Spider Strategies®

Spider Strategies® Hosted Solutions: Data Centers, Security and Support Services

October 24, 2025

Table of Contents

Spider's Hosted System – Data Center Providers

Spider Strategies works with three high-security Data Center Providers to host customer installations: Linode, Rackspace, and Amazon Web Services (AWS):

- **Linode (multi-tenant):** Our standard cloud hosting option, Linode.com (est. 2003) is now owned by Akamai Technologies. Linode provides high performance Linux-based virtual servers hosted in strategically located data centers. Spider customers' data is primarily hosted in Dallas, TX and Frankfort, Germany data centers, but other geographies are available.

- **Rackspace (multi-tenant):** Our legacy hosting option, Rackspace.com (es. 1998) hosts Spider customers who started their hosted services prior to October 2017. These servers are physical Windows-based servers located in an Ashburn, Virginia data center. Our Rackspace offering is a secondary option for customers who have special circumstances requiring non-standard technical configurations.

- **Amazon Web Services (single-tenant):** Our premium hosting option. AWS is recommended for customers who require their own dedicated server or have especially high security requirements such as restricting access by region.

Following is detailed information about our three hosting providers:

Hosted Installations with Linode

Spider Strategies' hosted installations with Linode.com (est. 2023, owned by Akamai Technologies) are currently housed on multi-tenant, Linux-based virtual servers. These systems are primarily hosted at either their Dallas, TX or Frankfurt, Germany data centers depending on each customer's geographic location or preference. Other geographic locations are available.

Linode Overview

Web: http://www.linode.com
Contact: 1-855-454-6633
Email: support@linode.com

The Fundamentals

- Founded in 2003
- Acquired by Akamai Technologies in 2022
- Linode is based in Philadelphia, Pennsylvania
- Data Centers operating within 26 core compute regions globally
- Data Centers host high performance SSD Linux services operating KVM (Kernel-based Virtual Machine)
- Over 400,000 customers
- 99.99% Uptime Guarantee by Linode for its Linux virtual servers
- Data Centers are compliant with HIPAA (U.S. Health Insurance Portability and Accountability Act) and PCI Data Security Standard (PCI DSS)
- Linode's security infrastructure includes:
    - Physical and Environmental Security: Linode ensures the security of its data centers through controlled access, surveillance, and environmental safeguards to protect against unauthorized access and physical threats.
    - Network Security: Linode employs advanced Distributed Denial of Service (DDoS) protection to defend against large-scale attacks, ensuring network stability and availability.
    - Infrastructure Monitoring: Continuous monitoring of systems and networks allows Linode to detect and respond to potential security incidents promptly, maintaining the integrity and availability of services.

Linode themselves operate within KVM or Xen virtualization, which ensures that each Linode has its own kernel and userspace, which are fully separate from other Linodes. This ensures that a malicious Linode cannot access either the host itself or other Linodes' resources.

Hosted Installations with Rackspace

Spider Strategies' hosted installations with Rackspace are currently housed on multi-tenant physical Windows servers hosted by Rackspace at their IAD3 Data Center in Ashburn, VA. Longtime customers who began their Spider hosted services prior to October 2017 are housed on these systems. Rackspace hosting is also a secondary option for standard customers who have special circumstances requiring non-standard technical configurations.

Rackspace Overview

Web: http://www.rackspace.com
Sales: 1-800-961-2888
Support: 1-800-961-4454

The Fundamentals

- Founded in 1998
- Based in San Antonio, TX
- A long-time leader in IT infrastructure and multi-cloud solutions.
- Spider Strategies' hosted installations housed at Rackspace's IAD3 Data Center in Ashburn, Virginia.

Physical Security:

- Data centers are protected by multi-layered physical security, including:
    - 24/7 surveillance and monitoring
    - Biometric and keycard-controlled access
    - Security staff on-site around the clock
- Facilities are built to withstand natural disasters, with robust power redundancy and climate control systems.

Compliance and Certifications:

- Rackspace data centers adhere to globally recognized compliance standards, such as:
    - ISO 27001: Information Security Management
    - SOC 1, SOC 2, and SOC 3 reports
    - PCI-DSS compliance for secure handling of payment data

- These certifications demonstrate their commitment to safeguarding customer data and operations.

