

# The Brightidea Cloud Infrastructure

**BRIGHTIDEA**<sup>®</sup>  
THE POWER OF INNOVATION

## Benefits of On Demand vs. On Premise

- **Faster time to Launch and ROI**
  - Days , installing, and configuring software
- **Lower Launch Costs**
  - No initial outlay of cash for hardware and hardware
  - No initial outlay of cash for installation and configuration
- **Lower Total Cost of Ownership**
  - No need for headcount to maintain the system after it's launched
  - Upgrades are automatically built in
  - Experienced support staff available 24 x 7 x 365
- **Fast, Secure, Available, and Scalable**
  - Proven performance: continuously and globally monitored
  - Network and application scans ensures tight security
  - Geographically separate and redundant warm DR system
  - Shared infrastructure with spare and standby capacity
- **Proven**
  - Serving Brightidea clients for over 4 years
  - Proven over 99.9% availability
  - Audited and used by major financial enterprises
  - Serves over 1 Million registered users
- **Third Party audited: annual SAS 70 Type II Certification**

## World Class Data Center Facilities

- Primary data center in Virginia with DR site in California
- Redundant UPS power, diesel generator backup, and HVAC facilities
- Fully meshed, Tier 1 IP connectivity to multiple Internet backbone providers
- Redundant edge routers, firewalls, load balancers
- Management processes and procedures backed by SAS-70 Type II audits
- European Safe Harbor Compliant
- Highest levels of security: Layered Approach
  - **Layer 1: Physical Security**
    - 24x7x365 onsite security staff
    - Windowless, bullet proof exteriors
    - Entire perimeter bounded by concrete bollards
    - Shipping and receiving area walled off from co-location areas
    - Silent alarm system with automatic notification of law enforcement
    - CCTV digital camera coverage of entire center
  - **Layer 2: Network Security**
    - Edge network attack detection and prevention from Denial of Service attacks
    - Industry-leading firewalls and intrusion detection and prevention systems
    - Internal Intrusion Detection Systems (IDS) monitored and managed by top-tier third-party service providers

## End To End Security

- **Physical**
  - 24x7x365 onsite security staff
  - Biometric hand geometry readers to secure all doors, including cages
  - Fully anonymous, windowless, bullet resistant exteriors
  - Entire perimeter bounded by concrete bollards/planters
  - CCTV digital camera coverage of entire center, including cages
  - CCTV integrated with access control and alarm system
  - Motion-detection for lighting and CCTV coverage
  - Silent alarm system with automatic notification of law enforcement
  - Shipping and receiving area walled off from co-location areas
  
- **Network**
  - Edge network attack detection and prevention from DoS and DDoS
  - Industry-leading firewalls and intrusion detection and prevention systems
  - Intrusion Detection Systems (IDS) are monitored and managed by top-tier third-party service providers
  - All data encrypted during transmission using HTTPS or VPNs AES based encryption
  
- **Application**
  - IP Restriction
  - Periodic third party application scans
  - Strong password settings
  - Access controls on all resources
  - Sessions validated for each request including IP matching
  - Encryption of sensitive data at rest
  - Integration with client systems for SSO

## Performance and Scalability

- **Head room to handle 20x the traffic of the largest client**
- **Can provision extra capacity within 24 hours**
- **Capacity planning maintains head room**
  - Client launches are carefully tracked
  - Upgrades for Servers, Storage, and Network planned accordingly
- **Stress testing every 6 months of production system to validate capacity**
- **Over 1M registered users and growing!**

## DR and Data Backups

- **Daily offsite backups**
  - Encrypted during transmission and rest
  - Data recovery fully tested on periodic basis
- **Disaster Recovery Site**
  - Disaster recovery (DR) data center located in California – independent of primary and geographically separate
  - Warm standby servers
  - Recovery Time Objective of 48 hours in event of major disaster
  - Fail over fully and periodically tested

## Monitoring and Alerting

- **Availability and Performance Monitoring**
  - Global 3rd party web site monitoring
  - Internal monitoring and alerting of all web sites
  - Internal monitoring and alerting of all server resources, networks, and storage
- **Security Monitoring**
  - Intrusion detection
  - Network scanning

## Annual SAS 70 Type II Certification

- **Developed by the American Institute of Certified Public Accountants**
- **SAS 70 is an internationally recognized auditing standard**
- **A rigorous audit of a company's control activities and operations**
- **Performed by an independent firm**
- **Indicates processes and policies are adhered to**
- **Renewed annually**