RIA WorkSpace

Powering the Cloud Desktop:
OS33 Data Centers

Info@RIAWorkSpace.com

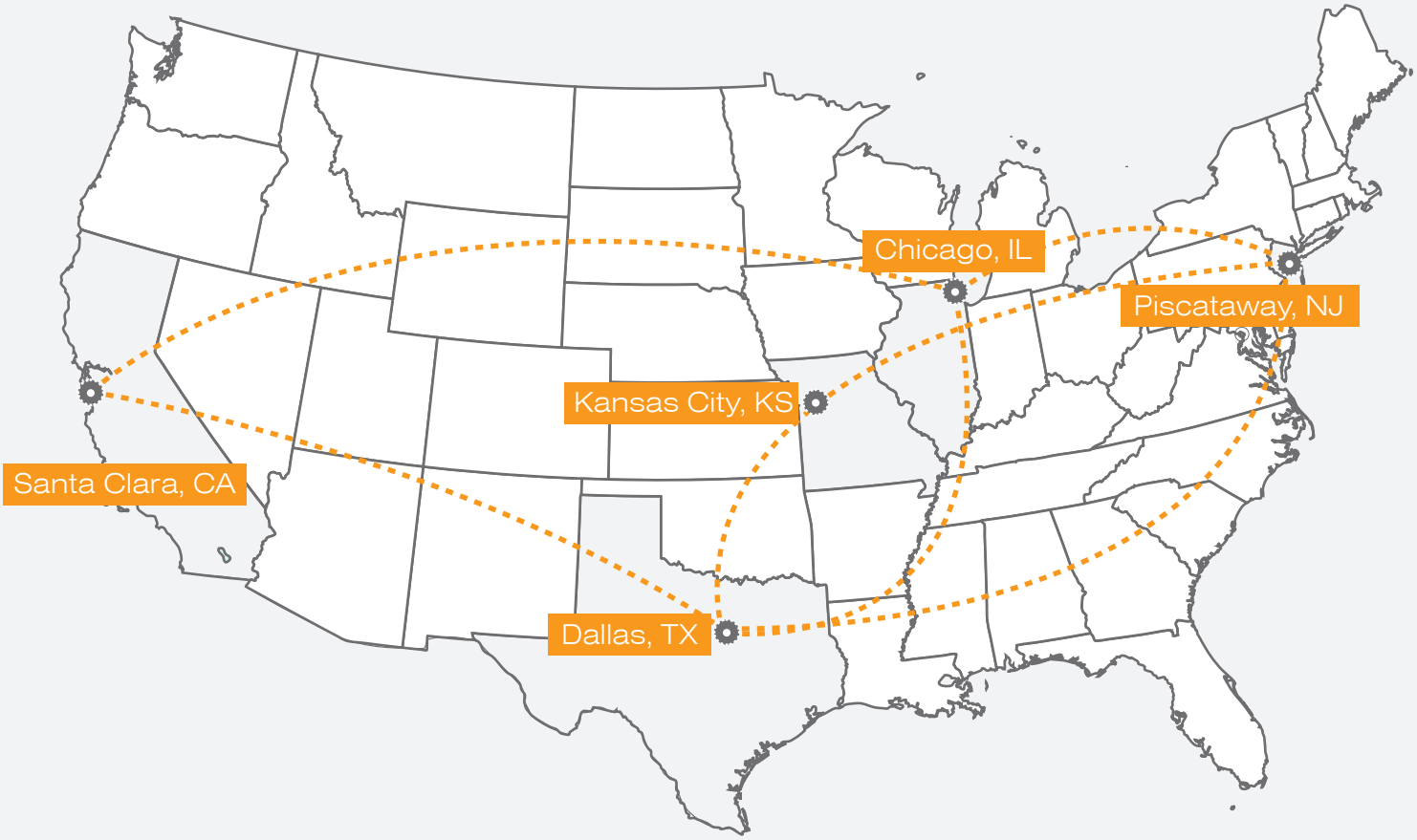
877.361.3499

www.riaworkspace.com

Powering the Cloud Desktop:
Our Data Centers

It is hard to overstate the importance of security and uptime, which is why we obsess over making sure that your corporate information assets and business-critical applications are always running and secure. Our data centers are at the forefront in terms of quality, security and reliability.

U.S. Data Center Footprint



OS33 has secure, geographically dispersed data centers to minimize latency, provide for disaster recovery, and best serve our clients whose offices span the United States and beyond. They provide a level of security and protection far greater than almost any small or midsize firm could build on their own.

99.99% UPTIME GUARANTEED BY SLA

Powering the Cloud Desktop:
Our Data Centers

Physical Access

Access to OS33 Data Centers is restricted to authorized personnel by security officers and two-factor authentication that includes biometric scanners. All entrances and common areas are monitored 24/7 via closed-circuit cameras, and recorded continuously. At a minimum, all our facilities must employ the following security features.