Network and Infrastructure Monitoring:

- Rackspace employs enterprise-grade monitoring systems to oversee the health of their physical and network infrastructure.
- Advanced threat detection mechanisms and regular audits minimize the risk of unauthorized access or downtime.

DDoS Protection:

- Their colocation services include optional DDoS protection, safeguarding your infrastructure from distributed denial-of-service attacks.

Disaster Recovery and Redundancy:

- Facilities are equipped with redundant power, cooling, and connectivity to ensure maximum uptime.
- Multiple data centers offer geographic diversity for enhanced disaster recovery options.

Hosted Installations with Amazon Web Services (AWS)

AWS is Spider Strategies' premium hosting offering for customers who wish to be hosted on a single-tenant server. This is the preferred option for customers who have exceptionally high security requirements – such as having a dedicated virtual server not hosting other customers' systems, restricting application access to specific geographies, etc.

At present, Spider Strategies hosts servers in three AWS Availability Zones:

- **us-east-2 (Ohio, USA)**
- **ca-central-1 (Toronto, Canada)**
- **me-central-1 (Dubai, UAE)**

Amazon Web Services Overview

Web: https://aws.amazon.com/
AWS Customer Service: 1-888-280-4331

The Fundamentals

- Founded in 2006
- Headquartered in Seattle, WA
- Global leader in cloud infrastructure, offering Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS).
- Operates 100+ Availability Zones within 30+ geographic regions worldwide, with plans to expand further.
- Compliance-ready infrastructure with a broad set of global and regional certifications, including GDPR, FedRAMP, HIPAA, SOC 1-3, ISO 27001, and PCI DSS.
- Backed by a 99.99% uptime SLA for compute services.

Physical Security:

- AWS data centers employ state-of-the-art physical security measures, including:
    - 24/7 surveillance and on-site security personnel.
    - Biometric scanning and keycard-controlled access.
    - Facilities designed to withstand natural and man-made disasters.

- Network Security:
    - Advanced Distributed Denial of Service (DDoS) protection with AWS Shield.
    - Web Application Firewall (AWS WAF) for enhanced protection against web exploits.
    - Encryption for data in transit (TLS) and at rest (AES-256).

- Infrastructure Monitoring:
    - AWS provides comprehensive monitoring through Amazon CloudWatch, offering real-time insights into server performance and security.
    - Proactive threat detection with Amazon GuardDuty, using machine learning and threat intelligence.
- Disaster Recovery and Redundancy:
    - Multi-Availability Zone deployments ensure high fault tolerance.
    - Elastic Load Balancing and auto-scaling features optimize performance during traffic surges or failures.

- Compliance and Certifications:
    - AWS adheres to global security and compliance standards, including:
        - FedRAMP High for government workloads.
        - FIPS 140-2 for cryptographic compliance.
        - ITAR compliance for defense-related workloads.
    - Regular third-party audits validate AWS's infrastructure security.

- Advanced Security Features:
    - Identity and Access Management (IAM) for granular permissions and access controls.
    - Hardware Security Modules (HSMs) for dedicated encryption key management.
    - Amazon Inspector for automated vulnerability assessments.

Access to Your Hosted Environment

Who can access your hosted environment and the data stored within it?

A single solution (Spider Impact®) operates as a powerful web application instance that can host many customer accounts. Customer data is isolated from other customers in that each customer has their own dedicated MySQL database on the server accessible by their own unique web address (URL). When a user logs into the software via their unique web URL, the software establishes a database connection directly to their dedicated MySQL database. It is not possible for the user to gain access to another customer's database - unless they are provided a URL, username, and password by that other customer.

