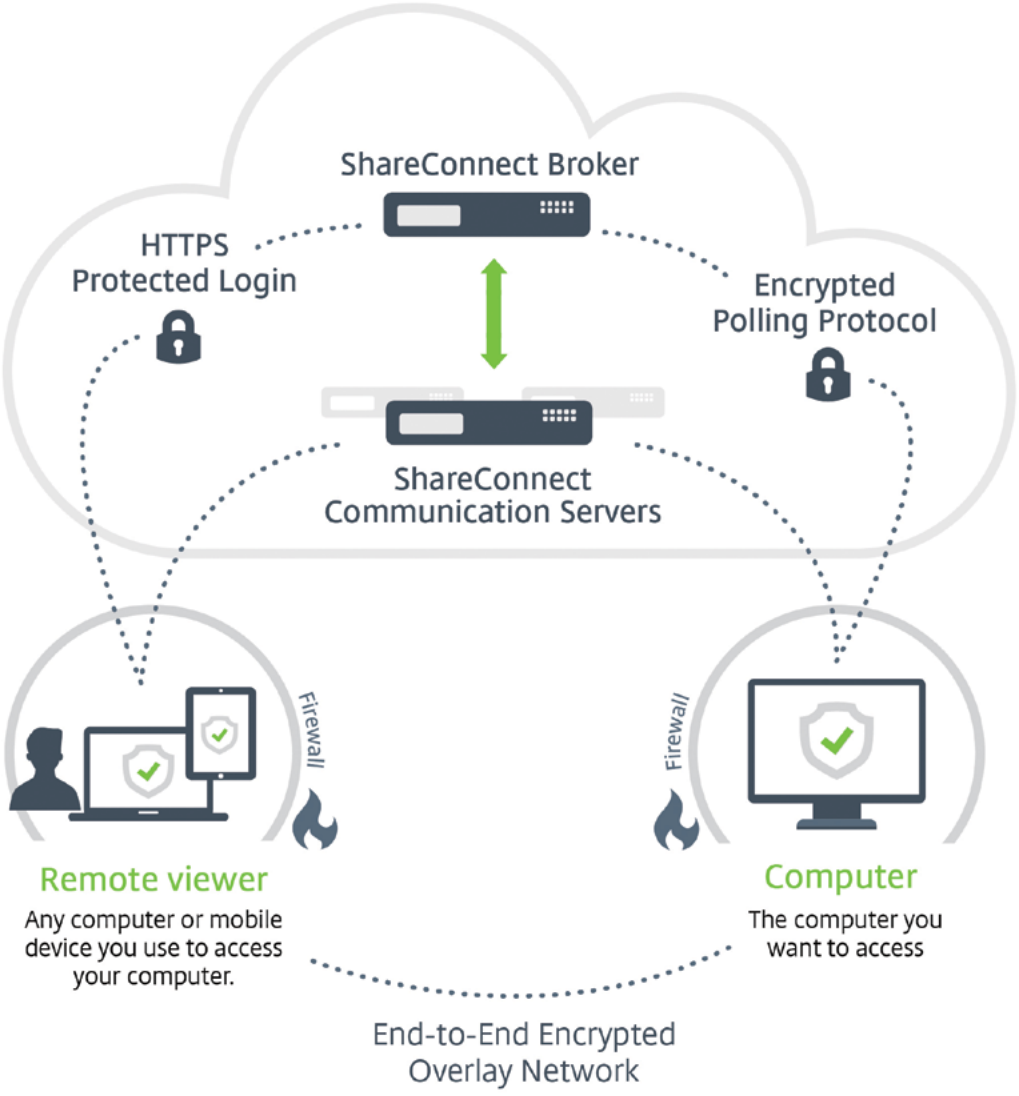
The Security Basics of Citrix ShareConnect

Citrix ShareConnect provides top security that's fast, reliable and simple to use when remotely accessing desktop computers from another computer or mobile device.

Security when using a computer for work is of utmost importance today. That's why Citrix ShareConnect provides a solution built for business that allows for total freedom and access while it maximizes confidentiality, integrity and protection.

At Citrix, we have designed ShareConnect to be secure from the ground up. With decades of experience running secure applications like GoToMyPC and ShareFile, we understand the importance of security and have built ShareConnect with this in mind.

ShareConnect has four main components that interact with each other to provide the user access to his or her data and apps, as shown below.



Computer

With ShareConnect, a small agent is installed on the computer to be accessed. Typically, this is a home or office computer with continuous Internet access. This host computer registers and authenticates itself with the ShareConnect broker.

Viewer

From the ShareConnect app on an iPad or Android tablet, a user clicks to connect to a computer, sending an SSL-authenticated, encrypted request to the broker. Alternatively, the user may connect with a HTML5 enabled web browser by visiting the secure ShareConnect.com website, entering a user name and password and clicking a button for the desired computer.

