



World-Class Security

FactoryDNA OnDemand™ Security Infrastructure

Overview of Security Infrastructure

FactoryDNA™ provides state-of-the-art security to ensure that your customer data is not compromised. At FactoryDNA, we know that security is crucial to you – that's why security is our top priority. We devote significant resources to continually develop our world-class security infrastructure.

Security Details

FactoryDNA OnDemand™ is configured by experts and rigorously tested before going into production, our world-class security infrastructure includes proven, up-to-date firewall protection, intrusion detection systems, SSL encryption, and other security technologies, including proprietary systems developed specifically for FactoryDNA.

Physical Security

Our production equipment is located in Austin, Texas at a facility that provides 24-hour physical security, keycard and hand geometry scanners, redundant electrical generators, redundant data center air conditioners, and other backup equipment designed to keep servers continually up and running.

Perimeter Defense

The network perimeter is protected by multiple firewalls and monitored by an intrusion detection system. In addition, FactoryDNA monitors and analyzes firewall logs to proactively identify security threats. FactoryDNA also proactively monitors our security configurations for changes, vulnerabilities, and errors and conducts vulnerability threat assessments including penetration tests.

Data Encryption

FactoryDNA uses the strongest encryption products to protect customer data and communications. The lock icon in the browser indicates that data is fully shielded from access while in transit.

User Authentication

Users access FactoryDNA OnDemand only with a valid username and password combination, which is encrypted via SSL while in transmission. A session key is encrypted and is used to uniquely identify each user.

Application Security

Our robust application security model prevents one FactoryDNA customer from accessing another's data. This security model is reapplied with every request and enforced for the entire duration of a user session. Every customer contains a separate logical database to eliminate the possibility of exposing customer's data to other users.

Operating System Security

FactoryDNA enforces tight operating system-level security by using a minimal number of access points to all production servers. We protect all operating system accounts with strong passwords, and production servers do not share a master password database. All operating systems are maintained at each vendor's recommended patch levels for security and are hardened by disabling and/or removing any unnecessary users, protocols, and processes.

Database Security

Whenever possible, database access is controlled at the operating system and database connection level for additional security. Access to production databases is restricted to a limited number of points, and production databases do not share a master password database.

Reliability and Backup

All networking components, load balancers, Web servers, and application servers are configured in a redundant configuration. All customer data, up to the last committed transaction, is backed up on a nightly basis. Disaster recovery plans are in place and are tested quarterly.