Spider Strategies' Staff Access to Your Hosted Solution Database

- Our technical support staff will have administrative access to your database for support and system management reasons only
- All support staff have undergone and passed background checks

Your Staff's Access to Your Hosted Solution Database

- You can assign Administrative authority to a specific user or users
- Spider's User Administration requires that each person have their own user account (user name / password) with the possibility of enforcing password complexity rules
- You can control which users have access to specific data, specific views, specific objects and what types of specific actions they can take within the system (from Power Users to View Only Users)
- The software utilizes "Group Security" where a user can belong to one or more security groups. These groups provide a granular customization to security in the system - with the members of each group being able to perform particular permitted actions within particular "Organizations" (content in the solution is organized by Organization / Business Unit). A user can belong to one or many groups.

- Spider does support LDAPS (Active Directory), OpenID (OAuth2, Azure AD), and SAML (Okta, ADFS) in the Spider-hosted model.

- For on-site implementations (not hosted by Spider Strategies), Spider supports those same authentication mechanisms and additionally supports Windows Domain authentication and HTTP Header variable based Single Sign-On (IBM, CA Single Sign-on).

Backing Up Your Hosted Data

Safeguarding your data for restoration if needed

The following outlines **Spider's Backup and Disaster Recovery Strategy**:

- We take nightly backups of all customer databases and application configurations. The nightly backups are stored for three months. A weekly copy is stored as long as a customer continues their service with Spider Strategies. Additionally, backups are taken prior to any software upgrades, software patch applications, or server migrations.

- Should a disaster occur – i.e., a server completely fails – Spider will promptly generate a replacement instance on a new server. Spider will then quickly apply the server image containing the necessary software (i.e. Java, Apache Tomcat, and MySQL), redeploy the correct Spider software version, and then restore the customer database(s) and configurations from the previous night's backup.

- Affected customers will be provided with email status updates throughout this process.

- We have been hosting our systems since 2008 and during that time have never had to execute such a disaster recovery. However, on occasion we have had customers request our assistance to roll back their database to an earlier nightly backup to restore their database to a previous state. (i.e. undo an Administrator's massive content deletion transaction, etc.)

- Upon formal cancellation of service by an authorized representative of your organization, all access to your hosted environment is removed and all of your data is deleted – including back-ups.

Data Encryption and Auditing

Data Encryption Details

With Spider, your hosted solution data is stored in a MySQL database (or a MS SQL Server database if you host the software within your own environment). The database itself is not stored in an encrypted state (*except on AWS-hosted systems) but the application transmits the data to the end user(s) encrypted as HTTPS/SSL.

Auditing/Logging

Our software uses a dedicated database table for auditing user logins and login attempts. This records the username, time of login, and source host/IP address.

The software uses a dedicated database table for auditing the creation / editing / deletion of most content in the system – while also recording the timestamp and user name of the person performing the activity. Some of this audit history can be viewed in context-specific locations within the software using a "View History" button.

The software does not audit what people VIEW.

Administrator-level users have SQL Console access to query the above-mentioned audit history tables and also have the ability to create Reports that query such information. Spider Strategies can provide examples of such SQL queries upon request. These reports can be exported to MS Excel, MS Word, PDF, etc.

AI Assistant Using Amazon (AWS) Bedrock

Impact Intelligence maintains complete data security through an innovative architecture designed to protect your sensitive information while delivering powerful AI capabilities.

How Your Data Stays Secure

Your actual data values never leave your secure environment. Impact Intelligence uses a metadata-only approach where Impact Assistant receives only:

- Dataset names and their descriptions
- Field names and field types
- Aggregate statistics about fields (not associated with any individual record):
    - For date fields: The earliest and latest dates
    - For text fields: The 10 most common values

This metadata enables Impact Assistant to understand what questions it can answer and provide meaningful filtering and queries, while ensuring sensitive data remains completely protected.

Example of Privacy Protection

Consider a dataset called "Customer Orders" with thousands of records. If the dataset contains a "Product Type" field where "laptops," "tablets," and "phones" each appear in at least 1% of records, Impact Intelligence will know these are common product types to support queries like "show me laptop sales last quarter."

However, if the same dataset contains a "Shipping Address" field, individual addresses almost certainly won't represent 1% or more of records, so specific addresses are never sent to the AI. This protects personally identifiable information while still enabling powerful data analysis.

