DATA CENTER SPECIFICATIONS

Our cloud services are powered by wholly owned equipment co-located in large-scale, secure, enterprise-grade datacenters in Salt Lake City and Las Vegas. These facilities are designed for 99.999% reliability (no more than 5 minutes average downtime per year), are SSAE 16 Type II Certified (replacement for SAS 70 Type II), and are HIPAA and PCI Compliant. While specifications of each facility vary slightly, all are designed to be highly secure and fault tolerant.

Security
- 10 foot razor fence with 24/7/365 surveillance and patrols by armed security guards.
- State of the art data center ID system and security including video surveillance and recording.
- Multi-level identity verification, including biometric scanning, card keys, and badge authentication.
- Real-time IPS and multilevel firewalling, which comprehensively autoblock sources of rejected traffic.

Power (2N+1)
- Multiple utility feeds from separate substations with diverse building entry
- 11 generators providing a total of 7 MW of power, with in-ground fuel tanks to provide uninterrupted power for several days of outages. Fuel contracts guard against long-term outages.
- A+B feeds to each cabinet with A+B computing equipment, with each feed backed by independent N+1 power paths, including breakers, UPS systems, generators, and main feeds.
- A connection to the most reliable power grid in the state of Georgia through quad vaults on 4 feeds. This grid protects the main hospital in Atlanta so it is on a last outage program for critical services and was extensively upgraded for the Olympics. For the last 8 years the generators have only been used for testing.

Environmental Controls (N+1)
- Environmentally friendly chilled water cooling, fed by redundant water sources (private well, city main), and powered by redundant pumps and paralleled 500-ton cooling towers.
- Redundant Liebert Air systems providing consistent temperature and humidity range throughout the 70,000 square feet of datacenter space.
- Continual environmental monitoring in each cabinet and through the data center, with threshold alarms monitored by the 24/7/365 NOC, providing fast resolution of anomalous conditions.
Network (2N)

- Redundant Cisco BGP routing and switching infrastructure with cold spares on site. If equipment failure occurs, there is no interruption of service.

- 62 Gbit/sec Internet connectivity, delivered through multiple independent fiber rings and lines. Dual feeds of all aggregation routers ensure 100% uptime - some of the best in the business.

- Avaya ANS BGP4 management system optimizing the routes on the network in real time, 7000 times per minute based upon trace route performance, to ensure low latency and high throughput.

- 6 backbone providers who are publicly peered with 12 providers including Earthlink. Our current network consists of multiple 10 Gig or Gig links to Abovenet, Cogent, Level 3, nLayer, SAVVIS, TeliaSonera, XO, and the Atlanta Internet Exchange public peering point.
DATA INTEGRITY AND SECURITY

When dealing with millions of GBs of data (petabytes), the utmost care must be taken to ensure that customer data is protected and preserved by adhering to the highest standards of data security and by providing systems that guarantee the integrity of the data. Although many cloud service providers talk a lot about data encryption, most don’t discuss or provide mechanisms to guarantee the integrity of the data, which is equally as important. After all, what good is your data if it becomes corrupted or damaged?

Silent data corruption is a real threat to your data. In a recent study by CERN, silent data corruption was observed in 1 out of every 1500 files. Redundant storage, RAID, mirroring, checksums on individual components, replication, and even backup are not sufficient to protect against silent data corruption. If data is silently corrupted without detection, this corrupted data is then replicated or backed up, thereby corrupting any redundant or backup copies. The causes of silent data corruption are many and include hardware, firmware, and software faults.

Our data integrity protection systems are second to none. Our end-to-end 256-bit checksums “tag” your data with cryptographically verifiable identifiers, and these checksums are then used to verify the integrity of the data throughout the entire process. If corruption within a particular block is detected, a redundant copy of that block is used to automatically repair the corruption.

The redundant copies of the data are split across physically separate raw storage devices each located in physically distinct storage subsystems. Storing the redundant copies physically far away from each other ensures that clusters of disk failures due to localized vibration, enclosure failures, or IO controller failures do not affect more than one redundant copy of the data, providing an unparalleled level of protection.

In addition to automatic detection and repair upon data access, all data is periodically verified against their end-to-end checksums to proactively identify and automatically repair silent data corruption.