- Staffed 24/7/365 with on-site security officers
- Visitors screened upon entry, identity verified, and escorted to appropriate locations
- Doors secured using biometric hand geometry readers and pass codes
- Building exterior fully anonymous, no windows, identifying marks and is bulletproof
- All entrances protected with silent alarms and automatic notifications to authorities
- Hi-resolution digital video cameras with archiving/retrieval capabilities

Physical Structure

The building shell, exterior, floors, and roof of all OS33 Data Center facilities meet or exceed local building codes and standards. In order to provide further protection, these facilities are built to effectively manage and withstand the effects of fire, flood and earthquakes.

Fire Suppression

- A dual-alarmed, dual-interlock, multi-zoned, water-based dry pipe fire protection system ensures an ideal environment.
- Sensory mechanisms (HSSD) are utilized to sample air and sound alarms prior to water pressurization.

Flood Control & Earthquake Management

- All OS33 Data Centers are above sea level, as well as 500-year flood plains. They have no basements, have tightly sealed conduits, and moisture barriers on the exterior walls.
- Every OS33 Data Center contains dedicated pump rooms, drainage/evacuation systems, and moisture detection sensors.
- OS33 Data Centers are built to meet or exceed seismic design requirements of local building codes for lateral seismic design forces.

Powering the Cloud Desktop:
Our Data Centers

Environmental Control

- In order to provide optimal environmental conditions for operation, the HVAC systems provide OS33 Data Denters with appropriate levels of airflow, temperature, and humidity.
- The HVAC systems use N+1 redundancy configurations and are also backed up by redundant diesel generators.

Enterprise-level Infrastructure and Backbone

- OS33 Data Centers feature Cisco multilevel architecture with redundant fiberoptic connections from multiple Tier 1 carriers. We provision a variety of dedicated circuits, including Gigabit Ethernet (GigE).

Redundant Power Systems

Redundant power includes uninterruptible power supplies (UPS) and backup generators, including on-site multiple-day fuel supply. Generator power is activated automatically in the event of a grid failure.

- Carrier diversity via multiple Tier 1 providers
- Redundant backup diesel generators, including on-site multiple-day fuel capacity
- Redundant 208v/30amp power to each cabinet
- N+1 HVAC
- N+1 UPS
- N+1 generators
- N+1 power distribution units (PDU)
- Full network tape backup services, offsite storage, and disaster recovery

NO SUCH THINGS:
UNICORNS
TOOTH FAIRY

OR

TOO MUCH
IT SECURITY

Powering the Cloud Desktop:
Our Data Centers

SSAE16 SOC1 Type II Certification

SSAE16 is an internationally recognized auditing standard, which gives you confidence that we follow the most rigorous standards for controls and safeguards available when hosting or processing your data. You will save time and money using our compliance reporting to support your own audit requirements.

Network Security

With OS33, your network will have security built into the infrastructure, from end-to-end. Among other tools, we use managed Cisco firewalls, enterprise-level security appliances and intrusion prevention systems. We also backup our clients with fully redundant security appliances. In the end, if your business isn't safe, neither is ours.

Intrusion Detection and Prevention Systems

OS33 employs systems that actively monitor all network traffic to detect any attempt to log in or access resources without authorization. If suspicious activity is detected, protective measures are taken and our technicians are notified immediately.

Centralized Security & Password Controls

Centralized systems make our network infrastructure easier to secure. A single point of access, connected to centralized permissions ensures that all users are properly authenticated and only have access to appropriate applications and data. Our built-in password management controls further strengthen security and facilities compliance, and adhere to government regulations.

Network Operations Center

We continuously monitor each piece of hardware and every service running within our OS33 Data Centers from the Network Operations Center 24/7/365. We make sure everything is up and running and working properly. If there's an issue, we resolve it, most of the time well before you even know about it.

Our Network Operations Center is responsible for:

- Proactive network management
- 24/7/365 monitoring of all systems
- Daily monitoring of all backups and security threats
- Deploy software upgrades and patches
- Troubleshooting and resolution
- Monthly trend and performance analysis
- Virus protection and security analysis
- Preventive maintenance to reduce network support needs

End-to-End Encryption of Remote App Delivery

With our hosted application delivery, data is kept in your chosen OS33 Data Center, while only screen updates, mouse clicks, and keystrokes travel the network.

As for those things that do traverse the Internet, we provide centralized password control, multi-factor authentication, and encrypted delivery.

Powering the Cloud Desktop:
Our Data Centers

We Audit Our Technicians

We incorporate expiring passwords, as part of our password tracking system, and change passwords on a regular basis. Access to a client's private file storage area is restricted, and heavily tracked and audited for accountability. Whenever a support technician is working with a client, troubleshooting or resolving issues, their actions are logged by a tracking system. In the unlikely event of suspicious behavior, a record exists to determine and remedy any possible wrongdoing.

Regulatory Compliance

Every OS33 Data Center is SSAE16 SOC1 Type II compliant, meets Securities and Exchange Commission (SEC) requirements, complies with the Sarbanes-Oxley (SOX) Act, and Health Insurance Portability and Accountability Act (HIPAA) guidelines. OS33 Data Centers absolutely meet these requirements.

We've gone to great lengths to ensure our data centers are both mother nature proof and intruder proof.

For questions and to learn more, please contact us.

Info@RIAWorkspace.com 877.361.3499 www.riaworkspace.com