

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.

Raindance, the premier provider of integrated web, audio and desktop video conferencing solutions, 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-Raindance is dedicated to ensuring that all aspects of a web conference remain safe from unauthorized access.

Raindance's architecture and our business practices are focused on ensuring total conferencing security and preventing breaches. With Raindance, 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, Raindance delivers a more secure conferencing environment, enabling customers to monitor and control both aspects of their conferences using a single vendor. Finally, because Raindance controls, maintains, and monitors all of its own equipment and does not outsource, enterprises can be assured that the technology always meets our highest standards of quality and security.

Raindance implements comprehensive security measures at three levels:

- Physical Security - Ensures the physical integrity of the Raindance 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 by Raindance in each of the three levels of security and how enterprises benefit from these measures.

Physical Security

Raindance's \$40 million convergent communications platform in Louisville, Colorado delivers 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 Raindance Network Engineering team can enter. These engineers provide 24/7 monitoring to maintain the infrastructure and troubleshoot problems.



Data Center

Raindance has invested over \$40 million in our convergent communications platform to provide a reliable service with a published uptime of 99.99%.

The Raindance 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

Physical security measures implemented to protect the comprehensive Raindance 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 Raindance 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 Raindance Network Engineering team, a group of designated and authorized engineers responsible for monitoring and maintaining all systems within the Raindance infrastructure, constantly monitor the Raindance 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.

In Raindance's Reservationless Conferencing solution, all data stored within the Raindance 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 Web Conferencing Pro 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 Raindance 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 Raindance 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.

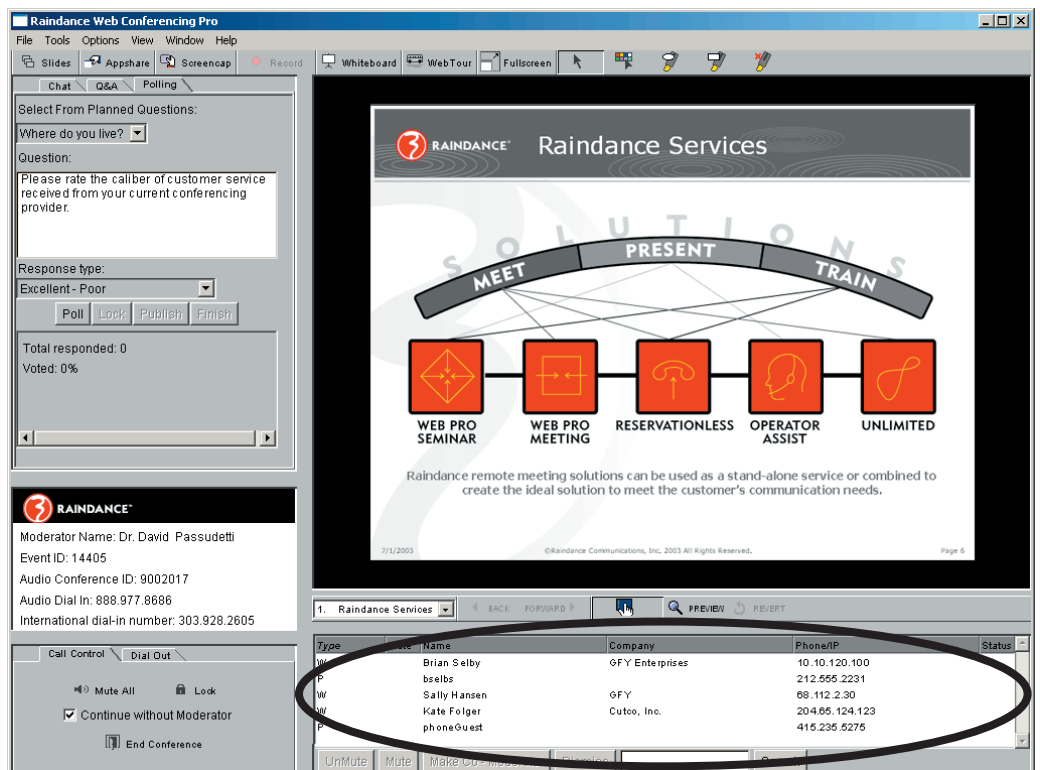
Finally, because the Web Conferencing Pro user interface for participants is a Java-based applet, rather than a downloadable plug-in, users can be assured that Raindance will have no impact on their files, file structures or file operating systems.

Access Control

Raindance has designed its conferencing platform to ensure 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, Raindance provides maximum security for conference access and document storage.

Raindance 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, Raindance allows moderators to create a security passcode unique to each audio conference.

In addition, Raindance provides methods for monitoring participants and their interactions. Raindance's 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 Raindance web interface.



The screenshot displays the Raindance Web Conferencing Pro interface. The main window shows a presentation slide titled "Raindance Services" with a diagram illustrating solutions: MEET, PRESENT, and TRAIN. Below the diagram are five service icons: WEB PRO SEMINAR, WEB PRO MEETING, RESERVATIONLESS, OPERATOR ASSIST, and UNLIMITED. The interface also includes a sidebar with a poll question "Where do you live?", a moderator information panel, and a participant list at the bottom.

Type	Name	Company	Phone/IP	Status
W	Brian Selby	GFY Enterprises	10.10.120.100	
W	bzelbs		212.555.2231	
W	Sally Hansen	GFY	68.112.2.30	
W	Kate Folger	Cutoo, Inc.	204.65.124.123	
W	phoneGuest		415.235.5275	

Additional security is provided with the following access control features for the conference moderator:

- Conference Lock - Ensures no other participants enter the conference, including the conference operator unless requested.
- Entry/Exit Announcements - A tone or the participant's name notifies the moderator who has entered or left the call.
- Participant List - Within Reservationless Conferencing and Web Conferencing Pro, the Raindance web interface lists both participant names and Automatic Number Identification (ANI) to verify identities and provide participant count.
- Dial-out to Participants - Raindance enables users to dial-out to participants via telephone or web interface to ensure the identity of participants.
- Security Codes - The moderator can designate security codes for any audio conference, which are then required by audio conference participants to access the telephone portion of the conference.
- Document Protection - The conference moderator can choose to protect a presentation. In addition to encrypting the presentation or document using SSL, which is standard for Reservationless Conferencing and optional for Web Conferencing Pro, conference moderators can protect and/or publish documents by:
 - Excluding everyone except moderator
 - Allowing certain users by participant ID
 - Allowing public access
- Conference Operators - During a conference, a public or private conference operator can answer additional questions about the conference participants over the telephone or on the web.
- Post Conference E-mail Reports - After completion of an audio conference, an e-mail report details the participants in your event.

In Conclusion

From our significant investments in data center technology to our product architecture, security is, and has always been, a primary focus for Raindance. With comprehensive security measures implemented at multiple levels within each conference, customers can rest assured that their confidential information always remains safe and secure from unauthorized access. Raindance's commitment to secure, reliable audio and web conferencing means that customers can experience the tremendous productivity benefits and operational efficiencies of collaborative technology.