

# Arena Security & Availability

## Protect Critical Intellectual Assets with a Proven Financial Grade Security Infrastructure

Arena has created an ultra high security infrastructure by assembling leading technologies proven to be the most secure for each function. All firewalls and encryption devices are sourced from leading Internet security providers, configured by expert professionals, and tested rigorously before being placed into production. Our multi-tenant, single-instance architecture extends these benefits to all customers, protecting intellectual property and securing information from inappropriate access far more effectively than even the best on-premise deployments. Arena's extensive investment in a high-grade production networking system also provides near continuous system availability and fault tolerance.

### APPLICATION LAYER SECURITY

#### Application Security

Similar to multiple ATM machines accessing a centralized banking system, Arena's robust application security model prevents one customer from gaining unauthorized access to another customer's data when accessing Arena's centralized database system. This security model is applied and enforced for all Arena customers and staff.

#### User Authentication

Arena customer data can be accessed only with a valid username and password combination, which is encrypted via SSL for Internet transmission. Username and password verification is provided by a hardened authentication service that is maintained separately from the main application service. For further security, Arena does not store user passwords. Instead, all passwords are encrypted using a one-way hashing algorithm. Once an Arena session has been established, a randomized session ID cookie that does not contain username or password information is used to identify the user. Ninety minutes of inactivity causes the session to time out, after which a new session must be established in order to access customer data.

#### IP-based Access Restriction (Optional)

Arena offers our customers the option to restrict access to their Arena Workspace by IP address. Customers can define different access restrictions for different user groups, so that customer administrators can ensure that each user can access product data only from a trusted client network. This feature includes the capability to monitor and log user attempts to access the workspace from untrusted networks.

### DATA MANAGEMENT SECURITY

#### Data Encryption

Arena leverages the strongest encryption currently supported by browsers, using a 1024-bit RSA public key and allows users to access data with 128-bit encryption from their browsers. An SSL certificate—signed by authentication leader VeriSign and bearing the Arena domain name—as well as the lock icon in the corner of the user's browser, assure customers that their data is fully protected while in transit. In addition, all uploaded customer files are stored on Arena servers in encrypted form.

#### Database Security

Database access is controlled at the operating system and database connection levels for additional security. For each user session, the individual access to data is enforced at the database level, independent of the application layer, ensuring the highest level of data security. Access to production databases is limited to a minimal number of points. As with production servers, production databases do not share a master password database.

### OUR SECURITY PROVIDES:

- **Experienced**, professional engineers and security specialists dedicated to 24/7 data and systems protection
- **Continuous deployment** of proven, up-to-date security technologies, including proprietary products developed for Arena Solutions
- **Ongoing evaluation** of emerging security developments and threats
- **Complete redundancy** throughout the entire Arena Solutions online infrastructure
- **Total commitment** to a secure, scalable, private, co-location system (unlike a hosted system arrangement, Arena Solutions manages all aspects of its operations)

**SYSTEMS SECURITY**

**Internal and Operating Systems Security**

Within perimeter firewalls, Arena systems are safeguarded by a variety of security features such as network address translation, port redirection, IP masquerading, non-routable IP addressing schemes, internal firewalls, and other precautionary measures. Arena Solutions enforces tight operating system-level security by using a minimal number of access points to all production servers. For security, all operating systems are maintained at each vendor's recommended patch levels. Multiple, third-party security applications are used to ensure that each machine is secure before being placed into production.

**Perimeter Defense**

A strong perimeter defense is essential to prevent unauthorized or inappropriate system access. Arena secures the perimeters of both production and corporate networks with multiple firewalls. Primary production firewalls are managed by in-house technicians. An independent third party is employed to actively scan all public Arena IP addresses on all production and corporate networks for unauthorized open ports and known protocol vulnerabilities.

**Physical Security**

All of Arena's production equipment is owned and operated by Arena Solutions, and is co-located at a world-class co-location facility. Our co-location partner maintains 24-hour security at the co-location facility, with all visits logged against customer-defined access lists. Once authorization is confirmed, a cardkey lock allows visitors to access only their own equipment area.

**Reliability and Backup**

Arena further enhances its reliability by storing all customer data on redundant disks. To protect against data loss due to catastrophic events, all customer data is backed up on an hourly basis to a warm production-capacity disaster recovery site in a separate co-location facility, up to the last committed transaction. To further protect against data loss, archival backups of all customer data are created on a weekly basis and maintained for 26 weeks.

Availability: Arena Solutions has invested millions of dollars into world-class, state of the art infrastructure so you don't have to.

**Performance Guarantee**

As a multi-tenant, on-demand service, Arena brings economies of scale to its customers so they can benefit from a level of network availability and performance that is far greater than any solution they could ever hope to build for themselves using traditional client/server solutions.

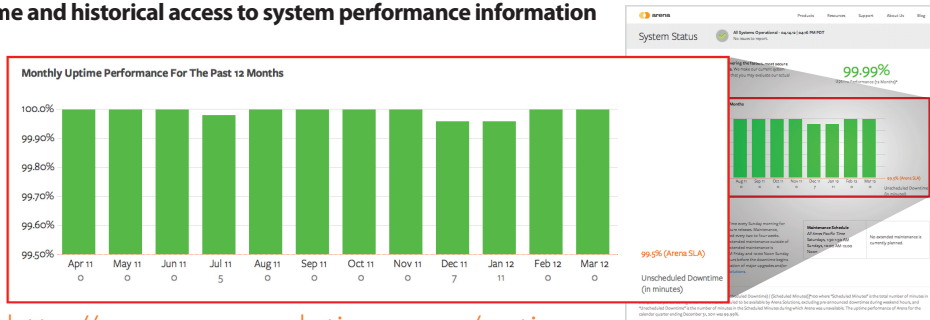
We guarantee an uptime of at least:

**99.5%**

Since inception of the service in 2001, Arena has had **more than 99.96% uptime** providing customers with unparalleled service performance and availability. But we don't expect you to take our word for it. Every Arena subscription comes with a **guaranteed service level agreement (SLA)** where customers can expect to receive a minimum planned uptime and availability of 99.5% on its service or they will receive a credit against their subscription.

Arena Solutions is committed to delivering the manufacturing community the best cloud solutions available today. That means providing customers with the greatest business value, highest network availability, most secure, and most reliable BOM and change management offering. To support this service commitment, Arena provides its customers with **real-time access to network availability**, uptime, and historical system performance so they can make **better informed decisions**.

**Real-time and historical access to system performance information**



<http://www.arenasolutions.com/uptime>

Arena BOMControl is the easiest to use, fastest to deploy, and most affordable BOM and change management solution available today, and provides manufacturers with unique business benefits that are simply not possible with traditional client/server solutions.

- Performance guarantee.
- Ironclad security.
- No software. No hardware. No IT.
- Instant on. Pay as you go.

**SALES CONTACT**

sales@arenasolutions.com  
p. 1.866.937.1438

**CORPORATE CONTACT**

Arena Solutions  
4100 East Third Avenue  
Suite 300  
Foster City, CA 94404  
P. 650.513.3500  
F. 650.513.3511

