WHITEPAPER

SECURITY + INFRASTRUCTURE

Central Desktop / Updated April 22, 2015

Table of contents

Introduction

The accessibility, security and integrity of your data are integral to the success of your company and the reputation of our business. Because Central Desktop is delivered as a cloud-based Software-as-a-Service (SaaS) solution, reliability and uptime of our services are of utmost important to your business and our success.

Your data is secure with Central Desktop. The Central Desktop platform runs on a proven infrastructure designed to provide maximum security, performance and reliability.

Central Desktop partners with leading data centers Alchemy Communications and Corexchange to provide its customers and partners with state-of-the-art perimeter, network, server, application and data security to ensure privacy and availability. The data center infrastructure includes raised floors, state-of-the-art fire suppression, abundant and redundant high-speed internet connectivity, redundant power and a self-contained cooling system. We maintain two geographically separated facilities to ensure customer data security and integrity in the event of any disaster.

Business these days is global, which is why Central Desktop has partnered with Akamai, the leader in content delivery networks and global application acceleration. Central Desktop leverages the Akamai infrastructure footprint to boost application responsiveness and file transfer performance, ensuring you and your collaborators get a great experience, no matter where on the globe you are using the collaboration platform.

Central Desktop provides our collaboration platform to more than 550,000 users worldwide. Our typical customer is a fast-paced, medium-sized business organization or a team or department within a large Fortune 500 or Global 2000 company. All these organizations, regardless of size, trust and rely on Central Desktop on a daily basis.

Security overview

Central Desktop's security and infrastructure were designed to provide maximum performance and reliability with state-of-the-art physical and data security and redundancy. Central Desktop's security policy was architected with multiple layers of security, safeguards, and redundancy to ward off external security threats.

Perimeter + physical security

Central Desktop is dedicated to developing and maintaining a state-of-the-art physical site security where it hosts its data and servers. Central Desktop hosts its primary servers and data at the Alchemy Data Center in Irvine, California. The Alchemy Data Center is designed to withstand power outages, fire, intrusion and tampering, and natural disaster scenarios including an 8.3 magnitude earthquake. Central Desktop hosts its backup servers and data in a geographically separate location more than 800 miles away in Dallas, Texas at the Corexchange Data Center.

Key security features + advantages

Surveillance

Physical access to the data center is controlled and monitored 24/7 by:

- Uniformed building security services
- Video camera and electronic surveillance with intrusion detection
- Onsite 24/7 technical personnel

Authorized access only

Central Desktop only allows authorized personnel to access the physical site servers and data (including any remote, virtual or tele-access to the data center).

Authorized personnel must pass criminal and historical background checks and must sign strict non-disclosure agreements (confidentiality agreements) with regards to protecting and accessing customer data. Breaches to the agreements carry severe legal penalties and ramifications. Authorized personnel are required to pass through electronic and visual identity validation systems to enter the data center. Access to the data center is maintained by time-stamped logs for historical retrieval.

All of Central Desktop's equipment (servers, routers, switches, storage devices) is stored in securely locked cabinets and cages.

Remote access

Remote Access to the Central Desktop servers are strictly controlled and limited to authorized personnel only. Any authorized remote access is solely executed via encrypted communications.

