



## For Interactive Meetings

Terra Firma Cybernar is the cost-effective way to host remote sales presentations, marketing seminars and training events. Save money and reduce travel by bringing the interactivity of in-person meetings online. This fully automated service integrates the web and the phone for seamless deployment of large-scale events with a 99.99% uptime guarantee and scalability of up to thousands over the web.

## Security

Terra Firma fully understands and supports the ever-growing need for increased security measures and has in place three levels of security - physical, data and access control. The physical integrity of our data center is of the utmost importance and our technologically advanced security system ensures that only authorized individuals have access to the data center.

The data stored within our secure facilities can also be highly protected with industry-standard 128-bit encryption methods, including optional SSL, Secure Sockets Layer, which verifies authenticity as well as integrity of data. Access to this data is further protected by a uniquely assigned conference ID and PIN with the ability to add a security passcode determined by the moderator over the phone.

### *Premises Security*

Terra Firma's physical infrastructure is constructed to exceed industry up time, reliability and security standards. Privately held servers are housed within our secure data center to ensure their safety. Terra Firma restricts data center entry to selected members of our engineering staff who must pass through biometric, multiple-authentication locks and video monitoring. These select engineers monitor the data center 24/7 to control maintenance and troubleshoot problems.

### *Data Security*

Whiteboarding, polling and application sharing sessions, as well as uploaded presentations and reports can be encrypted with optional SSL when transmitted over the web and are safe from unwarranted viewers. The following features assist in protecting uploaded content.

Java-based	Cybernar applet is Java-based to ensure there is no impact on files, file structures or file operating systems.
Content transmission security	Terra Firma offers an optional SSL/HTTPS environment, which authenticates and encrypts communication between clients and servers and ensures protection of confidential materials from unauthorized participants.

### *Access Control*

Terra Firma assigns each moderator a unique conference ID and PIN required to initiate a conference on the phone or web. To add another layer of security, moderators can create a security passcode unique to each conference. Terra Firma provides the following features allowing the moderator to control conference access.

Participant list	The conference lock function ensures no other participants enter the conference, including the conference operator.
Document protection	Moderators can protect a presentation and choose who can view specific slides. There are three ways of protecting and/or publishing documents. <ul style="list-style-type: none"> <li>• Exclude from everyone except moderator</li> <li>• Allow certain users by participant ID</li> <li>• Allow public access</li> </ul>
Conference operators	During your conference, a public or private conference operator can answer additional questions about your conference participants on the phone or on the web.

## Data Center

Terra Firma uses a \$40 million platform to provide a reliable service with a published uptime of 99.99%. The data center currently operates at only 50% of capacity ensuring that the full 125 ports are available to every conference moderator at any time.

The Terra Firma infrastructure includes:

- 400+ T-1s - over 10,000+ 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
- 450+ Mbps of Internet bandwidth

## Network Architecture

Terra Firma integrated data/telephony architecture is focused on high capacity and throughput while minimizing points of failure. Our services offer a total in-house solution comprised of several highly redundant connections that are monitored 24/7 by select engineers who focus solely on the Cybernar network.

### Multiple Telephony Carriers

Terra Firma utilizes multiple vendors for our entire communications network to ensure technical issues do not interrupt conferences. Through several top-tier service providers, Terra Firma utilizes a highly reliable and scalable backbone. Terra Firma's redundancy includes the following layers.

ISPs / Fiber providers	Three top-tier Internet Service Providers (ISPs) allow Terra Firma to distribute content over the Internet on several backbones to drastically reduce bandwidth problems. They also provide flexible local loop access, which disseminates users to supply almost unlimited scalability.
Border and Distribution Routers	Network border routers handle all incoming and outgoing traffic via the Internet with distribution routers managing distribution of data traffic to the company's integrated service offerings.  Cybernar routers manage all incoming and outgoing traffic to the Cybernar servers. If one of these routers fails, another handles all data traffic with no interruption.

### Firewall Compatibility

Terra Firma protocol is HTTP-based, allowing corporate end-users to easily gain access. State-of-the-art firewall security ensures all incoming and outgoing messages are thoroughly filtered to meet stringent security criteria. The standard port 80 is required to be open on the firewall.

## System Requirements

Implementing and managing Cybernar requires little to no internal resources and there is rarely a need for technical support. If users ever do experience a problem, customer support is available by phone or e-mail 24 hours a day, seven days a week.

Cybernar runs on most computer platforms that use a Java-enabled browser. It deploys with minimal bandwidth and no client downloads or plug-ins are required.

Hardware	A computer with a sound card and speakers
Browser software	Netscape Navigator 4.75, 4.79, 4.80 or 7.0 Microsoft Internet Explorer 5.xx or higher One of the following JVMs <ul style="list-style-type: none"><li>• Microsoft JVM</li><li>• Sun JVM* (requires 128 MB RAM and does not support playback of recorded audio components)</li></ul>
Operating system	Windows 98/2000/NT4/XP
Bandwidth minimum	56 kbps dialup or faster recommended
Graphic Formats for Web Presentations	Microsoft PowerPoint (animations are not supported)

\*Sun JVM Versions supported: 1.3.1\_02, 1.3.1\_04, 1.3.1\_06, 1.4.0\_01, 1.4.1, 1.4.1\_01