



Codesion Security is a powerful, seamlessly integrated portfolio of services, managed devices, hosted datacenters, and best practices - designed to deliver the highest level of security to customers.

Codesion Security includes four key components:

1. **Datacenter Security**  
Ensuring all servers, hardware, and internet connectivity offer customers the highest level of protection.
2. **Network Access Security**  
Involves using the latest patches, dedicated hardware/software firewall services, and software tools on regularly replaced servers.
3. **Operational Security**  
Involves creating internal policies that follow best practices to limit access to confidential customer data.
4. **Data redundancy**  
Involves ensuring that customer data is regularly backed up while ensuring easy accessibility.

#### Datacentre Security

- All customer data is stored on dual-CPU servers in SAS-70 compliant datacenters (Softlayer.com)
- Facilities connected via multiple redundant 10 gigabit backbone links
- Secured site perimeters
- CISCO Guard Denial of Service (DOS) Protection
- Tipping Point / IDS Protection
- Arbor Peakflow Traffic Analysis
- HVAC needs are supplied via five one hundred ton onsite water chillers to deliver N+1 cooling
- 6000 amps 480v Input Power
- 6 x 750Kva UPS Battery Backup Units
- 3 x 2000Kw Diesel Generator with Fuel Storage
- Pre-Action Dry Pipe Fire Suppression

#### Operational Security

- Data center access limited to authorized employees (Datacenter)
- Proximity Security Badge Access (Datacenter)
- Digital Video Surveillance (Datacenter)
- Codesion employees trained on documented information security policies
- Customer data is only accessed or manipulated at the request by the account owner in writing
- Access to confidential information restricted to authorized personnel
- System access logged and tracked
- All customer passwords stored in encrypted form

#### Network Access Security

- Server access is limited to secure protocols (HTTPS/SSL)
- Codesion servers undergo PCI Level 1 compliance testing every 90 days
- Servers are locked down so only pre-designated users can physically access their account data via a multi-master authentication system (LDAP)
- Customer backups stored on separate servers on a private (not routable on the Internet) subnet
- Dedicated hardware / software firewall services to block unauthorized system access

#### Data Redundancy

- Customer data is backed up every 10 minutes to separate servers on our private subnet, which has no public interface
- Private backups: Customers may elect to download (daily) Subversion / CVS modules, and Trac / Bugzilla database dumps
- RAID hardware used on all customer servers