joinder

DATA INTEGRITY POLICIES



Data security is Joinder's highest priority. We strive to assure that data is protected from unauthorized access and that it is available when needed. These are the policies we use to protect your data.

Joinder Production Systems & Services

- Production Systems that create, receive, transmit, or store the customer's data are hosted on Amazon Web Services (AWS).
- Joinder follows the AWS "Well-Architected Framework" in implementing and reviewing "Best Practices" for building secure, high-performing, resilient, and efficient infrastructure for their applications.
- Customers may choose to have their data and backups physically stored in the United States or within the European Union to meet regional compliance and data residency requirements.
- The General Data Protection Regulation (GDPR) is supported.
- Joinder does not share customer data with any third party.
- All Production Systems are only to be used for Joinder business needs.

Infrastructure Protection

- All Production Systems disable or remove non-essential user accounts, applications and services that are not required to achieve the business purpose or function of the system.
- Production web servers are protected by network firewall controls, which restrict access to network protocols required to achieve business needs. This is analogous to placing an on-premise web server on a DMZ behind a firewall.
- Production web servers are protected by a web application firewall (WAF) to scan for malicious content and protect against common web exploits.
- Production web servers validate data requests and access the database servers via a private secure API. Unfiltered data or commands are never sent directly to the Production database servers.
- Production database servers are protected by network firewall controls, which only allow database traffic between the web services and database servers.
- Production database servers are isolated on a Virtual Private Cloud (VPC) and located on a protected network segment, separate from the web and other internet-accessible servers. This is analogous to placing an on-premise database server on an internal network behind a firewall.

Data Protection



- Production Systems enforce Identity Controls, requiring strong passwords, Multi-factor Authentication (MFA) and/or Single Sign-on (SSO).
- Customer configurable access controls enforce user permissions and restrictions over reading or modifying customer data on a per document basis.
- All Production Data is segmented and only accessible to authenticated users who are authorized to access the data.
- All Production Data is stored encrypted at rest.
- All Production Data is encrypted in transit. Customers may access the Production web servers via HTTPS.
- All Production Data is periodically and cryptographically archived on a separate Production Database instance.
- Customers may securely download a copy of their data store and documents via a RESTful API call.
- Databases use Row Level Security (RLS) policies to allow ACL enforcement at the lowest level.

Detective Controls



- All access to Production Systems must be logged. This includes network connections as well as attempted logins.
- All access to Production Data must be logged. This includes the creation, modification, reading, importing, or exporting of documents.
- All Production Systems are monitored using IDS technology and scanned for malware. Suspicious activity is logged and alerts are generated. Detected malware is evaluated and removed.

Operations and Maintenance



- Joinder access to Production Systems is controlled using centralized tools and authentication. Access is limited to Production System administrators in the Joinder Operations Group and logged for auditing.
- Up to date system lists and architectural diagrams are kept for all Production environments.
- Amazon Inspector is used to perform configuration assessments for known bugs or vulnerabilities
- Production System administrators leverage and actively monitor external threat feeds and vulnerability resources (e.g. US-CERT, CVE, OWASP, etc.) to help secure Production Systems.
- Patches, applications, and system OS versions are kept up to date at all times. New versions are tested before deployment and software rollback is supported.
- Vulnerability scanning of Production Systems must occur on a predetermined and regular basis. Scans are reviewed, with defined steps for risk mitigation.
- External third-party Penetration Tests occur on a regular basis, no less than annually.
- Disaster Recovery and Availability policy requires storing encrypted backups off site and in a different region.

joinder

Security FAQ

Regulatory Compliance and Independent Validation

Do you conduct independent audits for reviewing the efficiency and effectiveness of implemented security controls to ensure compliance obligations?

Yes. Joinder maintains a full-time compliance program to meet its SLA and regulatory requirements.

Joinder complies with the AICPA SOC 2 Trust Services Criteria for Security, Availability and Confidentiality. An independent CPA firm conducts audits annually. Joinder was first audited for SOC 2 in February 2021.

Do you have the capability to continuously monitor and report on the compliance of your infrastructure against your information security baselines?

Yes. Joinder performs internal audits and continuous monitoring throughout the year to maintain compliance.

Do you make third-party audit or certification reports available?

Yes. Our SOC 2 report is available to customers by request via the Joinder service portal.

Do you conduct penetration tests of your cloud infrastructure?

Yes. We partner with an independent third-party to conduct both network and application penetration tests of the Joinder cloud service infrastructure at least annually.

Do you conduct any third-party reviews of your platform or services?

Yes. Joinder partners with Amazon Web Services, to provide a reliable and secure service. This includes periodically performing an AWS Well-Architected Framework review to ensure we are following best practices and leveraging the infrastructure's security offerings to their fullest.

Risk Management

Does Joinder maintain a Risk Management program?

Yes. Risk assessments of Joinder and its service providers are performed to identify and categorize risks, understand their cause and potential impact, and outline mitigation steps that reduce their impact or severity.

How frequently does Joinder conduct risk assessment?

Assessments are conducted annually, as well as before any major change to the service, and are reviewed by senior management to ensure risks are both understood and accepted.

Personnel & Operations

Are Joinder employees subject to background checks?

