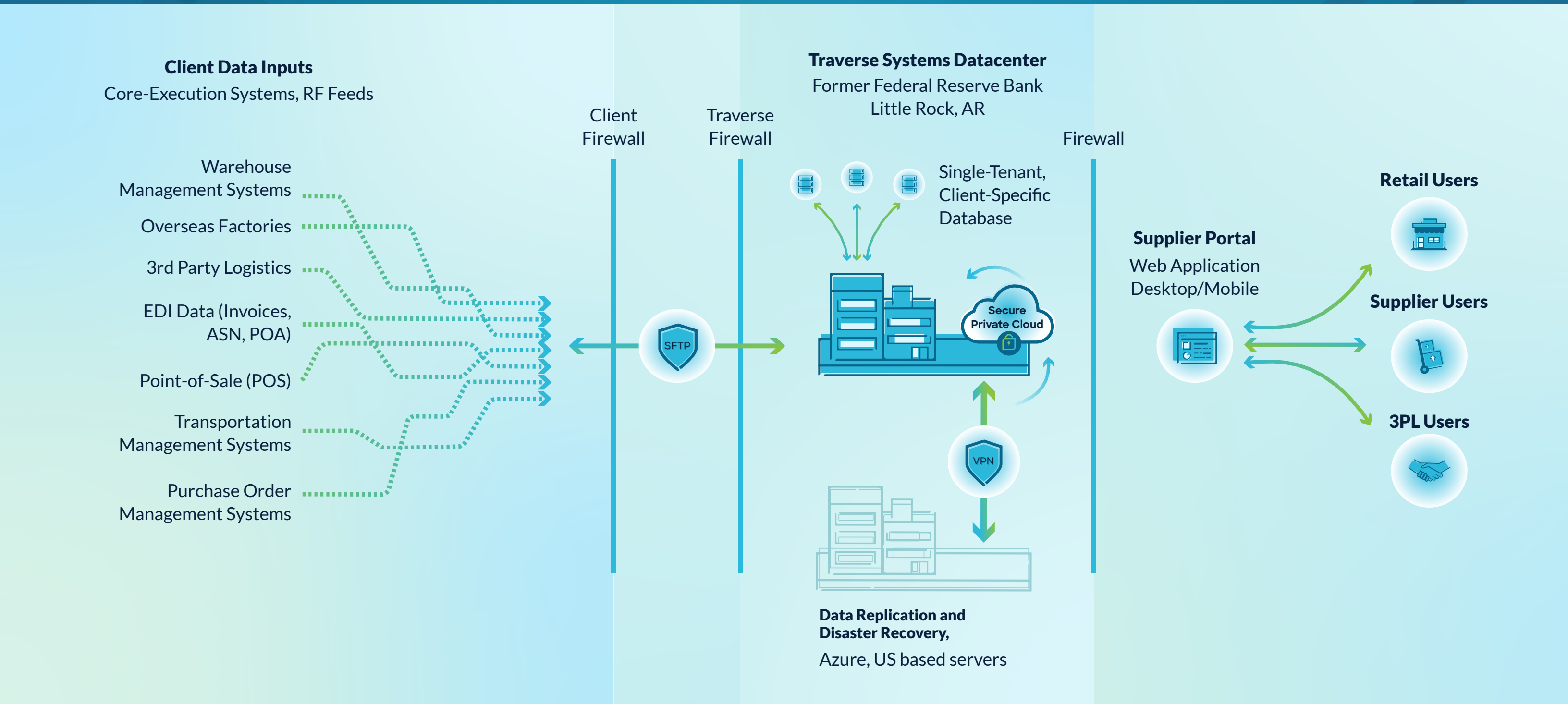
Traverse Systems Security FAQ

traverse
SYSTEMS


Client Data Inputs
Core-Execution Systems, RF Feeds
Warehouse Management Systems
Overseas Factories
3rd Party Logistics
EDI Data (Invoices, ASN, POA)
Point-of-Sale (POS)
Transportation Management Systems
Purchase Order Management Systems
Client Firewall
Traverse Firewall
SFTP
Traverse Systems Datacenter
Former Federal Reserve Bank
Little Rock, AR
Single-Tenant, Client-Specific Database
Secure Private Cloud
VPN
Data Replication and Disaster Recovery,
Azure, US based servers
Firewall
Supplier Portal
Web Application
Desktop/Mobile
Retail Users
Supplier Users
3PL Users

Principal Service Commitment and System Requirements.

