



InterCall Streaming Services

Security Planning and Training



www.intercalleeurope.com

Application

InterCall Streaming Services software development uses a security first approach in conjunction with our agile development process to deliver software that complies with industry standard security measures and best practices. Design phases include test planning activities surrounding security (in addition to other test cases). Application development includes routine security audits on new feature sets and regression testing / auditing with new releases of the software. A well defined quality assurance and defect detection resolution is in place and is intrinsic to the overall software development lifecycle.

Infrastructure

Infrastructure design for InterCall Streaming Services starts with the physical security layer, ensuring controlled physical access to all equipment, either via directly controlled datacentres hosted by Level3 Communications, or via managed datacentres by Rackspace Hosting. All locations housing critical data require controlled access to locked cabinets, CCTV monitoring, and logging of all visitors.

Network layer security involves the use of basic firewall options enabled directly on servers, in addition to dedicated network firewalls, and a managed Intrusion Detection/Prevention System, with 24x7 monitoring provided by AlertLogic.

OS security includes a controlled patch schedule to address any significant security updates, with patch status checked automatically via AlertLogic internal security scans.

User access is also tightly controlled, with access to production servers granted on a per-user basis. Expired and unused accounts are also automatically reviewed via the AlertLogic appliance.

In the event of a successful Denial of Service attack or other system failure, external monitoring, as provided by AlertSite, will notify the appropriate administrative staff immediately.

Intrusion Detection and Prevention

As any site available to the Internet has the potential to be attacked, we work with AlertLogic's managed service to minimize our risk. This service involves a locally-installed hardened Linux-based appliance behind each firewall, which then runs security scans and log monitoring services against all servers in a given datacentre facility. Any traffic directed to a server is also mirrored to this appliance, allowing constant non-disruptive monitoring of all traffic directed to our servers. In the event of suspicious activity, including Denial of Service attacks, alerts are generated. Specific attack methods can also be automatically blocked on a per-attacker basis when detected, allowing for unattended threat assessment and neutralization.

SOPs for log review, scanning, etc.

At present, we run weekly vulnerability scans against our servers both internally and externally, all managed by AlertLogic. Reports are generated based on these scans, and analyzed by the Network Security team to determine the appropriate course of action.



Personnel Security

DATA CENTRE ACCESS

We have implemented firewalls in our self-managed datacentre to minimize our servers' exposure to the Internet. Only authorized services are run from our datacentre, and within our location, we also run Intrusion Detection and Prevention Systems in concert with a managed monitoring service, for 24/7 security and semi-automated threat response.

By default, event registration systems, web servers, streaming media servers, integration services and databases are located on servers dedicated to InterCall, but are shared between InterCall clients. There are rigorous safeguards in place to ensure that data cannot be accessed except by authorized individuals and in cases where additional physical segregation is required, InterCall Streaming Services can provide dedicated web, database and application servers. Portable and sensitive workstations run full drive encryption. Physical access to these devices is limited by auto locking policies and separate locked doors for servers and machines containing sensitive information.

DATA ACCESS

Customer data, including but not limited to end user personally identifiable information, is accessible only to InterCall Streaming Services personnel on a need-to-know and least-privilege basis and is compliant with West Corporation enterprise policy on this subject. Production systems responsible for storing customer data are secured with a strict set of procedures. These practices include standardized server hardening, intrusion detection / prevention, patch analysis and management, strong firewall and physical access policies, logging and log auditing, all of which are continually reviewed and refined.

HIRING / BACKGROUND CHECK PROCESS

InterCall performs pre-employment background checks on all new hires. This includes previous employment verification and criminal history.

TRAINING

InterCall invests in its employees and believes in developing all employees through internal and external training programs. The training and development programs begin from the time of hire with the New Hire Orientation, and continue through "on the job" training, skills training, customer service and management development. Various training programs are offered to all employees through the Human Resources Department, while other more skill oriented training programs are offered through the individual departments. Employees are encouraged to participate in the various external and internal programs. New Associates must receive security awareness training and be made aware of the Information Security Policies and Standards Manual as part of their orientation. Existing employees must receive continued security awareness training on an annual basis. All new Associates must sign an Information Security Policies and Standards Acknowledgement form to acknowledge that each new Associate has read the Information Security Policies and Standards Manual and understands their responsibilities in connection with the security policies and standards and the consequences of an infraction. There is a formal disciplinary process for employees that have not complied with security policies and standards.



