



A CONNECTED WHITE PAPER

Connected Subscription Service Security Overview

March 10, 2003

Connected Corporation
100 Pennsylvania Avenue
Framingham, Massachusetts 01701
www.connected.com

© 2003 Connected Corporation

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of Connected Corporation. The information in this document is subject to change without notice and should not be considered a commitment by Connected Corporation. While Connected has made every effort to ensure the accuracy and completeness of this document, it assumes no responsibility for the consequences to users of any errors that may be contained herein.

Some software products marketed by Connected Corporation and its distributors contain proprietary software components of other software vendors.

Connected and SendOnce are trademarks and DeltaBlock is a registered trademark of Connected Corporation. All other marks are property of their respective owners.

Contents

Connected Security Overview.....	1
What is Connected Subscription Service?	1
Connected Subscription Service: Security	2
Understanding Key Security Aspects of Connected Subscription Service	3
Backup and Retrieve Session Security.....	3
Archival Security.....	3
Network & Firewall Security	4
Client Account Security.....	5
Administration Security.....	5
Connected Security Integrity.....	6
Connected Uptime – Mirrored Data Protection.....	6
Summary & Conclusion	8

Connected Security Overview

The majority of corporate data originates with PC users. Regardless of where your corporate data is created – inside your firewall or out on the road, Connected has the ability to capture and store this vital information, while dramatically reducing storage costs.

It is not enough, however, that Connected back up the data. PC data that's being backed up and stored must be secure from outside threats. Connected provides the data protection Subscription Service solution that truly and comprehensively protects the PC data that belongs to your organization.

Connected follows rigorous standards to keep your data safe and away from others. Many of these standards are security best practices, while others were developed by Connected to reinforce these best-practice security measures. The bottom line: Connected Corporation takes data protection very seriously – we have gone to great lengths to protect this data from all credible threats.

This document serves as an introduction to the security measures put in place within the Connected data protection architecture to prevent unauthorized access or damage to Connected customer data relative to physical access, via the Internet, via dial-in access, or by Connected employees. Connected provides security at every level of the Connected Subscription Service from backup through storage through data retrieval.

What is Connected Subscription Service?

In short: Connected specializes in off-site data protection and storage of PC data. Connected's Subscription Service solution is a client-server system that enables file backup for personal computers over any TCP/IP network. Data is stored at a central server cluster managed by Connected Corporation at Connected facilities or at Connected Partner facilities.

The Connected Agent is a small, lightweight application that runs on every PC in an enterprise or business to manage backups and enable: retrieval of data, scheduling and backup, and transaction logs.

Patented data reduction technology enables even large backups to take place in minutes. The software provides effective PC backup and recovery, even at connection bandwidths as low as 28.8 kbps. Connected Subscription Service provides a level of security for the user's data better than, or comparable to, alternative practices for handling computer data.

Connected Security Lifecycle

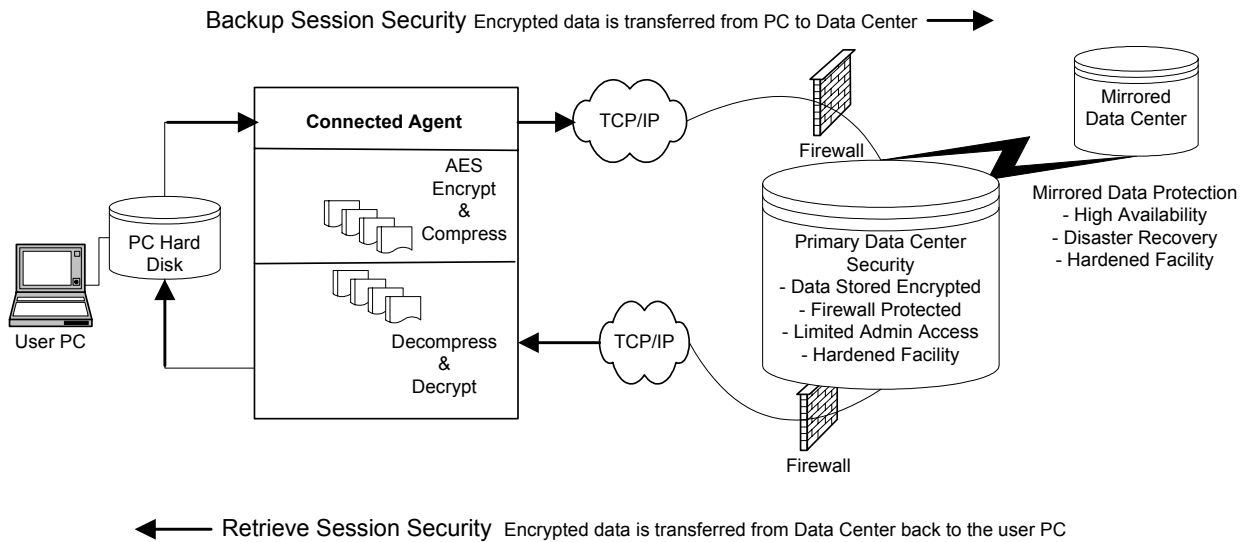


Figure 1. Connected Subscription Service maintains security at all levels of the data protection process. Data enters the process encrypted and is stored encrypted at the Data Center. Only when the user is authenticated, can the data be retrieved, decrypted and restored at the user PC.

