

Data Security

with Kinaxis RapidResponse

Whenever or wherever you access your supply chain data, we ensure it's safe, secure and ready when you are.

The old adage is true. Your supply chain is only as strong as its weakest link. The same holds true for your supply chain data. That's why Kinaxis® prides itself on using the most advanced internet security technology available to keep your supply chain data safe and secure. Kinaxis RapidResponse®, our cloud-based supply chain planning platform, comes with the peace of mind of knowing we take your data security concerns seriously.

Security and compliance

We work around the clock to keep your data safe with routine performance and security monitoring coupled with 24/7/365 customer support and emergency response. From physical security measures to in-depth application security controls and vulnerability scans, we take every precaution to safeguard your supply chain so you can rest assured, your data is in good hands.

System architecture and availability

Get global access to your supply chain data, anytime, anywhere, with RapidResponse's secure data architecture. Easily connect from a web browser and enjoy continuous access to your most valuable supply chain data across the globe. Our Internet Service Providers and Content Delivery Network solutions have been specifically selected to ensure high operational uptime and low latency connectivity, giving you maximum performance.

User access management

We make sure your data is only visible to those you want to see it. With secure logins using HTTPS/TLS encryption and customer-defined user permission levels, you choose who can see and interact with specific information and application functionality, extending from suppliers to customers. SAML/Single Sign On support eliminates the need for multiple logins, and you can configure your own password management policies to align with corporate guidelines, including password expiry, complexity requirements and user lockouts.

Key benefits

- Access your data anywhere, anytime
- Role-based user access and permissions
- Global Optimized Network
- Web Acceleration industry-leading solutions enabling high performance
- Low latency connectivity
- 24/7 customer service and emergency response

Key security features

- SOC1 Type II audited
- SOC2 Type II audited
- BSI C5:2020 Type II audited
- Single tenant SaaS model
- 100% AES256 bit "in-transit" and "at-rest" encryption
- Disaster RTO & RPO of no more than 24 hours
- Advanced SOC monitoring 24x7x365
- Industry-best practices for data privacy and physical security

Security and data privacy standards

We adhere to strict industry standards for data privacy and security to ensure our service is constantly in line with applicable data privacy laws and regulations, such as the General Data Protection Regulation (GDPR). Alongside ensuring annual SOC1, SOC2 and BSI C5:2020 audits of our service, we routinely conduct internal and external assessments—following documented enterprise-wide processes which include management oversight to ensure the confidentiality, integrity and availability (CIA) of your data.

- Encryption keys in FIPS-compliant store
- Security Information and Event Management (SIEM) tools
- Certificates for secure data transfers (SFTP)
- OWASP standards for third-party penetration tests

Data center security

Kinaxis relies only on enterprise-grade data center facilities to co-locate its systems. Each data center facility implements best-in-class physical security, including:

- 24x7x365 security personnel
- Multiple security authentication layer
- Keyless, biometric security systems for employees
- Multifactor authentication mechanism
- Complete N+1 infrastructure with network and firewall redundancies
- All ingress and egress point monitored by camera
- Secure visitor access registration process
- Secure logging of activities and CCTV video with integrated alarms
- Restricted access to authorized personnel only
- Certified facilities ISO 27001, SOC1 & SOC2 Type II, PCI-DSS

Security, availability and performance monitoring

To ensure your data always remains safe, we've implemented a comprehensive network security monitoring system with fully automated intrusion prevention systems, and we perform both scheduled and ad hoc security scans using advanced security tools. Our incident management processes include both automated and manual security monitoring, as well as a path for escalations of verified security risks, as defined in our incident handling procedures. You'll be able to quickly determine any localized or general service outages. Take advantage of our Customer Log Collector to review the real-time availability and performance of your RapidResponse service anytime.

Secure administrative access

All remote administrative access by Kinaxis Customer Support agents, who are never third-party contractors, is controlled by Virtual Private Network (VPN) with multi-factor authentication (MFA) and firewall access control, wherein all data transmissions are encrypted.

Need more information?

For more detailed security information, talk to your account executive or email us at info@kinaxis.com.

