Safeguard Your Data

Caspio Bridge Reliability and Security Overview

The flexible architecture and design of Caspio Bridge empowers users around the world to create diverse and innovative web applications that can be seamlessly deployed anywhere.

The increased productivity gained through Caspio is complemented by enterprise-class data security and highest level of service reliability. This document is an overview of the Caspio Bridge technology and its reliability and security measures.

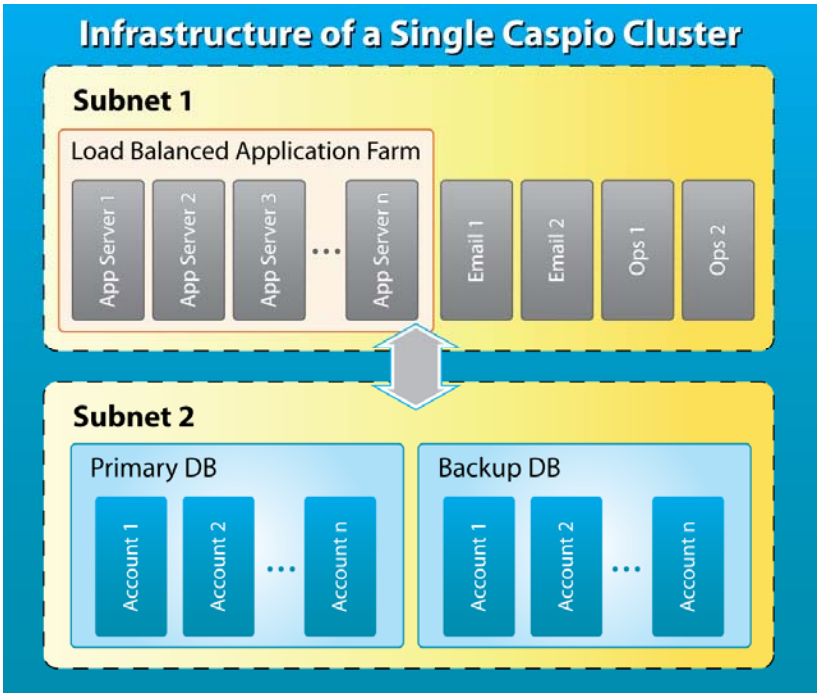
Standards-Based Technologies

We base our product innovation on proven and best-of-class standard technologies that have gained the trust of IT departments across companies of all sizes.

- Caspio is a **Microsoft Gold Certified Partner** representing the highest level of competence and real-world expertise with Microsoft technologies.
- The multi-tier technology of Caspio Bridge uses Microsoft SQL Server as its database, with business logic and proprietary patent-pending technologies primarily in .NET.
- The Caspio Bridge administrative console is a rich browser-based AJAX interface heavily utilizing XML.
- Deployed applications integrate seamlessly with any web site (hosted anywhere on any platform) and work with any browser.
- Caspio Bridge applications are entirely xHTML and CSS 2.1 compliant and our mobile applications are WML/WAP compliant.
- Caspio Bridge Web Services is SOAP compatible.
- Platform extension is possible through standard scripting and programming languages such as Java Script, ASP and PHP. Caspio does not use a proprietary language.

Platform Infrastructure

- The Caspio Bridge infrastructure consists of multiple clusters, each self-sufficient to achieve the highest levels of scalability.
- Each customer account is in its assigned cluster in a separate logical database schema. Customer data is not in shared tables.
- Each cluster includes a number of application servers. Additional application servers are deployed on-demand to address traffic spikes.
- Database servers are clustered in active/passive mode to ensure highest availability. Databases are in a subnet with no direct connectivity to the internet.
- Our infrastructure eliminates most single points of failure through live redundancies.



Caspio is powered by multiple clusters, each similar to this diagram.

