Hoot Meetings

Security Whitepaper

As organizations unlock the true potential of meeting over the web they need to be confident that their content and information is protected. Whether meeting internally or with trusted external parties, it is important for meeting participants to be able to collaborate and share sensitive corporate information freely yet securely, within the confines of strict firewall protection.

With these goals in mind, Hoot Meetings was developed to be secure by design, providing users with high-level security throughout all phases of a meeting, presentation storage, delivery and collaboration.

Hoot Meetings is a hosted service with all the necessary tools for managing online meetings one-click at a time – without sacrificing security or quality.

Security applies to Hoot Meetings through:

- In-meeting: user-controlled privileges
- Customization: client defined customization
- Secure Design and Access: Standards based encryption
- Platform: strong networks and systems
- Physical: world-class infrastructure

This paper describes how security controls are effectively used to protect organizations using Hoot Meetings including discussions of how it provides standard security protocols at the account and presentation levels, additional security options such as Transport Layer Security (TLS) encryption and firewall transparency.

User-Controlled Privileges

Hoot Meetings requires a one-time registration process for moderators using an email address as username and user created secure password. Registration process can also support Single Sign-On (SSO) and JIT User Provisioning. Additional options below can be enabled to enhance the security of the registration.

Account Registration

- User created password
- User creates their own password. Complexity requirements and expiration can be set at a company level.
- Multi-Factor Authentication (MFA)
- User will be sent an email with a one-time security code that expires in 10 minutes.
- Security image
- An anti-phishing feature that allows the user to select an image from a predefined list and assign a label to it. It will be displayed in the succeeding logins to verify the authenticity of the website.
- Google re-captcha
- Uses Google's "I am not a robot" re-captcha service for spam and abuse protection.

In-Meeting Features

- Lock Meeting
  - Moderators may "lock the door" to a meeting so additional participants trying to enter the meeting will go into a virtual waiting room where they wait until admitted by the moderator.
- Content Share Permission
  - Moderator approval is required for a participant to share content.
- Participant List
  - Participants can identify who is in the meeting.
- Dismissing Participants
  - A moderator can quickly dismiss an individual or all participants from the meeting at any time.
- Session Management Features
  - End of Meeting
    - When a moderator ends a meeting, participants are automatically dismissed from the meeting
  - Session Management Values
    - Hoot uses a randomly generated token, chosen from 42 billion possible combinations and stored as a session (non-persistent) cookie. This token is required for validation and authentication to be allowed to either start or join a meeting.
    - A different token is required for each server connection type: meeting, application sharing. The token generation process is automatically handled by the servers and clients.
    - Token validity have a limited lifespan.

Client Defined Customization

Hoot Meetings allows feature customization on a company level. If these features pose a security risk, it can be customized.

- Registration Options
  - Moderators register for a profile using an email address and user created secure password. Organizations can opt to use Single Sign-On (SSO) or Just-In-Time (JIT) User Provisioning.
- Password Requirements
  - Password complexity and expiration can be set according to your organization's security preference.
- Multi-factor Authentication (MFA)
  - MFA can be required every time the user signs in or only the first time.
- Secure Image
  - Security Image is optional. It can be turned on or off.
- Social Media Integration
  - If the company has strict policies on social media access, this feature can be disabled entirely or for specific social media platforms. We support Google, Twitter, Facebook, and LinkedIn.

Secure Design and Access

- All Hoot Meetings features operate in a proxy friendly manner.
  - Some of the features do utilize different port numbers and types like UDP to enhance performance and in-meeting experience.
  - If those ports are not accessible, Hoot will fall back and default to using HTTPS on port 443.
- Operating Systems
  - Hoot is based on standard web server technology (Linux servers) and proprietary servers developed from the ground up, built specifically to meet the demands of online conferencing.
  - All servers are secured using best practices, as well as proprietary security measures.
- Testing Fields and Processes
  - All user input fields are checked for validation and possible attacks like SQL injection.
  - All processes are extensively tested before being put into production.
- Security Event Logging and Archiving
  - Security logs are recorded and archived for all components.
- System Development Life Cycle (SDLC)
  - Security is designed and applied from the ground up and throughout the development and product life cycle.
- Change Management
  - Implementation and rollback plans are mapped out in detail before any changes are made.
  - Releases follow a formalized product release cycle and are thoroughly tested on pre-production servers to ensure that upgrades to do not affect functionality or meeting data.
- Encryption
  - We treat the protection of your information very seriously. We secure all meeting traffic sent over the public Internet using HTTPS and standard encryption.
  - All communications between data centers are secured over encrypted VPN tunnels.
  - Data transfer between the client and the servers is done using Secure Socket Layer (SSL) and Web sockets.
- Fraud Detection
  - Fraud detection is implemented in Hoot to hold dial outs until a moderator is present in the meeting.
  - Tracking of all dial out requests and it will block an IP when it is making multiple dial outs to same number in the same meeting within a set time (15 dial outs within 5 minutes).
  - Blocking accounts that failed to login after multiple attempts over SIP or H.323.
  - Blocking of conference code harvesting.

Platform

Secure Service Platform	Intrado Cloud Applications	
	Vulnerability Management Regular scanning, documented patching process – classification, assessment, deployment	**Strict Access Controls** Least privileged access, separation of duties, access controls, audit logs
	High Availability 24/7/365 service monitoring, transparent component fail-over, datacenter / geographic fail-over, disaster recovery and business continuance	**Hardened Networks** Firewalls, secure device configuration baselines, VPNs, intrusion detection / intrusion prevention systems
	Intrusion Detection and Response 24/7/365 monitoring, incident response, forensics	**Hardened Systems** STIG derived hardening standards

Physical Access

The physical access to our data centers follows strict rules. Here are some examples of some of the systems that have been implemented:

- Access to all data center locations are restricted access and all access must be pre-cleared by NOC, with identity validation by government-issued ID only.
- Two-factor authentication
- Access logging
- Video surveillance systems are installed in all premises.

Security Assessments and Audits

To ensure that our server and application infrastructures are always at the highest level, several assessments and audits are conducted at various times.

- Internal vulnerability assessments (monthly)
- Internal web application PEN testing (periodically)
- Third-party network vulnerability review and assessment (annually)
- Third-party Hoot web application PEN test (annually)
- ISO 27002 review and assessment (annually)
- Hoot data centers are covered by their own audits
- The primary Hoot IDC is covered by a SOC 2 audit

About Intrado

Intrado develops innovative, cloud-based technology to make it easier, more effective and efficient to deliver connections that count in this increasingly complex world. Our solutions connect people with each other and the information needed to gain insights for better decisions on the issues that matter most.

Intrado has sales and/or operations in the United States, Canada, Europe, the Middle East, Asia Pacific, Latin America and South America. Intrado is controlled by affiliates of certain funds managed by Apollo Global Management, LLC. For more information, please call 1-800-841-9000 or visit www.intrado.com.

Intrado
Information to Insight

200715SM-DOC-01-Hoot Meetings Security Whitepaper