As an additional measure of data integrity assurance, every data block backed up to our cloud is digitally signed by your encryption key and then verified during restore. This provides cryptographic assurance that your data has not been tampered with by anyone and is 100% identical to what was originally backed up.
We’re also serious about data confidentiality. In addition to our in-depth network security mechanisms, our services adhere to stringent internationally accepted standards for data encryption and network transmission, including Blowfish 440-bit, FIPS-197, NIST 800-38A, HMAC-SHA-256, PBKDF2, and RSA 3072-bit.
SECURE, ALWAYS-ON NETWORK

High performance and resilient internet connectivity is crucial to providing fast and reliable cloud services. Our network connectivity has unparalleled redundancy and performance, utilizing geographically diverse external fiber paths, distinct fiber entrances, mesh routing, and extensive peering relationships. Actual measured uptime over the past 5 years exceeds 99.998%—even if scheduled maintenance periods are included in the uptime measurements. The network has truly proven itself to be an always-on network. Security is equally important at every layer and participant in the network. Real-time security ensures threats are stopped cold. Attempted network probing or rejected packets cause senders to be immediately blocked. Separate and independent firewalls dedicated to each storage node combined with security filters inside the switching fabric provide deeper isolation, segmentation, and threat identification and mitigation.
Monitoring and Management

Real-time monitoring of all networks, servers, services, storage, and other key IT infrastructure is critical to providing reliable cloud services you can depend upon. We use two separate external and an internal automated monitoring systems, which leverage differing technologies to monitor the same systems. This diversity of monitoring technologies and systems ensures that our engineers will always be alerted of degradations in fault tolerance or performance. Alerts are processed 24/7/365 by our team of engineers.

We operate true “lights-out” data centers. Once new equipment is physically installed, our engineering team has comprehensive control over every component in the data center. Except for the replacement of failed physical components, our engineers can diagnose and resolve issues faster than if we were standing right there in the data center. Additionally, all data center facilities are staffed by qualified data center engineers 24/7/365 (including holidays) to quickly install or replace equipment or cabling.

Power, temperature, humidity, component/service health, and performance metrics are collected across our entire infrastructure every few minutes and aggregated into a single global dashboard monitored by our team. Our years of performance introspection and fine-tuning allow us to provide cloud services with unparalleled levels of performance, reliability, and availability.
SAFE AND SECURE LOCATION

Our locations are far from flood plains and liquefactions zones. The facilities are constructed with appropriate seismic reinforcements, and building construction is encased in granite or 6” cement walls.

Physical security takes a defense in depth approach. Razor fences, patrols by armed security guards (who are often off-duty police officers with the authority to make arrests), perimeter lighting, and video surveillance and recording protect the exterior.

Our data centers are strategically located within disaster-safe regions, providing a safe home for your data. Entrance to the facility and data floor spaces are protected by multi-level security measures, including photo identity verification, biometric scanning, card keys, and badge authentication. All equipment coming into or out of the building is checked by the guards, audited, and logged. Individual equipment cabinets utilize locking front and back doors combined with video surveillance and recording.
**COMPLIANCE AND EXTERNAL AUDITS**

We understand the importance of transparency into the operating controls and procedures for the facilities that contain your data. That’s why we’ve partnered with facilities that meet the highest industry standards, such as SSAE16 and SAS70, and are compliant with key industry regulations, such as HIPAA and PCI. SSAE16 and SAS70 are standards created by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA) that require companies to enumerate the risks to their operations, and document their controls and procedures to mitigate these risks. Additionally, in a Type II audit, an independent accredited firm will frequently audit the actual operations of the business at random intervals during a 6 month period. Auditors record whether controls and procedures are accurately being followed. Our data center facilities have all achieved successful SSAE16 or SAS70 audits that are renewed on an annual basis. The auditor’s detailed report is available upon request.

PCI is another important industry regulation that provides rules and regulations for companies that process credit card information. Companies that are required to follow PCI regulations must ensure that any data centers containing sensitive cardholder data also follow PCI regulations. In order for a data center to be PCI compliant, any sensitive areas of the data center that store, process, or transmit cardholder data must adhere to the following security standards (SAQ Validation Type 5, SAQ v1.2 D):

9.1 Appropriate facility entry controls should be put in place to limit and monitor physical access to systems in the cardholder data environment.

9.1.1(a) Video cameras or other access-control mechanisms should be used to monitor individual physical access to sensitive areas.

9.1.1(b) Data collected from video cameras should be reviewed and correlated with other entries.

9.1.1(c) Data from video cameras should be stored for at least three months (unless otherwise restricted by law).