Broker

The broker is a matchmaker that listens for connection requests and maps them to registered computers. When a match occurs, the broker assigns the session to a communication server. The computer maintains a persistent connection with the broker. This allows ShareConnect to know which of your computers are online and connected to the Internet and can initiate file and app access when needed.

Communication server

The communication server is an intermediate system that relays an opaque and highly compressed encrypted stream between the client device and host computer for the duration of each ShareConnect session. Protecting the integrity of users' data and the privacy of sensitive information is of utmost concern to anyone. Whether you're using ShareConnect for business or personal use, security is essential.

Security at multiple levels

Citrix delivers ShareConnect using a SaaS model designed expressly to ensure robust and secure operation while integrating seamlessly with a company's existing network and security infrastructure.

Secure facility

Highly secured worldwide datacenters host all ShareConnect web, application, communication and database servers. We restrict physical access to servers, and other strict security measures protect the Citrix network operations center.

Secure network

Citrix access routers watch for denial of service attacks and log denied connections. Two firewalls provide multi-layer perimeter security: one between the Internet and web servers, another between the ShareConnect broker and back-end databases.

Secure platform

Citrix servers run on well-tested Linux servers. We regularly monitor and test our service infrastructure for vulnerabilities and continuously conduct audits on our system logs for suspicious activity.

Secure administration

Authenticated and encrypted connections administer Citrix servers.

Scalable and reliable infrastructure

The Citrix infrastructure is both robust and secure. Redundant routers, switches, server clusters and backup systems ensure high availability. For scalability and reliability, switches transparently distribute incoming requests among Citrix web servers. For

optimal performance, the ShareConnect broker load balances the client/server sessions across geographically distributed communication servers.

Protection for customer privacy

Citrix understands about the importance of privacy and has a strong privacy policy that prohibits unauthorized disclosure of personal or business information to any third party. You can review the ShareConnect privacy policy at https://www.shareconnect.com/privacy-policy. This policy identifies what information is collected, how it is used, with whom it is shared and how customers can control the dissemination of information.

Disclosure of customer information

To deliver service, Citrix must collect certain user information, including first and last name, email address and account-level passwords for ShareConnect. Unless expressly authorized, Citrix will not disclose this confidential information to any third party or use this information in any manner other than to deliver agreed upon services and as otherwise provided in the ShareConnect Privacy Policy.

With its users' express consent, Citrix sends service update messages to its users at the email addresses they provided when requesting the service. Even when ShareConnect is accessed from a public computer, data left behind poses no privacy threat. ShareConnect stores remote machines login credentials and other information in the iOS and Android apps using the keystores that comply with the operating system security standards. If the user logs out of the app, all data stored about that user is deleted.

ShareConnect uses an optional cookie to track traffic patterns and retrieve registration information. This cookie holds a unique number generated at the time of registration, but it does not contain any personally identifiable information or passwords. Users can block this cookie if desired.

After a session ends, browser history will indicate that ShareConnect was accessed — but information in the history cannot be used to access the account or any computer without a complete set of credentials, including the user's login and password and (optionally) a one-time password.

Access to customer information

Limited access is granted to certain Citrix employees on a need-to-know basis for the express purpose of customer support. Citrix uses session logs to maintain quality of service and assist in performance analysis. ShareConnect tracks domain names, browser types and MIME types for traffic management. However, this data is gathered in the aggregate and is never correlated with an individual user or company account.

Detailed connection logs

The ShareConnect broker logs additional information for each connection, including the last user access time, type of browser (user agent), download status for the viewer, communication server ID, who closed the connection (server/client/broker/session

timeout), a close error code and the build number of the computer. This information is intended to aid problem diagnosis; access is limited to Citrix customer support on an as-needed basis.

Traffic and credential privacy

ShareConnect communication servers relay traffic between the client browser and host computer in encrypted packets. Citrix or anyone else cannot decipher this traffic.

Digitally signed applications

You install ShareConnect by visiting the ShareConnect website and downloading the installer there or by using the link in the email sent to install ShareConnect. The server software is permanently installed on the host computer.

Most security parameters are preset and do not need to be configured by end users, such as blanking the computer screen and locking the keyboard during or after access sessions to prevent keystroke capture attacks. Users are always responsible for setting their own passwords, thereby ensuring end-user privacy.

Protection for confidential data

ShareConnect uses a highly compressed, encrypted stream to ensure data confidentiality without sacrificing performance. All traffic between the ShareConnect client and host computer is protected with end-to-end 128-bit Advanced Encryption Standard (AES) encryption in Counter Mode (CTR).