SSAE 16 Type II

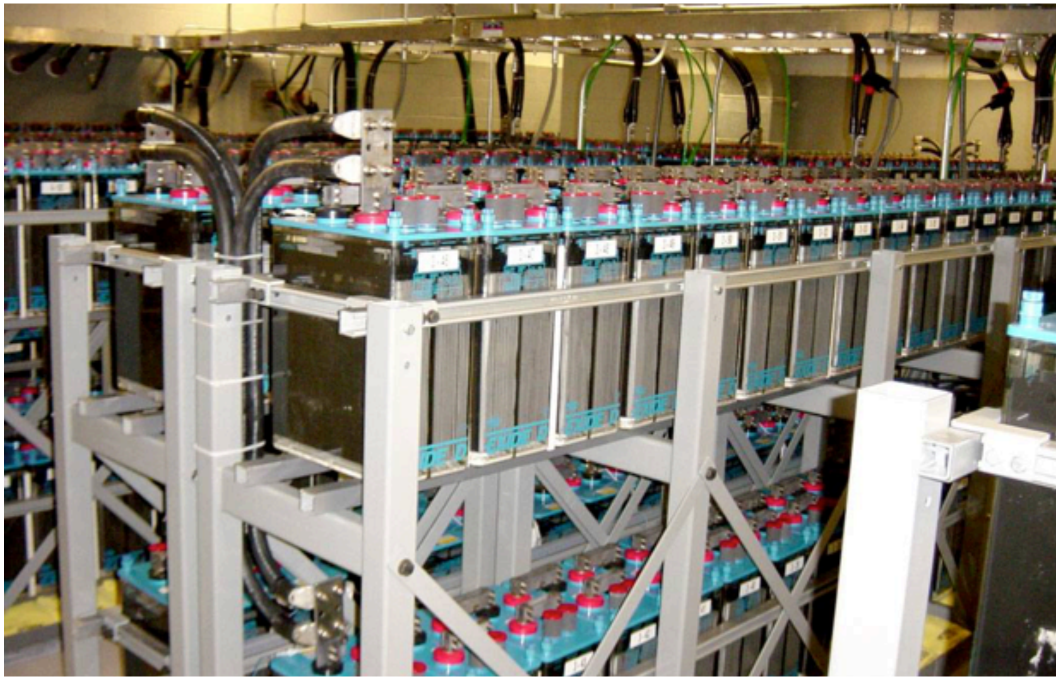
Central Desktop and all of its data centers are SSAE 16 Type II compliant. Ask your sales representative for a copy of our latest reports.

SSAE 16 is an enhancement to the previous standard for Reporting on Controls at a Service Organization, the SAS70. SSAE 16 is a widely recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). A service auditor's examination performed in accordance with SSAE 16 ("SSAE 16 Audit") represents that a service organization has been through an in-depth audit of their control objectives and control activities. This audit often includes controls over information technology and related processes. Central Desktop's SSAE 16 Type II audits ensure that appropriate processes and controls have been established and that a 3rd party has reviewed these controls over a period of time and found them to be working effectively. Your company can use the Central Desktop service with complete confidence

Building, fire suppression + power backup

Alchemy's newest data center is a state-of-the-art 42,500 sq. ft. facility located less than two miles from John Wayne Airport. This carrier-neutral facility has diverse entry points, with both Verizon and AT&T Point of Presence. Constructed in 1989, the building features 18-inch raised floors and is equipped with every essential to house and protect your data. The telecommunication abilities are endless with dark fiber to One Wilshire in addition to multiple fiber carriers such as TW Telecom, Level3, Verizon Business, and AT&T. Never fear a power outage again: the Irvine Data Center has N+1 redundancy on all systems, and four 600KW Caterpillar Generators with enough fuel capacity to run for 16 hours.

Plus, the data center accesses two Southern California Edison Power Grids for maximum power redundancy. Alchemy goes to great lengths to ensure the safety of your data, from a superior cooling system of sixteen independent DX-based air handlers, to high-grade fire suppression systems of double interlocking pre-action dry pipes for both Halon and FM-200. With biometric security and card readers controlling building access, as well as video surveillance and a Dedicated Network Operations Staff patrolling all building entrances, it is clear Alchemy takes great care in not only data-retention, but also data-protection.



This battery backed-up UPS system ensures that none of the critical equipment has an interruption of power while waiting for the generators to kick in.

Application security

User authentication / login security

Physical access to the data center is controlled and monitored 24/7 by:

- Uniformed building security services
- Workspace members (users) are invited by administrators and workspace owners, thus ensuring secure access is restricted to specified users.
- All Central Desktop users create a unique username and password when they create a profile.
- User authentication is controlled via unique and valid username and password combination that is encrypted using a one-way hash. When users submit username and password via this one-way hash to Central Desktop, a unique digital signature (or fingerprint) is created, which in turn identifies and authenticates the sender and the contents of the message.
- After the one-way hash secure login, the security model is reapplied with every request and enforced for the entire duration of the session. The security measures are transparent to the user and do not cause any performance drag, latency, or slow down.
- Each additional request is re-verified and if the user's session cannot be authenticated or the user's status on the site has changed (i.e., the user is deleted from the workspace or company by the administrator), the user will not be allowed to access the specified workspace or data.
- Central Desktop does not use "cookies" to store other confidential information and has implemented advanced security methods based on dynamic data and encoded session IDs.
- Central Desktop uses "expiring headers" which enables users with the ability to ensure maximum security after they log out of the system – eliminating the ability for other users to access cached pages in the browser.

