Hosting Security

COMPU-DATA
International, LLC

Data onDemand™ Cloud Hosting Infrastructure Overview

CDI has direct partnership relationship with various Infrastructures as a Service (IaaS) secure cloud providers, serving the needs of clients and partners nationwide. During the selection process, CDI has ensured that our IaaS partners have the financial backing and stability needed to keep the infrastructure at state-of-the-art levels.

In addition to our Virtual FileRoom™ hosted product offering, our partner relationships allow us to offer product/service lines that include:

- Virtual servers – designed to meet a client's specific needs
- Cloud-based storage – 3 tiers of performance options
- Cloud-based backup – we are ExaGrid's exclusive cloud-based backup provider
- Cloud-based disaster recovery – options available depending on RTO requirements
- Cloud-based archival solutions – applications for client of all sizes and industries

Data onDemand

Infrastructure

Our cloud offerings are based on private-cloud architecture, as opposed to the public clouds such as Amazon, Azure, Google, and others. This architecture provides advantages in overall security (discussed below), and legal/compliance requirements. Best-in-class hardware and services from EMC, HP, Cisco, PureStorage Systems, Assureon, and vBlock are utilized. There are Tier IV data centers (highest rating) in Dallas, with other data centers geographically dispersed for redundancies, disaster recovery, and specific client needs.

TIER4
- Enterprise Corporations
- 99.995% Uptime
- 26.3 minutes Downtime Per Year
- 2N+1 Fully Redundant
- 96 Hour Power Outage Protection

TIER 3
- Large Businesses
- 99.982% Uptime
- 1.6 Hours Downtime Per Year
- N+1 Fault Tolerant
- 72 Hour Power Outage Protection

TIER 2
- Medium Size Businesses
- 99.749% Uptime
- 22 Hours Downtime Per Year
- Partial Redundancy in Power and Cooling

TIER 1
- Small Business
- 99.671% Uptime
- 28.8 Hours Downtime Per Year
- No Redundancy

Security

Security is addressed in several ways:

- Knowing where the data resides – our clients' is easily located for legal and compliance reasons
- The data center is equipped with water detection devices to detect and mitigate water damage in the event of flooding or water leak
- Physical security – the data is housed in Tier IV or Tier III facilities completely located in the continental U.S. (Dallas/Houston/Las Vegas, Louisville, Kentucky, Georgia, Norcross). The buildings are secured with: On-site security, 7x24x365, Feet-thick steel and concrete walls and vehicle barriers, No direct street access or outdoor signage, Biometric access (multiple points, with other security card points), Redundant power: in addition to diverse power feeds, there are 6-2000kW diesel generators with 6-3000 gallon fuel storage tanks
- User access to physical servers is provided only through a secure VPN connection, which includes multiple levels of network security in itself
- Application access is also available through secure VPN connection and/or https 128bit encryption.
- The data center meets SSAE-16, PCI, and HIPAA compliance requirements
- Quarterly penetration testing
- Intrusion Detection Services & Intrusion Prevention Services available (monitoring & prevention of web-based threats)
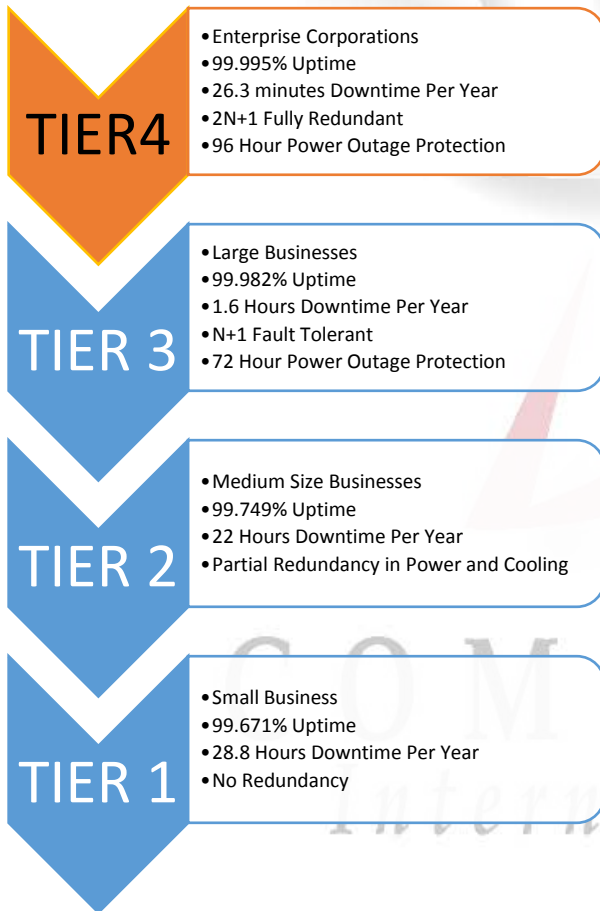
# FAQ'S

- ### Is the company viable?

Before handing over your critical applications and data, an important first step is to assess the financial viability of the company. Find out how long the company has been in business. Given the relative immaturity of this market, it may be unlikely to find vendors with several decades of presence, but you almost certainly don't want a company that has just set up shop either. In addition, look for any indicators of past or future economic issues, along with frequent leadership changes.

- ### Are service level agreements offered?

Yes we offer SLAs; and we can customize as needed. For organizations entrusting mission critical data to a vendor, you'll want to ensure that your systems will not suffer from frequent or extended outage periods. Downtime can have disastrous consequences both in terms of financial loss and damage to company reputation. For this reason, a service level agreement with negotiable terms should be available. This agreement should outline provisions for everything from server or software issues, to more detailed disaster recovery plans.

- ### How is security handled?

Perhaps the most frequent reason cited for not pursuing cloud computing is security. Many organizations have invested considerable financial and human resources in order to secure their network environments and the thought of abandoning that level of control and comfort to an unknown entity can seem like an unnecessary gamble. The platform is a fully-managed private virtualized cloud environment built upon enterprise-class Cisco UCS servers, EMC VNX Storage Area Network (SAN) STORGAE, Cisco Nexus switching, and VMware virtualization software.
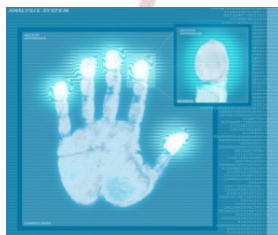
The decision to pursue cloud computing is one that many organization have or will make as this technology grows and matures. But this decision need not be one fraught with uncertainty. With a little due diligence, and answering a few key questions, you can ensure that your cloud vendor selection is a sound one.

If you're unsure whether or not the cloud is right for you, take a look at this article from vExpert David Davis on What "The Cloud" Really Is and Is It Right For You