Hosted Customer Sites Security Protocol

Article Number: 140 | Rating: Unrated | Last Updated: Tue, Aug 23, 2022 at 1:46 PM

Hosted Customer Security and Downtime Protocol This article describes the Evanced Solutions hosting environment and processes/procedures applied to a security breach or downtime scenario. Definitions Hosted Server A server maintained by Evanced Solutions and provided to our customers for housing our applications (Events, Room Reserve, Genealogy, Signup, Dibs, and Spaces). The "Cloud" Evanced Solution's current hosting hardware architecture. The "cloud" is basically a hardware environment where there is a distinct separation between the software and the hardware. The operating system is virtualized in this environment and managed by a virtual software manager. This allows for 2 major benefits: The virtual OS can be moved or copied easily allowing for complete snapshot backups which provide quick catastrophic recovery times. The hardware can be replaced or modified quickly with little impact on the running system. In reality, this type of architecture is no different than a standard server from a user's perspective, but it does have significant benefits to the administrators. SSL SSL is a protocol that allows for an encrypted connection between the client (end user) and the server (application). Using this protocol protects the data that is passed between the browser and the server and makes it more difficult to see that data that is passed. All Evanced Solutions servers have SSL built-in. To utilize this protocol simply change all of your starting links from "HTTP" to "HTTPS". Some features require an SSL connection, primarily online payments. **Web Site Structure** Evanced Solutions applications consist mainly of a database application and a web site application. While it is possible for both of these applications to exist on the same server (most non-hosted installations use this method) our hosted solution uses an independent server for the database. This allows us to allocate specific resources to database tasks but also helps to ensure a degree of security. The database server is configured to allow only one type of connection (a connection to the database) and only from one of our hosting servers. This is accomplished through the network configuration and a series of firewalls. This type of configuration helps to ensure that the only connection made to the database server is one that we control from our application. **Downtime Failures** While we always do our best to ensure the highest up-times possible, the inevitable is bound to occur. Evanced technitions routinely monitor (and receive automatic notifications of) situations that can potentially be a downtime situation. In the event of a downtime situation our monitoring systems will email and text a list of Evanced Solutions contacts. We will work with our hosting provider to determine the cause. If the downtime situation is isolated, we will directly notify any customers whose sites were potentially involved. If the downtime situation affects more than a few sites, a description of the situation will be posted to our blog along with updates and resolutions as they become available. This type of failure can usually be classified into one of 2 categories; Hardware Failure or Configuration Update/Error. **Hardware Failure** A Hardware Failure is the easiest to explain but the least likely to cause downtime on our current system. A Hardware Failure is the failure of a physical component (hard-drive, network cable, etc.). The "Cloud" architecture and the network redundancy currently in use in our hosting environment (the Amazon Elastic Compute Cloud) provides quick, automatic switching when a hardware failure occurs. Most failures like this will not be noticed because the switching takes place nearly simultaneously with the failure. Virtual servers with duplicate images, redundant server hardware and network paths all help to ensure that this type of failure does not normally cause a downtime situation. **Configuration Update/Error** A Configuration Update/Error is an error or downtime event caused by a change in the application environment. At Evanced Solutions we strive for update, installation and maintenance processes that cause a minimal amount of downtime. Minor updates to the server and applications are applied routinely and reviewed for performance as soon as complete. Major updates are tested in a staging environment that is a duplicate (or a portion of) the entire production environment. We will generate an advance email and blog post for updates that affect more than one library. **Security Breach** A Security Breach is a situation whereby a connection to the database or server has been made by a means outside of our normal expected operation. Evanced Solutions routinely monitors (and receives automatic notifications of) situations that can potentially be a security breach. In the event of a security issue we will work with our hosting provider to determine the cause and evaluate the potential validity of the security breach. If valid, we will take steps necessary to isolate the method the breach used and we will directly notify any customers whose sites were potentially

involved.

Custom Fields Applicable To: All Users**Attachments:** No**Summary:** Hosting Security