Advanced password security options

Available with Central Desktop for Enterprise, Agencies and Marketers

Central Desktop provides an additional layer of password security by allowing the administrator to adjust a range of password options such as:

- **Minimum password length**
  The administrator can determine what the minimum password length must be for all users within the company. To ensure a minimum level of password security, Central Desktop natively requires a minimum of 6 characters, but can support up to a 50-character minimum password length.

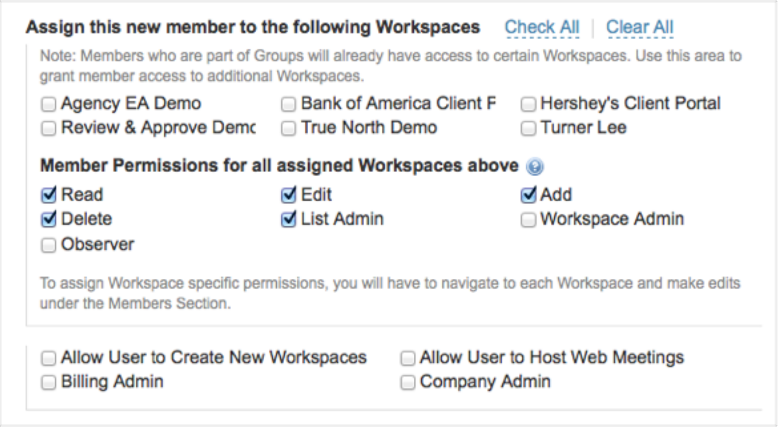
- **Password save option**
  The administrator can determine whether or not to enable the "Remember Me" function at the point of login for all users within the company. This option should be disabled if administrators are concerned about users accessing Central Desktop from public terminals and locations and want to ensure that login credentials are not saved. (Note: Whether or not this feature is enabled, users can still save username and password locally via the web browser.)

- **Password complexity**
  Administrators can require users to use "complex" password credentials. Enabling this feature will require all users to include the following details in passwords:
  - At least one lowercase character
  - At least one UPPERCASE character
  - At least one digit (numeral)
  - At least one special character – one of the following characters: @#$%^&+=-!

- **Password change frequency**
  Administrators can determine how often user passwords expire, forcing users to create a new password every 30, 60, 90, 180, or 365 days.

Permissions and rights management

Central Desktop provides customizable permissions and rights management to accommodate a variety of customer needs. User permissions are managed at both the company level and at the workspace level, allowing access to specified workspaces only and allowing the administrator to further restrict user permissions at the workspace level.



Assign this new member to the following Workspaces Check All | Clear All

Note: Members who are part of Groups will already have access to certain Workspaces. Use this area to grant member access to additional Workspaces.

□ Agency EA Demo □ Bank of America Client F □ Hershey's Client Portal
□ Review & Approve Demc □ True North Demo □ Turner Lee

Member Permissions for all assigned Workspaces above

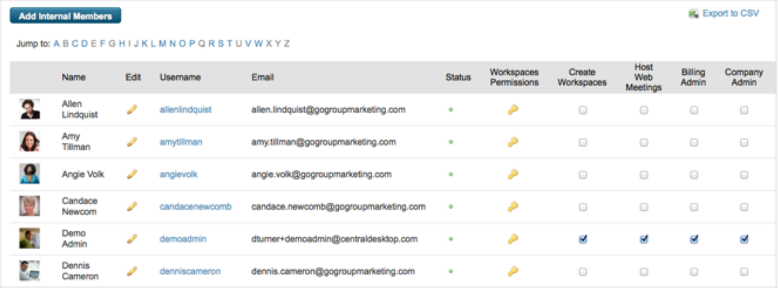
☑ Read ☑ Edit ☑ Add
☑ Delete ☑ List Admin □ Workspace Admin
□ Observer

To assign Workspace specific permissions, you will have to navigate to each Workspace and make edits under the Members Section.

□ Allow User to Create New Workspaces □ Allow User to Host Web Meetings
□ Billing Admin □ Company Admin

Company permissions management

User permissions and access can be managed at the company group level, allowing easy administration of user rights and access to workspaces.