Security and Reliability

At Caspio, we know that data security is crucial in order to trust a third-party with your data and applications. That's why security and reliability are not mere after-thoughts for us. These fundamentals are built into the fabric of our technology and services. Our platform implementation is based on state-of-the-art infrastructure and best practices that far surpass the requirements of most security-sensitive organizations and applications.

Our security measures are applied to multiple layers:

Physical Layer

Caspio's servers are owned and managed by Caspio and are co-located at a SAVVIS Tier 1 data center in the United States. Security measures provided by SAVVIS include:

- On premise security guards
- Exterior-building cameras, false entrances, vehicle blockades, parking lot design, bulletproof glass/walls, unmarked buildings
- Biometric systems which include palm scanners
- Security cameras with digital recorders, Pan-Tilt-Zoom (PTZ) capabilities
- Portals and man traps, only a single person authenticated at one time

Network and Systems Layer

Our network is protected by top-of-the line firewalls from industry-leading vendors. These firewalls remain up-to-date with upgrade and patches provided by vendors and they are configured to allow only the absolute minimum level of access to internet users.

Various security measures are employed and enforced inside of the perimeter firewalls and on internal systems. The exact nature of these measures is kept confidential.

All operating systems are kept current with all the patches recommended by their vendors. All unnecessary users, protocols, and ports are disabled and monitored.

Our databases can only be accessed through trusted authentication and are kept inside layers of protection.

Human Layer

All data maintained in your Caspio Bridge account is owned and accessed solely to you. Our employees do not have direct access to production equipment, except where necessary for system management, maintenance, monitoring, and backups. We do not outsource data management to service providers. Only select qualified Caspio permanent employees are allowed access to database servers, and only when their access is absolutely necessary. Caspio also performs highly-critical hiring practices and extensive background checks for administrative and IT positions.

Our technical support engineers can only log into your account when you specifically authorize them to do so, and only to resolve problems or issues reported by you. All account login activities are logged.

Application Layer

Caspio Bridge offers extensive features to protect and secure your account, data and applications:

- **Caspio Bridge Authentication** – All clients log into their Caspio Bridge accounts with a username and password. Caspio Bridge does not store sensitive user data in cookies or utilize other high-risk user or session tracking methods.

- **Data Encryption** – When you login to your Caspio Bridge account, your session is secured with 100% data encryption. When you deploy your DataPages and applications on your web site, you have the option of securing them through the same industry-standard SSL security at no extra cost. You also have the option of blocking non-SSL access to your data and applications. This ensures secure data transfer between your users and our servers.

- **Web Application Security** – You can activate Web User Authentication, a standard built-in feature of Caspio Bridge, to protect DataPages and applications that you deploy on your website. By doing so, all application end-users must enter a username and password and you will be able to manage these users. You can have an unlimited number of authenticated users for your applications. Caspio also provides CAPTCHA human verification security as a standard web application feature.

- **IP Blocking** – You also have the option of granting or blocking access to your applications and DataPages through IP addresses. Using this capability you can limit access to an application to your internal network.

SAS 70 Type II Compliance

Caspio's network infrastructure is housed in a state-of-the-art data center which conforms to the Statement on Auditing Standards No. 70 (SAS 70). SAS 70 evaluates company controls related to managed security services, change management, service delivery, support services, backup and environmental controls, logical and physical security.

A SAS 70 examination is widely recognized, because it represents that a service organization has been through an evaluation of their internal controls as they relate to an audit of the financial statements of its customers. A Type II report not only includes the service organization's description of controls, but also includes detailed testing of the design and operating effectiveness of the service organization's controls.

Caspio is focused on developing and refining systems and processes that fully secure our service delivery infrastructure. Our customers are faced with increasing compliance requirements and the SAS 70 examination is an important factor as they evaluate outsourcing their IT infrastructure.

Note: Use of the Caspio Bridge online service is subject to the Caspio Bridge Terms of Service. Caspio may change its security infrastructure and practices from time to time.