Commercial Cloud Security

For commercially hosted customers, we use Amazon Web Services with enterprise-grade security to process metadata. The AI services have contractual agreements that **your data will never be used for AI training**. This guarantee applies to both the metadata we send and ensures your organization's information remains completely private.

Key Security Benefits

- **No data values leave your environment** - All actual data processing happens securely on your server
- **AI cannot hallucinate data** - Since all values come directly from your database, Impact Assistant can only show real information
- **No AI training on your data** - Contractual agreements prevent any use of your information for model training
- **High performance** - Minimal data transfer means fast, responsive interactions

Technical Support Services

Customers with a current and paid subscription to Spider's hosted solution of Spider Impact®, have access to Spider's Technical Support team throughout their hosting period.

Technical Support means the e-mail, online HelpDesk portal, and telephone technical services that Spider offers regarding the use and function of the hosted software solutions. Spider will provide support and respond to Service Issues as further described below.

Spider's Hosted Support Services include coverage of:

- Application of software upgrades and patch fixes
- Backup and Recovery of your hosted software instance/environment
- Responses to "How Do I" questions about the hosted software solution
- Service Issue resolution as further defined below

A "Service Issue" is a customer inquiry regarding the functionality or use of the hosted software solution. Spider's support obligations concerning the hosted software solutions' use with third party products, including compilers, operating systems, web browsers, data sources and other Licensed Product(s), is limited to those items set forth in the documentation for the software.

Service Issues are assigned a classification at the time of a customer's initial contact with Spider, and are classified according to the severity levels set forth below. Spider will initially respond in accordance with the response times applicable to Service Issues

reported by e-mail, support portal or telephone during Spider's regular service hours as shown below. Spider's ability to provide technical support will depend, in some cases, on the ability of a customer's representatives to provide accurate and detailed information and to aid Spider in handling a Service Issue.

Spider will provide support for each Major Release for at least eighteen (18) months after the subsequent release is first made commercially available. After such period, Spider will provide support, as needed, to customers to update their use of the hosted software solution to the latest release of the software.

Spider Service Issue Classifications for Technical Support Escalations

Service Issue Classification	Spider Support Team Response Time	Next Steps
Severity 1—Critical Business Impact: Hosted software is not functioning or is stopped or severely impacted so that Customer cannot reasonably continue use of the hosted software and no Workaround is available.	One business day	Once the Service Issue is verified, Spider will engage development staff to provide a work around or circumvention to the Error within 5 business days if possible and will provide a best effort resolution to such Severity 1 Error within 10 business days of reporting.
Severity 2—Major Business Impact: Hosted software issue that renders certain significant and fundamental features or portions of the program unusable and no immediate Workaround is available.	One business day	Once the Service Issue is verified, Spider will engage development staff to provide a work around or circumvention to the Error within 5 business days if possible and will provide a best effort resolution to such Severity 2 Error within 15 business days of reporting.

Severity 3—Minor Business Impact: Hosted software is functioning inconsistently or in a way causing slightly impaired Customer usage and productivity, but Customer can work around such inconsistency or impairment.	Two business days	Once the Service Issue is verified, if appropriate and achievable in Spider's sole discretion, Spider will provide a resolution to such Severity 3 Error within 30 business days of reporting.
Severity 4—No Business Impact: Hosted software is functioning consistently, but Customer requests minor changes in software solution such as Documentation updates, cosmetic defects or enhancements.	Three business days	Once contact has been made with Customer, Spider, at its sole discretion, will consider Software enhancements for inclusion in a subsequent Release.
No Software Error Reported – Customer has questions on proper use of hosted software functionality	Two business days	Spider support team members will reply to customer inquiry as soon as possible.

Spider Technical Support Hours of Service & Contact Information

For Customers Worldwide:

Contact us by:	At	During
Email – Note: Best response times are via emailed requests	helpdesk@spiderstrategies.com	Monday- Friday 8:00am to 5:00pm Eastern
Phone – Scheduled Appointments	Email us to schedule a phone or web-based meeting appointment or leave voicemail at 703-345-0614	Monday- Friday 8:00am to 5:00pm Eastern; voicemails will be returned within 16 business hours

** All contact information is subject to change upon notice from Spider.