



Introduction

In web and audio conferencing, as in all areas of telecommunications, security is an overriding concern. Balancing the productivity and operational efficiency gains of conferencing with the security of shared information is paramount. Often, highly confidential information-critical to a company's competitive advantage-is shared by meeting participants who depend on web conferencing to collaborate more effectively with other employees, partners, and customers.

Terra Firma recognizes that security is a high priority among enterprises, and ensures that its conferencing solutions give customers the peace of mind they need to fully experience the benefits of conferencing technology. With multiple layers of security implemented at each stage of the conference-from uploading documents to the actual meeting to post-conference reporting-Terra Firma is dedicated to ensuring that all aspects of a web conference remain safe from unauthorized access.

Terra Firma's architecture and business practices are focused on ensuring total conferencing security and preventing breaches. With Terra Firma, participants are not required to download any plug-ins or applications, thereby minimizing security risks. As a single-source provider of both web and audio components, Terra Firma delivers a more secure conferencing environment, enabling customers to monitor and control both aspects of their conferences using a single vendor.

Comprehensive security measures at three levels:

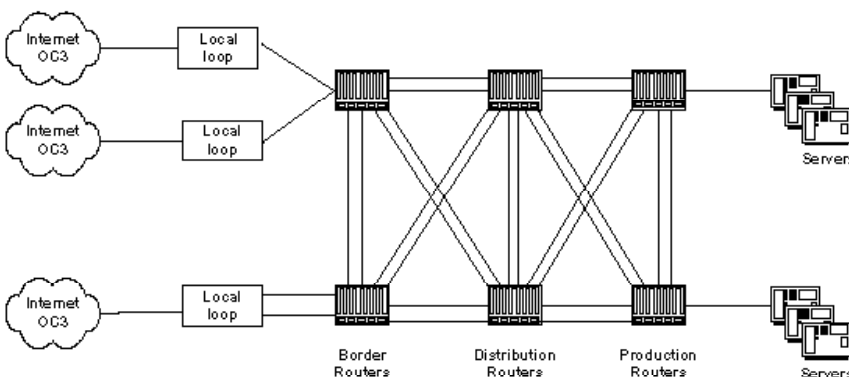
- Physical Security - Ensures the physical integrity of the data center
- Data Security - Ensures the security of presentations and other data on the network
- Access Control - Ensures that unauthorized individuals cannot access secure conferences

This white paper describes, in detail, the security measures taken in each of the three levels of security and how enterprises benefit from these measures.

Physical Security

Terra Firma utilizes a \$40 million convergent communications platform in Louisville, Colorado which delivers a 99.99% uptime-exceeding the industry standard for these metrics. The company's private servers are housed within the secured data center, which is protected with biometric, multiple-authentication locks, and around the-clock video monitoring to ensure that only designated, authorized engineers within the ettingengineering team can enter. These engineers provide 24x7 monitoring to maintain the infrastructure and troubleshoot problems.

Diagram of the Data Center



The infrastructure:

- 550+ T-1s - over 13,000+ phone lines
- Redundant Tier 1 Internet and voice communications providers
- Redundant systems, servers and communications hardware
- 6 terabytes of real-time storage
- 3 OC-12's of local loop on redundant data feeds
- 550+ Mbps of Internet bandwidth

Physical security measures implemented to protect the comprehensive data center described above include:

- Around-the-clock security patrols
- External and internal, digitally recorded video surveillance on all exterior doors and throughout the building
- Biometric and key-card access to authorize entry into data center
- Glass-break detection on all exterior windows
- Fire and smoke alarms
- Forced entry alarm

Data Security

The data center is protected by state-of-the-art firewall security, which ensures thorough filtering of all incoming and outgoing messages meet the company's stringent security criteria. Select members of the network engineering team, a group of designated and authorized engineers responsible for monitoring and maintaining all systems within the infrastructure, constantly monitor the firewalls, preventing security breaches before they occur and ensuring the stability of the firewalls. Two-factor authentication is used for administrative control of the routers and firewalls within the data center for the highest levels of protection against unauthorized tampering of or access to the security policy.

All data stored within the data center is protected by the industry-standard 128-bit SSL encryption method, which verifies the authenticity as well as the integrity of the data through public and private key technology. SSL is the same technology that is used to secure commerce transactions on the web. This layer of data security is optional for Cybernar customers. Whiteboarding, polling, and application sharing sessions, as well as uploaded presentations and reports, can be encrypted using SSL/HTTPS when transmitted over the web to ensure protection of confidential materials from unauthorized users.

The data center is further secured with separate physical and logical environments for development, testing, and production, isolating each environment from one another and from potential security breaches.

All services are HTTP-based, requiring only the standard port 80, 443 for SSL, to be open on the customer's firewall. This eliminates any erroneous communications or malicious attacks using other port numbers on the firewall to gain entry into the customer's network.

Finally, because the Cybernar user interface for participants is a Java-based applet, rather than a downloadable plug-in, users can be assured that Terra Firma will have no impact on their files, file structures or file operating systems.

Access Control

Terra Firma utilizes a conferencing platform that ensures that only those authorized can access each conference and shared data. By designating a conference moderator and giving the moderator complete control of all aspects of the conference, Terra Firma provides maximum security for conference access and document storage.

Terra Firma assigns each moderator a unique conference ID and PIN, which are required to initiate a conference on the telephone or the web. For another layer of security, Terra Firma allows moderators to create a security passcode unique to each audio conference.

In addition, Terra Firma provides methods for monitoring participants and their interactions. The web interface enables moderators to view each participant's information quickly and easily. Audio conference participants are listed with the telephone number from which they dialed in; web conference participants are listed with their name and unique IP address. Moderators can restrict access to a conference and accept or reject an attendee based on the participant's email address. A moderator can also dismiss an individual from a conference directly from the web interface.