Strong encryption keys

Even a strong cipher is vulnerable if it does not use strong, confidential encryption keys. ShareConnect generates unique secret keys for each connection derived using a zero-knowledge, public-key-based protocol called Secure Remote Password (SRP). The key components needed for this SRP are uniquely generated for each session and securely distributed to computer and client by our broker.

Protection against message replay and modification

Data packets include a sequence number to prevent any attempted message replay attack. These packets carry highly compressed binary data that are framed in a proprietary protocol and encrypted with AES. Packets also carry an integrity check to ensure no tampering has occurred. These packets cannot be modified without changes being detected by the recipient.

End-to-end authentication

Whenever a client connects to the host computer, they authenticate each other, using a shared secret known as an access code generated for a one-time use and transmitted only to the viewer and host computer. Citrix servers never store this access code.

ShareConnect uses the SRP protocol standard for end-to-end authenticated key agreement between the viewer and host. This patented, well-reviewed protocol provides outstanding cryptographic strength, performance and resilience against a wide range of potential attacks. For more information, visit http://srp.stanford.edu/.

Inactivity timeouts

Users sometime walk away from public

computers without logging out and leave home computers unattended. ShareConnect addresses these threats by applying inactivity timeouts. This feature automatically disconnects users from ShareConnect if their SSL connection is inactive for 15 minutes. .

Keyboard and mouse locking and screen blanking

To ensure that the user's data and activity is private even if someone is physically present at the computer site that is being accessed, every ShareConnect access automatically blanks the computer's screen that is being accessed and lock the keyboard and mouse. The computer is also locked when the user disconnects from ShareConnect so that no one can take over that computer use.

Data flow and ports used

Sessions are initiated only through outgoing HTTP/TCP to ports 80, 443 and/or 8200.

Direct connections

Once the user is authenticated and connected, ShareConnect attempts to establish a direct connection between the client and host, bypassing the ShareConnect communication server whenever possible to increase the connection speed and improve in-session performance. The Direct Connections feature instructs both the client and host to listen for a limited time for incoming connections and also to attempt outgoing connections to each other; whichever signal arrives first establishes the connection.

The client and host then proceed to execute an SRP-based authenticated key agreement and establish an end-to-end secure connection. Should the direct connection be blocked or interrupted, the previously established connection through the communication server maintains the communication.

Firewall compatibility

ShareConnect is firewall friendly. Because most firewalls are already configured to permit outgoing web traffic, you do not have to bypass or compromise your corporate or branch office firewall or your remote worker's firewall to implement secure access through ShareConnect.

Many other solutions require servers to receive incoming packets at a public IP address. The ShareConnect host establishes a persistent TCP connection to the broker (poll.shareconnect.com) that allows it to be notified if any connect requests have been received. The host will attempt to keep the connection open by sending TCP "keep alive" packets approximately every 60 seconds. This makes ShareConnect completely compatible with application proxy firewalls, dynamic IP addresses and network/port address translation.

Please note that some firewalls may block Direct Connections or give you a warning message asking for your permission to allow it, because it creates an incoming connection at one point. This does not limit ShareConnect's compatibility with firewalls; if Direct Connections is blocked or interrupted, the connection will simply automatically continue

through the communication server via outgoing signals.

Also, because ShareConnect is firewall friendly, you can use it with computers at your company without creating a headache for your IT team.

Security with simplicity

The Citrix recipe is straightforward: Start with a secure hosted service and operational practices that preserve customer privacy. Protect access connections with state-of-the-art encryption to keep users' information safe. The end result is that ShareConnect offers a simple and seamless end user experience while maintaining the level of security that is needed in today's corporate workplace.
Ultimately, we believe that users should have access to their data, apps and devices when they need to, and corporations should feel comfortable in enabling their employees to be productive by providing this type of access that is built on a strong foundation of experience and continuous innovation.

To learn more about how ShareConnect can let your business get more done on the go, visit our website at www.ShareConnect.com.

Corporate Headquarters
Fort Lauderdale, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

EMEA Headquarters
Schaffhausen, Switzerland

India Development Center
Bangalore, India

Online Division Headquarters
Santa Barbara, CA, USA

Pacific Headquarters
Hong Kong, China

Latin America Headquarters
Coral Gables, FL, USA

UK Development Center
Chalfont, United Kingdom

About Citrix
Citrix (NASDAQ:CTXS) is a leader in virtualization, networking and cloud services to enable new ways for people to work better. Citrix solutions help IT and service providers to build, manage and secure, virtual and mobile workspaces that seamlessly deliver apps, desktops, data and services to anyone, on any device, over any network or cloud. This year Citrix is celebrating 25 years of innovation, making IT simpler and people more productive with mobile workstyles. With annual revenue in 2013 of $2.9 billion, Citrix solutions are in use at more than 330,000 organizations and by over 100 million people globally. Learn more at www.citrix.com.