9.1.2 Physical access to publicly accessible network jacks should be restricted.

9.1.3 Physical access to wireless access points, gateways, and handheld devices should be restricted.

9.2 Procedures should be in place to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible.

9.3 All visitors should be handled as follows:

9.3.1 Visitors must be authorized before entering areas where cardholder data is processed or maintained.

9.3.2 Visitors must be given a physical token (for example, a badge or access device) that expires and that identifies the visitors as non-employees.

9.3.3 Visitors must be asked to surrender the physical token before leaving the facility or at the date of expiration.

9.4(a) A visitor log should be used to maintain a physical audit trail of visitor activity.

9.4(b) The visitor’s name, the firm represented, and the employee authorizing physical access should be documented in the log.

9.4(c) The visitor log should be retained for a minimum of three months (unless otherwise restricted by law). All of our data center facilities have controls in place to ensure that these requirements are met.
ENVIRONMENTAL AWARENESS

When data centers were first being built, nobody really thought much about things like energy efficiency and environmental impact. But we’re helping to change that. While servers and storage still require a significant power supply of electricity, a carefully maintained indoor environment, and fail-safe backup systems, we’re developing new ways to do it all in a more sustainable way.

When Bigger is Not Better

The temptation for any successful organization is to build the largest, most impressive structure you can afford. But according to the Leadership in Energy and Environmental Design (LEED) Green Building Rating System, developed by the U.S. Green Building Council, the less material you use in the construction of your building the better. We’ve built our Data Center with a minimum of materials that are not required for effective operation. A grand entryway may be impressive to a few clients, but the more drywall, marble and paint that goes into a facility the more energy is required to make and install those materials. And using more materials also results in more volatile organic compound being produced in the manufacturing of the materials. It also takes energy to transport these materials, which, along with their byproducts, end up in our landfills.

Keeping Cool and Still Using Less

Heat Pumps to Recycle Data Center BTUs

It doesn’t take many computers to generate a lot of heat, but it’s important to their stability that they run in a carefully controlled climate. Many data centers use additional gas or electricity to heat and cool the non-data portions of their facilities. But we’re implementing heat pumps that utilize the heat from the data center to heat the offices and generator rooms in the winter and utilize the data centers highly efficient cooling towers to provide cooling to the offices in the summer. This not only saves us money on burning gas or electricity to heat the space, but is more environmentally friendly. Our use of well water for the cooling towers also provides geothermal heat removal since all the water being input to the towers is from the earth at a constant 55 degrees Fahrenheit which removes BTUs from the water and building naturally.

Geothermal Cooling

Another cooling resource we’re exploring is the use of well water in an outside cooling tower. As mentioned above it gives us natural BTU removal through geothermal cooling but it also gives us a big savings in water replacement and reduces the amount of electricity needed to distribute city water over long distances and the harmful chemicals used in its treatment for drinking purification, as well conserves potable water in the city’s watershed.

Air to Air Heat Exchange

Another cooling resource we’re exploring is the use of well water in an outside cooling tower. As mentioned above it gives us natural BTU removal through geothermal cooling but it also gives us a big savings in water replacement and reduces the amount of electricity needed to distribute city water over long distances and the harmful chemicals used in its treatment for drinking purification, as well conserves potable water in the city’s watershed.
Optimizing Pumps and Fans for Better Efficiency

Under the old way of designing a cooling system, you’d hire an engineering to come in and do a Doppler flow study on your water distribution pipes to make sure that the pumps when running at full speed were providing enough gallons per minute to your air conditioning units to remove enough BTUs from the air. Then you would manually adjust flow restricting valves that would “balance” your system to the proper amount. This is highly inefficient because pumps running at 100% are using most of their energy to achieve the last 30% of the motor curve. Also, when the amount of water the pump is able to move is restricted, it works harder, uses more energy, and reduces its effective life.

State of the Art VFD and Computer Optimizing Systems

Water Pumps Fueling the A/C Units

Backup Power Generators
Cutting Needless Packaging By Up To 66%
Because we're constantly upgrading, we receive a steady stream of new equipment and supplies. Unfortunately, it's not readily recyclable in most areas and a huge amount of "filler" ends up in landfills. To cut down on needless packing materials, we've requested that our suppliers ship our new equipment to us in bulk packaging when possible.

And Recycling Just About Everything
We recycle our cardboard, metals and our old computers. Nothing goes to landfills except non-recyclable garbage. We're serious about our commitment to the environment. As a customer, you can be sure that we're doing our best to be Atlanta's least wasteful, most energy efficient data center.