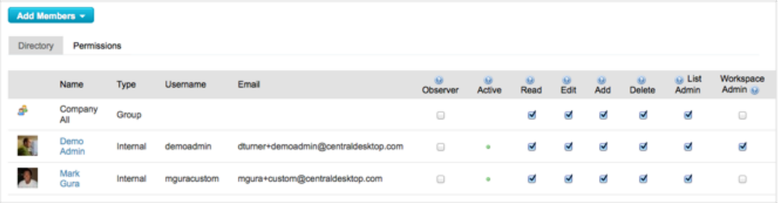


Add Internal Members
Export to CSV
Jump to: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Name	Edit	Username	Email	Status	Workspaces Permissions	Create Workspaces	Host Web Meetings	Billing Admin	Company Admin
Allen Lindquist	✎	allenlindquist	allen.lindquist@gogroupmarketing.com	●	🔑	□	□	□	□
Amy Tillman	✎	amytillman	amy.tillman@gogroupmarketing.com	●	🔑	□	□	□	□
Angie Volk	✎	angievolk	angie.volk@gogroupmarketing.com	●	🔑	□	□	□	□
Candace Newcom	✎	candacenewcomb	candace.newcomb@gogroupmarketing.com	●	🔑	□	□	□	□
Demo Admin	✎	demoadmin	dturner+demoadmin@centraldesktop.com	●	🔑	☑	☑	☑	☑
Dennis Cameron	✎	denniscameron	dennis.cameron@gogroupmarketing.com	●	🔑	□	□	□	□

Workspace permissions management

Granular permissions are managed at the workspace level for users (members) and groups. Permissions such as Read, Edit, Add, Delete and Admin rights are granted on a user-by-user or group-by-group basis at the workspace level.



Name	Type	Username	Email	Observer	Active	Read	Edit	Add	Delete	List Admin	Workspace Admin
Company All	Group			□		☑	☑	☑	☑	☑	□
Demo Admin	Internal	demoadmin	dturner+demoadmin@centraldesktop.com	□	●	☑	☑	☑	☑	☑	☑
Mark Gura	Internal	mguracustom	mgura+custom@centraldesktop.com	□	●	☑	☑	☑	☑	☑	□

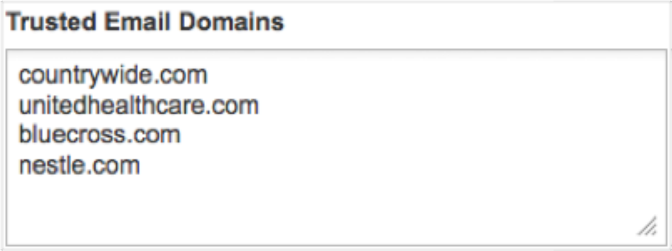
TLS encryption and trusted email domain support

Available with Central Desktop for Enterprise, Agencies and Marketers

Just as SSL protects your data in transit to/from your web browser, Central Desktop uses Transport Layer Security (TLS), a protocol that encrypts and delivers email securely. The TLS encryption and trusted email domain feature allows you to control access and send encrypted emails to trusted users.

Email domains that are listed as trusted domains will receive a TLS-encrypted email with all of the contents of the discussion, comment, or documents available for the user to read.

NOTE: Additional TLS software configuration and setup is required by the company to support TLS encryption.



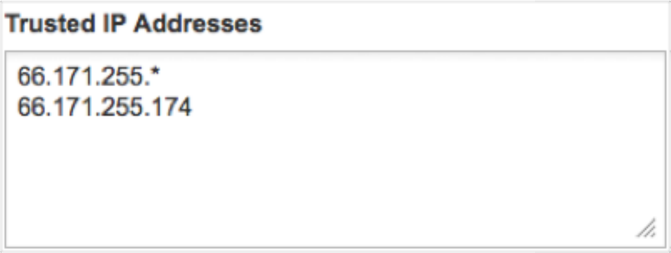
Trusted Email Domains

countrywide.com
unitedhealthcare.com
bluecross.com
nestle.com

Trusted IP addresses

Available with Central Desktop for Enterprise, Agencies and Marketers

The trusted IP address feature allows administrators to restrict access to Central Desktop by IP address or IP range. Only listed IP addresses will be allowed access to Central Desktop. This is ideal for organizations that need to restrict access to Central Desktop via a VPN or office location IP address. This feature can be configured at the company level and overridden at the user level.