Yes. Joinder employees undergo reference and background checks before being granted access to any customer information or the Production Environment.

Are Joinder employees subject to employment agreements and mandatory training?

Yes. All employees are subject to a perpetual Non-Disclosure Agreement to ensure confidentiality.

Joinder employees receive mandatory information security and privacy training upon hire and at least once per year thereafter. The content includes (but is not limited to) company and policy requirements, security risks, and user responsibilities.

Availability & Infrastructure

Where is the Joinder service hosted?

Production systems for processing and storing customer data are hosted on Amazon Web Services (AWS).

Primary and backup data centers are located within the United States and European Union regions to meet regional compliance and data residency requirements.

Can I specify what data center to use?

Data Sovereignty is a customer choice. You decide where to have your data physically stored and it will never be moved without your prior consent.

Does your organization have a plan or framework for business continuity management or disaster recovery management?

Yes. Joinder maintains a framework for business continuity. This includes plans for both Disaster Recovery and Incident Management.

How does Joinder manage backups?

Joinder performs geo-redundant encrypted backups on a daily basis. Backup verification and restoration are included in the automated process.

Customer data backups are securely maintained for thirty days.

Does Joinder support a High Availability solution?

If you require a highly available data center, please contact Joinder regarding Amazon availability zones.

What is Joinder's commitment to service uptime?

Joinder maintains a 99.9% target for uptime and service availability. Our SLA commitments including RTO and RPO may be accessed via the customer portal.

Incident Management

How do I contact Joinder regard a security related issue?

If you believe you have detected a security event or potential vulnerability, please let us know by emailing us at security@joinderapp.com.

Does Joinder maintain an Incident Response Team?

Yes. Joinder maintains a team to monitor for security and availability issues and, if needed, implement our incident response plan.

What is Joinder's policy regarding breach notification?

Joinder complies with the General Data Protection Regulation (GDPR).

Data Protection

Does Joinder ever share my data?

No. Joinder does not share customer data with any third party.

Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?

Yes. Replication or use of production data in a non-production environment is strictly prohibited. Access to Production Systems is restricted to the Joinder Operations team and the principles of least privilege and need to know are implemented and regularly reviewed.

Do you have procedures and technical measures in place for data access segmentation in multi-tenant system architectures?

Yes. All production data is segmented and only accessible to authenticated users who are authorized to access the data.

Do you encrypt my data at rest (on disk/storage) within your environment?

Yes. We leverage AWS KMS and encrypt production data at rest using AES-256, including files, databases and backups.

Do you encrypt my data in transit?

Yes. Data is encrypted in transit over HTTPS using TLS 1.2 or greater.

Identity and Access Management

Do I have granular control over who may access my data?

Yes. As an organization, you have control over whom you invite to access your data and to what degree. Production databases use Row Level Security (RLS) to allow you to specify and enforce granular per-object access controls within the Joinder service.

How does Joinder enforce identity controls within the service?

By default, production systems require strong/complex passwords and Multi-factor Authentication (MFA).

Can I use my own Identity Provider?

Yes. Joinder supports integration with a customer specified IdP.

Platform and Network Security

Does Joinder support a Three Tier Architecture?

Yes. Production database servers are protected and isolated on a Virtual Private Cloud, separate from the web and Internet accessible servers.

Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?

Production systems are protected by network firewall controls to restrict access as well as Web Application Firewall (WAF) controls to protect against common web exploits.

Are production servers hardened to provide only necessary ports, protocols, and services to meet business needs?

Yes. Production servers are built from a standard template as a baseline, with non-essential accounts and applications removed or disabled

Are production servers scanned for vulnerabilities?

Yes. Vulnerability scanning of production systems occurs daily. Security patches for the applications and system OS versions are included in our baseline image build framework and are kept up-to-date at all times.

Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?

Yes. Servers are deployed from a master image, which includes file integrity monitoring and whitelisting controls.

What security tools are implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents?

Anti-malware and Intrusion Detection technologies are applied both on the network and production servers.

Production systems are monitored in real-time and generate alerts for both security and availability related events.

Are audit logs centrally stored and retained?

Yes. Internal audit logs are centrally stored and retained for 12 months for forensic purposes.

Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, etc.)?

Yes. Access to Production Systems and infrastructure is restricted to the Joinder Operations team and is audited. The principles of least privilege and need to know are implemented and regularly reviewed.

Secure Development

Are Joinder services built and deployed in accordance with leading industry standards?

Yes. Joinder is committed to following a Secure SDLC to develop, implement, and comply with industry-standard secure coding best practices.

All changes to the Joinder service, included but not limited to software updates, network or system configuration changes, and security controls go through a formal change control procedure. Process phases include design, development, functional, integration and regression testing as well as risk assessment. Prior to release to production the source code and application services are scanned and tested for vulnerabilities.

We follow OWASP security by design principles and all changes to the service require peer review and approval by senior management before being released to production.

Zero-downtime deployments allow us to make changes without waiting for a change window and allow us to return the application to a previous state easily.

Are production services isolated from the development process?

Yes. Test and staging environments are separate from the production environment. Customer data is never used or stored in non-production environments or as test data.

Other questions?

Choose a time for a briefing with our security team