Traverse Systems designs its processes and procedures related to Traverse Platform to meet the objectives set forth in its information technology (IT) policy and procedures. Commitments are based on the service level agreements that Traverse Systems makes with its customers. Security commitments are documented and communicated through customer agreements. The commitments include but are not limited to:

- Use of encryption technologies for data communications into and out of the Traverse Platform.
- Monthly vulnerability scanning and remediation of high and critical risk vulnerabilities.
- Security information and event management (SIEM) monitoring and alerting

Does the Traverse platform require access to our network?

- Never. Our clients access their encrypted version of the Traverse Platform through Microsoft Remote Desktop Gateway (RDG) service utilizing TLS encryption.
- The use of the remote desktop access prevents Traverse Systems' servers from having access to the customer networks and restricts the access of customer machines to Traverse Systems' network.

Why does Traverse Systems secure my data on a single-tenant database rather than a multi-tenant database?

We insist on the use of single-tenant, client-specific databases as we believe this offers our clients the highest level of security.

Is my data stored on the same servers as other Traverse clients?

While our clients do share the same servers, the data is logically separated into single — not multi-tenant — databases to provide an extra layer of security.

Where is my data stored?

Your data is stored at a third party facility, Mainstream Technologies, Inc. located in Little Rock, Arkansas. The site is a former Federal Reserve Bank backup facility hardened both internally and externally. The servers are housed in MTI's secure data center and monitored by MTI's network operations center (NOC) with the following measures in place:

Infrastructure

- Generator backup for power outages
- Redundant internet connectivity
- Fire suppression
- Redundant data center air conditioners and other back-up equipment designed to keep servers and data continually up and running to the best of our abilities.

On-site security

- 24/7 security
- Mandatory escorts, fencing, intrusion detection, etc.
- Key card and biometric scan required for access

Network monitoring at data storage facility

Does Traverse backup my data in case of an emergency? How secure is the backup of my data? How often is my data backed up?

- Local backups of customer data are within the confines of our hosting facility in Little Rock, Arkansas with backups every 15 minutes to Microsoft Azure for disaster recovery purposes.
- We restrict the back up of our clients data to United States data centers only.

Is Traverse Systems audited by a third party?

- Traverse Systems undergoes a rigorous SOC 2 Type II Audit every year to ensure the strictest safeguards of our clients' data. The SOC 2 Audit is based on a Trust Service Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.
- A copy of our SOC 2 Type II Audit is available to our clients upon request.

Does Traverse Systems have security policies and procedures in place?

Traverse Systems maintains an Information Security Policy and Procedures Manual that identifies and addresses the following topics:

- Information security communication and responsibility
- Acceptable use
- Logical security
- Service, protocol, and port documentation
- Network change and configuration testing/ approval
- Network perimeter control review
- Antivirus software
- Security patch management installation
- Programming change control
- Adherence to Open Web Application Security Project (OWASP) programming standards
- Transport Layer Security (TLS) Encryption

Does Traverse Systems have a Risk Assessment Process?

Traverse Systems periodically conducts risk assessments of the Traverse Platform and Traverse Systems. The risk assessment process is designed to identify and assess the severity of risks to current and future operations while focusing primarily on ensuring business availability and continuity for Traverse Systems and its customers. Examples of the risk assessment process include:

- Continually analyzing potential events that may negatively impact our environment, customers, company and employees
- Making judgements on the tolerability of the risk on the basis of a risk analysis while considering influencing factors
- Determine if existing control and security measures are adequate or if more should be done
- Bi-weekly vulnerability scans with automated reporting to assess threats
- Annual penetration tests to ensure proper safeguards are in place

Is Traverse PCI compliant?

The Traverse Platform does not accept Payment Card Industry (PCI) data and therefore is not subject to the industry standards.

Please Note: *The FAQs apply to the Traverse Systems' platform exclusively and do not apply to other products from Traverse Systems.*