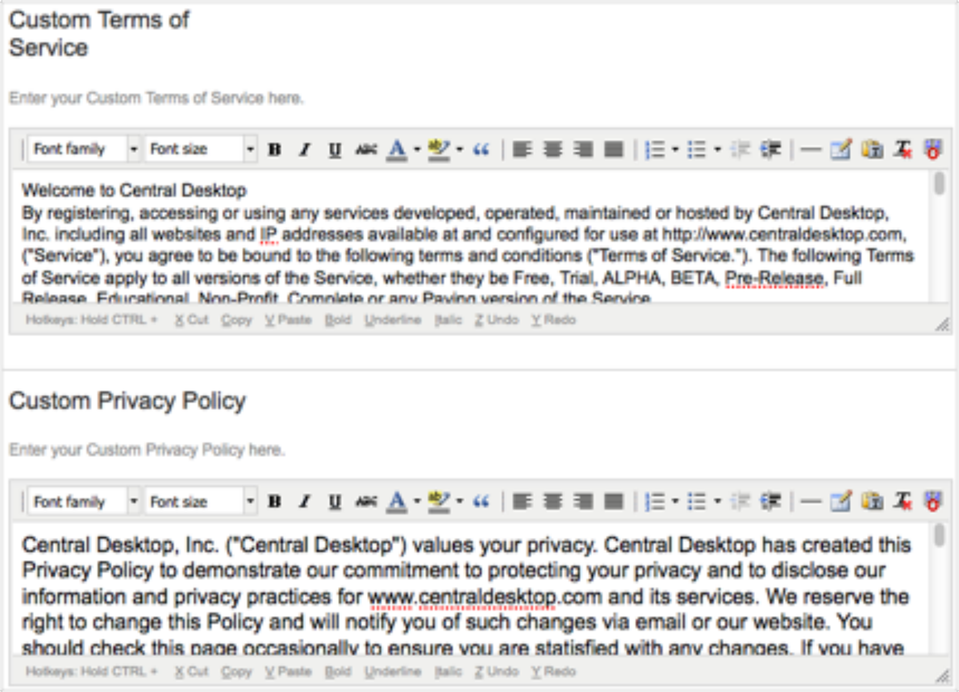
Trusted IP Addresses

66.171.255.*
66.171.255.174

Custom terms of service and privacy policy

Available with Central Desktop for Enterprise, Agencies and Marketers

The custom terms of service and privacy policy feature allows administrators to force internal members and external members to agree to custom terms of service and privacy policy when they register with Central Desktop. This feature enables companies to comply with certain confidentiality or terms of use required under certain corporate policies or statutory requirements.



Custom Terms of Service

Enter your Custom Terms of Service here.

Welcome to Central Desktop
By registering, accessing or using any services developed, operated, maintained or hosted by Central Desktop, Inc. including all websites and IP addresses available at and configured for use at http://www.centraldesktop.com, ("Service"), you agree to be bound to the following terms and conditions ("Terms of Service."). The following Terms of Service apply to all versions of the Service, whether they be Free, Trial, ALPHA, BETA, Pre-Release, Full Release, Educational, Non-Profit, Complete or any Paying version of the Service.

Custom Privacy Policy

Enter your Custom Privacy Policy here.

Central Desktop, Inc. ("Central Desktop") values your privacy. Central Desktop has created this Privacy Policy to demonstrate our commitment to protecting your privacy and to disclose our information and privacy practices for www.centraldesktop.com and its services. We reserve the right to change this Policy and will notify you of such changes via email or our website. You should check this page occasionally to ensure you are statisfied with any changes. If you have

Global performance

To assure constant and continuous connectivity to the core Internet backbones, Central Desktop's network infrastructure leverages multi-homed bandwidth carriers. This ensures global access and uptime in the event of network discontinuity with a single carrier.

The redundant layers that comprise and support the network infrastructure ensure continuous connectivity. In the event of a bandwidth layer failure, the remaining supporting layers will detect the failure and transfer control in a matter of seconds. This is often described as a “self-healing” or “automated” network. This architecture ensures that any single point of failure prevents network disruption.

The best way to improve web application performance is to get the data closer to the end user. Central Desktop leverages the Akamai global content delivery network to speed up both application delivery in addition to file upload/download performance.

Central Desktop has integrated Aspera WAN acceleration for the ultimate in file transfer performance. This feature is especially useful for large file transfers and bulk uploads/downloads.

Akamai and Aspera ensure a great Central Desktop experience no matter where you are in the world.

Akamai aspera

Network security

Central Desktop has architected a multi-layered approach to secure and defend your data from external attack. We leverage state-of-the-art hardware and software security methods to prevent unauthorized intrusion by external users attempting to access your data. Our infrastructure proactively deters and monitors for external attacks and unauthorized intrusions.

Central Desktop employs experienced engineers, system administrators, and IT professionals who pass through rigorous testing, confidentiality agreements, and background checks to secure your data. The Central Desktop team is proactively monitoring and deploying new security measures via software and hardware on a regular basis as appropriate.