DATA CENTRE

Our partner, Level3 Communications (Level3), has well defined procedures to protect all equipment associated with customer solutions.

- + Access to inventory areas are strictly controlled, documented and managed by data centre managers.
- + Surveillance cameras are deployed internal and external to all Level3 facilities monitoring zones 24/7 with CCTV/DVRs.
- + Man traps and card access are deployed at all locations.
- + Level3 has deployed a multi-layered physical security approach consistent with the requirements defined with Industry Standards.
- + Access is controlled by photo badges, proximity access cards, keypad devices, individual per-cabinet combination locks, CCTV/DVRs, and alarms.
- + Visitor access is strictly controlled.
- + Level3 employees utilize proximity badges and access cards to enter the building.
- + Only Level3 Data Centre customers are allowed to access the server/production floor. That entry access is controlled by a numeric keypad access device and proximity access cards.
- + Any Non-Level3 personnel would be considered a visitor and must be escorted. We do have a visitors sign-in log which requires visitors to present a valid photo ID, reason of visit and a Level3 POC. Corporate security performs a monthly audit of security and visitor access logs.

At InterCall and InterCall subsidiary facilities, security is controlled by keycard access and strict visitor policies.

Document / Record Retention and Destruction

InterCall Streaming Services takes the privacy concerns of its clients very seriously. As such, we offer secure data destruction options for all stored data, involving multiple-pass data deletion/overwrite, as per DoD 5220.22-M guidelines. As all data is being moved to pooled SAN storage, data can be isolated on a per-volume basis, but individual hard disk degaussing/destruction on a per-client basis is no longer an option. In the event of a complete site hardware migration, all affected clients will be notified, and all decommissioned storage will be subject to a full multiple-pass data wipe, followed by destruction of the original drives by Iron Mountain, who can provide a Certificate of Destruction at that point.

Records on paper are destroyed via cross-cut shredder, and records on optical media can be destroyed as per corporate guidelines, involving destruction of the metallic layer via microwave, destruction of the media via cross-cut shredder, or both.

Application Security

Application security for InterCall Streaming Services is implemented through a proprietary access model. In general, most programs are secured through username and password. Additionally, mechanisms exist to limit access using an integration / single sign on approach where the customer pre-authenticates users and securely passes them to the application. There are a multitude of other methods to provision credentials and access to users that often includes a custom implementation based on customer requirements.

ROLE BASED SECURITY MODEL

All access to InterCall Streaming Services software is based on proprietary role based mechanisms which secure access to data, feature functionality, and services and reporting functionality at a highly granular level. Roles are configured on a per account basis, allowing a customer to fine tune roles to restrict access on a particular role type as desired. User roles are comprised of role module permissions (access to discrete

ACCESS SECURITY

Application access is typically provided for all user roles via a username and password, although customers may choose to provide anonymous or unauthenticated access to content as appropriate for the sensitivity of the content and intended audience. When accessing administrative modules a username and password is required. User accounts correspond to an implementation (customer account) and users cannot use one account to log into multiple implementations. The user roles associated with an account are a unique entity within an implementation, and user access security therefore may present differently to the user depending on the context that the user is accessing the application in. Logins are authenticated against hashed database passwords and assigned server based sessions accordingly. Session expiry duration will depend on the modules being accessed by the customer. Although the application does not mandate password complexity or expiration this can potentially be implemented based on customer requirements and with engineering support from InterCall Streaming Services. Customers leveraging our user authentication API may bypass username / password authentication in favor of a single sign on approach in some cases.



ENCRYPTION

Sensitive data can be secured using SSL. We are able to secure HTTP delivered content over SSL as well as streaming content over RTMPS or RTMPE. File data can be sent and delivered, optionally, over SFTP and a variety of file encryption types.

SSL security on all items is not the default configuration and should be requested during the client kick off or initiation call.

USER ACCOUNT PROVISIONING

User accounts are provisioned within the administration tool where the user data can be manually entered and a role selected or via batch spreadsheet imports. User accounts for less privileged roles (webcast participants) may occur through the registration system if that is the customer's chosen method of providing access or through the integration API (see Integration security).