Connected Subscription Service: Security

In the Connected Subscription Service client/server architecture, the client Agent is responsible for initiating backups; the Data Center servers are responsible for managing the data and keeping this data secure. The following sections illustrate how Connected creates a secure environment for data transfer, storage and manageability.

Connected's security design objective is four-fold:

1. Prevention of unauthorized parties from gaining access to users' data during transfer over the Internet – **Backup & Retrieve Session Security**
2. Prevention of unauthorized parties from gaining access to users' data on the server – **Archive/Data Center Security**
3. Prevention of unauthorized parties from deleting users' data from the server - **Administrative/Client Account Security**
4. The physical security practices and building hardening that creates **Connected's Security Integrity**

Understanding Key Security Aspects of Connected Subscription Service

Backup and Retrieve Session Security

At the core of the Connected Agent is the backup engine. This piece of the Agent enables all backup and retrieval behavior at the client level. At the time of backup, the Agent scans the PC's disk, and determines what data to send to the off-site, highly available, mirrored Connected Data Center servers.

Backup is initiated when:

- The Agent contacts the Data Center via TCP/IP socket.
- Connection is authenticated via the user encryption key.
- Following authentication, the Agent encrypts each file flagged for backup with Triple-DES [112-bit key] or AES [128-bit key] and sends the data to the Data Center.
- The Data Center packs all the encrypted files from a given client's backup session into a single file on the server's file system, leaving the files encrypted.
- **Retrieve:**
- The Agent contacts the Data Center.
- The Agent then sends to the Data Center a list of files to retrieve.
- The Data Center transmits the encrypted files to the client, and the Agent decrypts them upon arrival and places them back on the client's disk.

A password option prompts the user to input a password prior to retrieval – using this password can prevent unauthorized persons with physical access to another person's client from performing retrieves from the server.

Archival Security

The data sent from the Agent to the Data Center is sent either in entire files or in deltas (changes to files previously backed up). Data is encrypted prior to transmission from the client PC. To prevent unauthorized parties from gaining access to users' data on the server:

-
- Connected encrypts all data with encryption algorithms
 - Triple-DES [112-bit key] and, as of Version 7.0, AES [128-bit key] (Q2/03)
 - The encrypted output is sent to the Data Center. The Data Center stores the encrypted files without decrypting them.

It is important to note that the Connected Data Center is established as a storage repository and is not part of a communications system. The Data Center servers do not provide a view to user data. As a result, in the highly unlikely event that an individual is able to gain access to users' data files on the server, that individual would not be able to view the data.

Network & Firewall Security

Network Practices

The Connected Data Center Mirror:

- Is located at an undisclosed location.
- All data received by either Data Center is immediately replicated to its mirror.
- Outages or a disaster at either Data Center do not interfere with the availability of the data or the service.
- Connected has yielded 99.99% uptime for the past seven years.

Firewall Best Practices

Connected's firewall policies do not permit access from the outside to the Data Center file servers. Thus, access to customer archive files via remote connection to the production servers is not possible via the Internet. Connected uses a designated port that is only enabled for outbound traffic. Intrusion via this port is not possible.

File Retention

To prevent unauthorized parties from deleting users' data from the servers:

- There are no commands that allow deletion in the client-server protocol.
- Administration has operational control mechanisms to prevent unauthorized access to Connected's servers.

Connected retains the 10 most recent versions of any file backed up to the Data Centers.

Client Account Security

Each installation of Connected is unique to each customer. It is this ability to customize each deployment that enables Connected to maintain its lead in the PC data protection market. Data is transferred from PC to Data Centers on a daily basis. However, the administrator can customize administration rules and retrieval of accounts. This customization extends to the customer and their administration.

Visible/Invisible Keys

Recovery of an account requires an encryption key. Encryption keys have the option of being visible to select some, all or none of the administrative team, thus putting ownership of the data into the hands of the customer. It is for this same reason that Connected has an option to either escrow or not escrow all user encryption keys.

LDAP Authentication

Connected offers LDAP authentication via the Connected Enterprise Directory Interface (EDI). In this case, Subscription Service customers are authenticated via an HTTPS connection to a centralized database of usernames and passwords. Any challenge protocols to administrative credentials are initiated through the Connected EDI.

Ticketing

The ticket method uses a file (the ticket) that contains a single-use registration code. A ticket allows a single registration to the server and is usually provided in an email that accompanies the Agent Setup program. In this model, the data encryption key is provided to each Agent, also providing full-width randomness. Therefore, the problem of users selecting weak encryption keys is eliminated.

User Account Security (File Sharing)

File Security Descriptors (FSD) are employed to ensure that each user is only able to access the data associated with his/her account or an account to which they have been granted access. The FSD limits the client PC to only access its data, the data of a particular work group, or a department's shared folder. FSDs can be set to the folder level or the file level at the user PC. File Sharing can be turned on or off at the time of deployment.