McAfee® SECURE

Third-party network auditing

In addition to our own security measures, our network security is audited daily by industry-leading third-party security vendor McAfee. McAfee performs network security checks to verify the integrity of the Central Desktop network as seen from outside the network. Their tests look for vulnerabilities and report any issues immediately to the Central Desktop team.

Central Desktop's multi-layer network security protection

Central Desktop deploys a "multi-layered network security protection system" to secure and defend your data from intrusion and attack. Between our servers, which house customer data and the Internet, there are many layers of network security protection:

1. **Router**
   The first line of defense to protect your data is the router that resides in front of the firewall. The router is specifically configured to block the most prevalent worm attacks on the web by scanning and analyzing header and packet information. Via the scanning process, each packet is inspected and either granted authorized access or denied before ever reaching the firewall. The router is the initial line of defense to eliminate unauthorized and unnecessary traffic and blocks it from gaining access to the firewall.

2. **Firewall**
   All information and data requests that pass through the router must next pass through the firewall. The firewall places strict limits on ports and protocols and provides the second layer of protection for your data. NAT (Network Address Translation), also known as network or IP masquerading technology, is used in the Central Desktop data center firewall to provide an extra layer of security.

3. **Intrusion Detection System (IDS)**
   Passing the firewall, data flows are next scrutinized by the Intrusion Detection System (IDS). The IDS monitors network traffic for malicious activities or policy violations and reports anomalies to the Central Desktop web operations team.

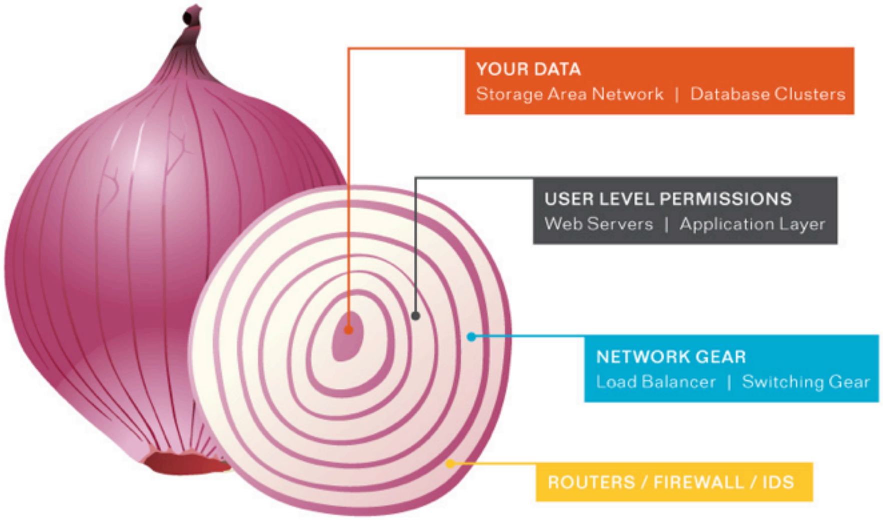
4. **Web server load balancing**
   Web server load balancing, while not strictly a security layer, also provides additional port screening and protocol protection. Web server load balancing can identify common DoS attacks and screen them before reaching the server. It ensures that the URL requests being made are well formed, thus rejecting attempted exploits.

5. Web/application servers
   The web/application server layer runs on FreeBSD with Apache as the web servers and Central Desktop as the application server.

   - Apache is configured to minimal configuration specifications required to run our application layer.
   - Application servers are configured to process HTTP requests only.
   - Other non-core Internet protocols and services are disabled.
   - Servers are locked down and secured at the operating system and system directory levels.
   - All non-essential ports and services have been blocked, locked, and disabled.

Security layers

Security is built in from day one with your Central Desktop solution. The Central Desktop system, with multiple layers of hardware, software, and network infrastructure, is designed and optimized to protect your data from intrusion.


YOUR DATA
Storage Area Network | Database Clusters
USER LEVEL PERMISSIONS
Web Servers | Application Layer
NETWORK GEAR
Load Balancer | Switching Gear
ROUTERS / FIREWALL / IDS

Site operations

- Regular operations and system administrator meetings are held to discuss and review near-term and long-term industry-compliant solutions.
- Central Desktop proactively monitors industry security warnings, channels, and alerts to uncover new and emerging security risks. Central Desktop engineers act immediately upon the discovery of any security risks or alerts.
- Central Desktop proactively scans vendor-specific security channels, including: Cisco Systems, Microsoft Corporation, FreeBSD, Linux, plus community-based forums and channels. Central Desktop also subscribes to all common email virus and bug notification and alerts lists.