INTEGRATION SECURITY

Customer wishing to integrate user authentication with an existing registration system or intranet may do so using our integration API which accepts user information and authentication details via a querystring which the user is directed to. It is possible to dynamically control the user's destination (webcast) using this method, however this method does not support access to administrative modules which must be accessed using a standard user account. By virtue of its design, the integration approach allows the customer to assume fine-grained control of what users are given access to content, how, and when. This API also exposes several security features to prevent tampering with / distributing of the generated link, such as shared secret hashing, timestamping, and / or full AES encryption on the querystring.

REGISTRATION SYSTEM SECURITY

Many customers will choose to provide access to content through the registration system for webcasts. Since the system is designed to allow users to register publicly for webcasts this should not be considered a secure option, but some mechanisms do exist to prevent unwanted access, including the ability to specify a password that registrants receive or allow registrants to create their own password. In some cases IP restrictions can be accommodated.

Infrastructure and Redundancy

INFRASTRUCTURE OVERVIEW

InterCall Streaming Services has documented and tested policies for business continuity and data recovery that involve redundancy in all critical IT aspects of our business. We have an alternate datacentre site also managed by Rackspace located in Herndon, VA. Additional streaming servers are deployed in London and Hong Kong, giving us global access to our customers without excessive dependence on trans-continental links to provide event services.

Beyond our basic capacity, we are also working with Level3 Communications to integrate their Content Delivery Network (CDN) with our systems, expanding our reach and our capacity without the time and cost of deploying multiple additional high-capacity datacentres.

Datacentre Locations

InterCall Streaming Services relies on a primary processing facility for data storage, located at Level3's datacentre in New York, New York. This co-located facility houses Fortigate firewalls with load balancing capability, Microsoft IIS web servers, Microsoft SQL database servers, custom-built media conversion servers, Adobe Flash Media Servers, and multiple terabytes of highly available synchronously replicated SAN storage, in addition to dedicated Intrusion Detection/Prevention hardware managed by AlertLogic.

Secondary datacentres rely upon direct-attached storage, but are still connected via redundant power, LAN, and Internet feeds from multiple carriers.

All datacentre locations:

- + New York, NY – Primary site
- + Herndon, VA – Secondary site
- + Dallas, TX – Streaming servers only
- + London, UK – Primary EMEA site
- + Hong Kong – Streaming servers only



CDN Integration Overview

InterCall Streaming Services has additional on-demand capacity via an agreement with Level3 for stream distribution via their Content Delivery Network. This network is fully redundant, with sites located worldwide. This redundancy, combined with our distributed streaming server architecture, allows us to deliver streams at any time as necessary

Redundancy

Internet

Internet access for this primary site is provided by redundant Gigabit Ethernet feeds over fiber optic media. Both connections are managed by Level3, with multiple diversified connections to the Internet backbone.

Power

All servers, storage nodes, and network devices have redundant power supplies configured and connected to isolated power feeds, backed by N+1 battery and generator backup, which is regularly tested by Level3. These power feeds are managed and monitored to ensure that a failure of a single power feed will not overload the remaining feed(s).

Devices

All critical server equipment utilizes redundant Gigabit Ethernet links to their respective VLANs, along with redundant network switches, allowing for uninterrupted network activity in the event of any single component failure. Additionally, capacity increases are designed with N+1 redundancy in mind, allowing for complete single server failure during maximum load without any effect on the performance of the InterCall Streaming Services Platform.

Data Centre Level

All relevant data, site content, server configurations, and SQL databases are replicated between the primary site in New York, and the secondary site in Herndon, VA, allowing for a rapid cutover to the secondary site in the event of a catastrophic datacentre failure. Between this backup site and our CDN arrangement, a failure at the Level3 datacentre will have a minimal effect on business continuity.

Backup

Data is backed up hourly using SAN-level snapshots, daily via incremental tape-based backups, and weekly via full tape backups. Incremental SAN snapshots are exported to our backoffice nightly, allowing for immediate volume recovery of all datacentre assets, and tape backups are removed and transported offsite on a weekly basis.