Administration Security

Password Handling

When Connected users have questions or need assistance, they will typically contact the customer's Help Desk or similar IT organization. Support Center's features and data are protected against unauthorized access - every technician must present credentials when invoking Support Center.

Designated Help Desk technicians are supplied credentials authorizing their access to Support Center. Credentials consist of a Technician ID and an associated password. Only after the technician is validated with the proper ID and password, will access be granted.

Connected Security Integrity

The Connected Data Center

Connected leases and controls the entire building which houses its headquarters and primary Data Center. Connected maintains two mirrored, secure Data Centers. Connected manages its service with the goal of 100% uptime, 24x7. This is achievable due to mirroring of the Connected Data Center.

Connected's Subscription Service is provided by a series of clusters which share a single registration server, each of which has one or more pairs of servers (mirrored). Mirrored servers are located at separate sites, which are connected by point-to-point, high-speed WAN links.

All Connected servers run Windows 2000 Server and SQL Server 2000. Connected follows Microsoft best practices and implements security patches and database service packs when released.

Case in Point: In January of 2003, the "Slammer virus" attempted to exploit security holes in MS SQL databases – specifically MS SQL Server 2000.

The vulnerability that is exploited by this worm was first corrected by a Microsoft security patch in July 2002. IT was corrected again in subsequent cumulative patches, most recently in October 2002.

Connected had implemented these security patches on our production floor, and as a result, experienced no business interruptions.

In addition to deploying all the latest Microsoft security patches, Connected uses up-to-date virus protection to disable any virus attacks that threaten the Connected Data Center.

Connected Uptime – Mirrored Data Protection

Connected's primary Data Center is located in two disparate locations. All data received by either Data Center is immediately replicated to its mirror. Outages or a disaster at either Data Center do not interfere with the availability of the data or the service. Connected has yielded 99.99% uptime for the past 7 years.

Most scheduled maintenance procedures and unscheduled outages affect only one member of a mirrored pair at a time. Mirroring practices enable Connected to service either side of the mirror without any business interruption. In the rare event that Connected must bring down both servers in a pair simultaneously, we will endeavor to do so outside normal business hours, and to give customers several days' advance notice.

Connected's Backup Network

Internet traffic volumes can cause congestion at both the server and network levels. Connected created the concept of utilizing dual redundant mirroring to alleviate Internet congestion, giving customers access to multiple servers. Traffic is load-balanced between the two sites, which eliminates degraded system performance. To further ensure access and performance, Connected utilizes multiple high-speed Internet access lines to connect the mirrored Data Center servers. Each server platform has fail over and redundancy, continuous server monitoring and performance tuning, assuring that storage capacity is never exceeded. All are purchased from multiple Internet Access Providers.

Hardening – Connected's Physical Security

Connected protects over 300 TB worth of data in its Data Centers worldwide. Access to these areas is restricted to Data Center Administrators only. Connected also takes the necessary steps to ensure that only Connected employees and signed-in guests of Connected employees can gain access to the Connected building.

- All Connected employees are issued a picture ID/card-key for entry to the building. Connected employees must display these Connected badges at all times. Card key use logs are reported and reviewed weekly.
- Access to the Data Center floor is limited by biometric-controlled entry and is reviewed monthly.

Other Data Center Security measures include:

- Internal and external closed circuit television monitoring
- Internal and external alarm systems with 24x7 monitoring and motion detection
- Generator backup (tested weekly) with unlimited capacity to run on reserve power
- Mirrors are located within a locked cage at an undisclosed location with 24x7x365 security
 - Access to the mirror is restricted to pre-authorized individuals.
 - Mirror is located on redundant power grids for increased availability in the event of a power failure.
 - A dry fire-suppression system is installed at each site.

Summary & Conclusion

As of January 2003, Connected is managing over 300 TB of data its Data Centers (mirrors).

Connected has been backing up PC data since 1995, from full-scale corporate deployments for some of the world's largest companies to small businesses. Connected recognizes and acts on the fact that protecting intellectual property is critical.

It is for these reasons that Connected takes extreme precaution in handling customer data.

- Data is encrypted at the client PC prior to transmission for session security; data is unencrypted only after data restoration is completed to the client PC.
- Data is stored encrypted at a secure, mirrored, hardened Data Center facility.
- Connected operates its Data Centers with the understanding that downtime is not an option when considering a business-critical solution.
- Best practices networking and best-of-breed routers, switches, firewalls, servers, facilities infrastructure, power grids and telecommunications circuits are all deployed with backup components to maximize Connected's fail over and redundancy.
- Disaster recovery mirroring assures that each client's data has a duplicate copy at a mirrored co-location to maintain access in the event of failure at the primary location. This effort translates into the highest levels of security, and availability of 99.99%.

This document serves as a high level overview of Connected Subscription Service. Should you be interested in learning more about Connected and our Subscription or Licensed Software data protection solutions, please contact us at **(800) 934-0956** or visit www.connected.com.