Security patches and upgrades

- The Central Desktop team routinely monitors, evaluates, tests, and applies security patches, fixes, updates, and upgrades.
- Any other mission-critical security patches, updates, and upgrades from vendor and community channels are notified and sent to Central Desktop and are routinely evaluated, tested, and applied, if applicable, within 24-72 hours of being notified.

Data integrity

Millions of data files reside within our customers' Central Desktop workspaces, and thousands of files are added every week. Central Desktop enlists a variety of methods to assure data integrity, including data protection based on network architecture, as described previously, plus software-enabled SSL data encryption.

Protected data storage

Your data's integrity is protected by numerous layers of state-of-the-art hardware and software security features to prevent hackers or other unauthorized individuals from gaining access to it. With our multiple-layer network security system, your data is safely sequestered well out of harm's way. The following details our approach to "defense-in-depth" security.

- Security model is reapplied with every request and enforced for the entire duration of the session.
- Application security model prevents customer data cross-over and ensures complete customer data segregation and privacy.
- Customer data is segmented from the application layer providing additional security buffers.
- Customer data is encrypted at rest using industry-standard AES algorithms (military-grade tools, NSA-classified encryption, NIST FIPS 197 encryption)

Virus scanning

- Central Desktop servers run the latest version of virus detection software. Our computers are additionally protected by Trend Micro Antivirus.
- Virus scanning software is updated daily.
- Files uploaded to Central Desktop are virus scanned to ensure safe information collaboration.

SSL data encryption

All Central Desktop customers can leverage 256-bit AES High Grade Encryption and Secure Socket Layer (SSL) that protects your data using both server authentication and data encryption.

- SSL encryption technology protects your data from being read during transmission from your computer to Central Desktop servers.
- SSL encryption software ensures that when the recipient of the transmitted data receives the information, the computer decrypts the information, authenticates the source, and verifies the data integrity.
- SSL encryption technology leverages digital certificates to verify the identity of the data flow over the internet and allows for encryption and decryption by authorized (authenticated sources).

Central Desktop uses Comodo/USERTrust for its SSL Digital Certificates.

- Comodo/USERTrust is the second-largest certification authority for ensuring identity trust and assurance on the web.
- Comodo/USERTrust's comprehensive array of technologies enables organizations of all sizes to secure e-business transactions cost-effectively.
- More than 200,000 customers in more than 100 countries, securing 500,000+ businesses and individuals, rely on Comodo/USERTrust products and services.
- Comodo/USERTrust operates one of the world's largest, fastest growing certification authority infrastructures with the highest standards as evidenced by KPMG annual audits.

Data backups and restoration

All Central Desktop has implemented rigorous backup procedures to ensure that your data is safely and accurately backed up.

- Central Desktop maintains a mirrored and redundant copy of the entire Storage Area Network (SAN). This acts as a “warm backup” ensuring quick access and retrieval of data in an emergency.

- Central Desktop maintains a full backup snapshot of data stored on the SAN. Central Desktop executes a daily backup and stores data for up to 90 days.

- Backup procedures include entire SAN, databases, and all configurations and code files for all servers.

- All backups are encrypted in transit and at rest using the same level of encryption and protections as live data.

- All backups are rotated into offsite rotation daily.

- Central Desktop is able to restore and retrieve data stored for up to three months. (Applicable fees will apply.) To initiate a restore request, please contact Central Desktop Support at **support@centraldesktop.com**.

- At any time, workspace administrators can access and download the entire contents of the workspace to give you additional peace of mind so that you can store a back-up of your data.

Complete system redundancy

System redundancy is the key to ensuring consistent and reliable uptime and to eliminating single points of failure. Central Desktop's infrastructure follows an N+1 model to provide full redundancy of all key system components and services including hardware, internet connectivity, and power systems.

- Redundancy is available on all key networking equipment including routers, switches, firewalls and load-balancing servers.

- Multiple load-balanced web servers and application servers are configured to ensure redundancy. If a web server fails, there are multiple web servers available to carry the website traffic and loads without interruption.

- Database and file servers use hardware RAID (redundant array of independent disks) technology to ensure availability during standard maintenance. This also ensures data integrity and redundancy in the event of any single hard drive failure – without interruption or data loss to the user/customer.

- Routers and web servers are optimized and configured to accommodate maintenance, software upgrades, server rotation, and configuration without a disruption of service.

Comprehensive disaster recovery plan

Central Desktop has planned for comprehensive disaster recovery and contingencies to protect your data and to provide critical access and business continuity to our applications. Business continuity ensures that you are able to conduct your business in the event of natural disaster or the suspension of services as a result of power or internet connectivity.

Comprehensive disaster recovery ensures the ability to re-establish a working data center at our secondary site if a disaster destroys or renders inoperable the primary data center site. In the unlikely event of a catastrophic disaster and failure at Central Desktop's primary data center site, Central Desktop has a comprehensive Disaster Recovery Plan in place.

A complete test of this Disaster Recovery Plan is conducted annually.

Contingencies and plans are in place to ensure that Central Desktop and its customers are up and running with complete Central Desktop functionality and restored data within 12 hours of the disaster.

The disaster recovery plan includes guidelines, procedures, and clear roles of responsibility and communication amongst the partners. The plan ensures timely action and quick response in such an unlikely event.

- Within 2 hours of notification of the disaster at the primary data center location, a disaster team is activated and prepared to begin the recovery.
- Our secondary facility (located in Dallas, Texas) is prepared and brought online.
- Key server configuration and customer data is updated and restored from the most recent backup.
- Central Desktop customers regain access within 12 hours of the disaster.
- The secondary hosting facility is capable of performing all hosting functions in the event of such an emergency or disaster. The secondary hosting facility is comparable to our primary facility.

Uptime / high availability

Central Desktop provides industry-leading uptime and service with high availability and uptime.

- Real-time updating of systems can be found at **http://status.centraldesktop.com**

- The measured uptime for Central Desktop typically exceeds 99.9%. (This is exclusive of scheduled maintenance, which includes hardware and network maintenance as well as software updates.)

- Hardware maintenance is typically performed in windows between 12:00 am and 3:00 am Eastern Time on weekends to avoid inconveniencing customers.

- Software update procedures typically require the site to be down for less than 60 seconds at a time. Central Desktop schedules software maintenance for weekend mornings (North America time) to ensure minimal customer disruption.

- Central Desktop uses real-time onsite and offsite alerts systems and site monitoring to ensure the availability and performance of distributed IT infrastructures — e.g., servers, operating systems, network devices, network services, applications, and application components. Proactive monitoring enables Central Desktop engineers to attack problems immediately before they become critical or emergencies.

Summary:
Your data is secure and protected

Central Desktop provides industry leading security and protection of your data. Whether you are working from your office, your home, or on the road, you can depend on Central Desktop to be available to you at your critical moments.

The ability to access your data anytime from anywhere ensures that you remain productive, protected, and connected to the information that you need to run your business.

For more information or questions, please contact **info@centraldesktop.com**.

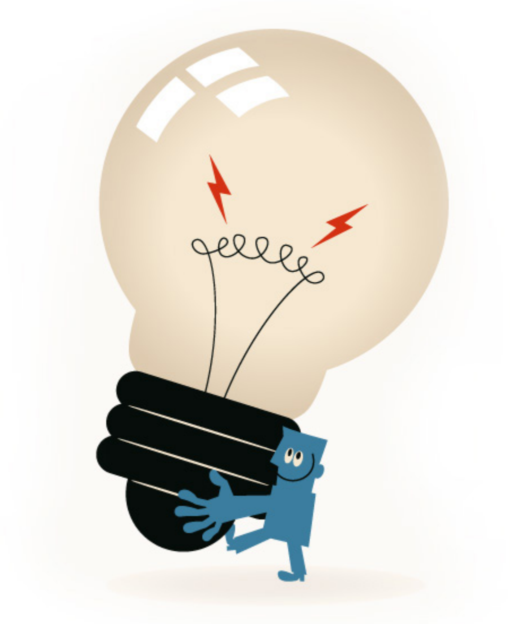
About Central Desktop

Central Desktop helps people work together in ways never before possible.

The Central Desktop collaboration platform connects people and information in the cloud, making it possible to share files, combine knowledge, inspire ideas, manage projects and more.

Central Desktop serves half a million users worldwide. Key Central Desktop customers include CareerBuilder, MLB.com, Sesame Street, PGA Tour, The Humane Society, CBS, Workday, WD-40, Pokemon and Pinkberry.

Founded in 2005, Central Desktop is a PGi company located in Pasadena, California.



click here to learn more about Central Desktop

(c'mon just click it!)

Contact us

We don't bite

866 900 7646
centraldesktop.com