WHITEPAPER

Conga Advantage Platform security and data protection

Table of contents

Introduction

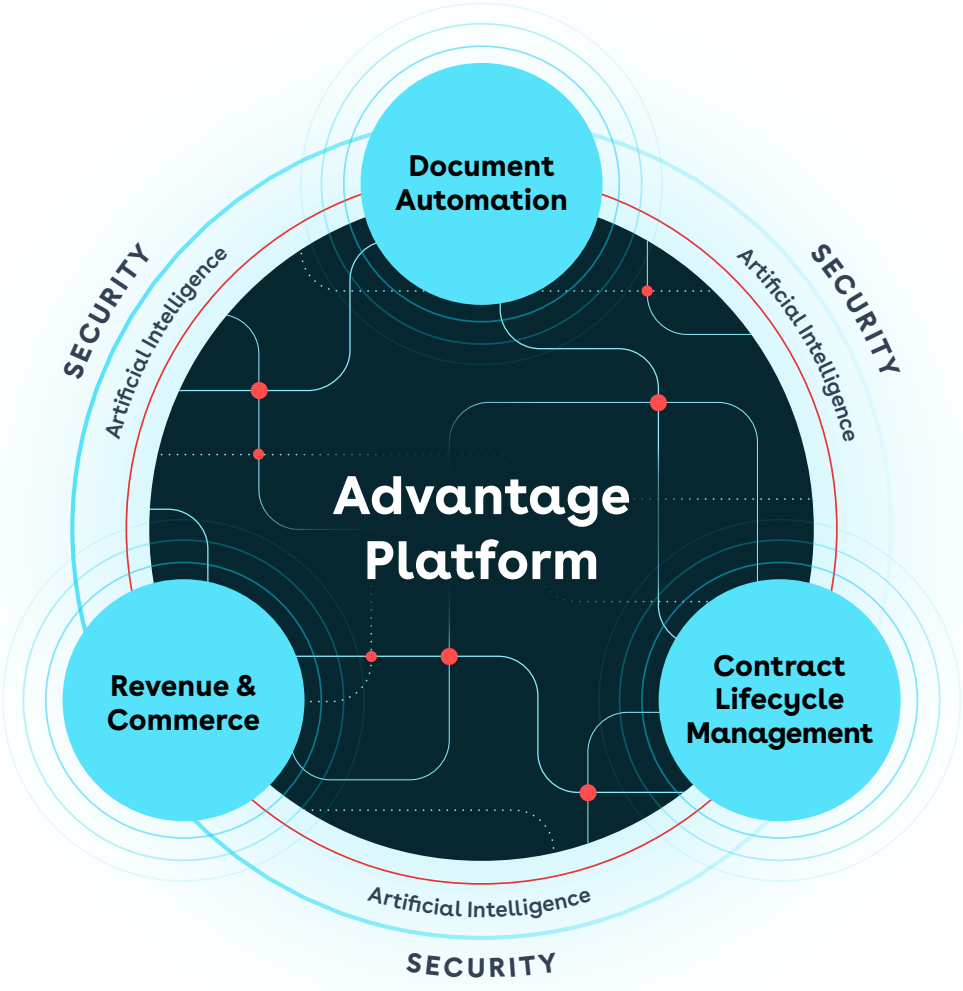
Conga Advantage Platform is the first open platform designed to run on any cloud infrastructure. It integrates Conga Configure, Price, Quote (CPQ), Conga Contract Lifecycle Management (CLM), Fulfillment, Billing, Renewal, and Document Automation (Conga Composer and Conga Sign) on one platform.

This comprehensive suite simplifies complex processes and ensures consistency to accelerate the journey to becoming a more connected and intelligent business. Conga seamlessly manages these processes to enhance customer lifetime value, from proposals and quotes to contract finalization, billing, invoicing, fulfillment, and renewal.

Conga keeps pricing, contracts, data, and templates secure, updated, and accessible across various systems. It offers complete solutions for proposal generation, negotiation, execution, management, fulfillment, and renewal, boosting efficiency and predictability by addressing your organization's specific challenges.

Flexible, scalable, and high-performing, Conga's API-first approach enables seamless integration with any business software.

Conga services are designed to leverage the benefits of cloud architecture, including the capability to scale computing, memory, and network resources to meet our customers' demands. Conga uses auto-scaling features offered by cloud providers to maintain application availability and scale our capacity up or down automatically, according to demand.



1 Secure software development

Conga has three major product releases per year: spring, summer, and winter. Each release goes through rigorous testing and benchmarking. Additionally, Conga deploys minor releases and bug fixes on a weekly basis. For more information on our releases, visit: https://community.conga.com/s/release-resources.

1.1 Development framework

Conga Revenue Lifecycle Management is a multi-tenant cloud platform that supports the complexities of Revenue Lifecycle Management, leading to improved efficiency and certainty for businesses to drive configure, price, quote, contract, negotiate, manage, collect, and renew revenue. It helps unify and automate all revenue-generating processes to help customers increase lifetime value.

1.2 Quality assurance

As part of Conga's SDLC, all code undergoes both manual and automated security testing before production release. Conga has security built into the CI/CD pipeline, including peer-reviewed manual code reviews, Static and Dynamic Application Security Testing (SAST and DAST), Software Composition Analysis (SCA), and unit, integration, and functional testing to ensure quality and security.

1.3 Third-party testing

On an annual basis, Conga contracts with a qualified third-party firm to conduct periodic penetration testing. The third-party firms are rotated on a regular basis to ensure Conga gets different approaches and perspectives when completing penetration testing. Testing may include access to our source code to enable targeted and informed testing, infrastructure review, and external network testing. Executive summaries of penetration test findings and remediation status are available in the Compliance portal of the Conga Customer Community.

1.4 API security

A WAF and API gateway inspect and block malicious traffic to the APIs. All APIs use OAuth 2.0 for authentication. Monthly DAST scans test the security of the APIs. Secrets are scanned on pull requests to prevent secrets in code.

1.5 Data privacy by design

As part of each major product release, the Conga product and release management teams review the data privacy impact assessment for each product to determine updates to key data considerations, such as data elements processed, volume of data processed, storage of data, etc.

1.6 Data residency options

Conga customers can choose where to store and process their data. We leverage AWS data centers in the United States, Europe, and Australia.

1.7 Ethical AI

At Conga, we are committed to developing and deploying solutions that leverage the power of artificial intelligence (AI) responsibly and ethically. Conga AI can be a powerful tool for enhancing customer experiences, but ensuring its use aligns with ethical principles and respects user privacy is crucial. We will achieve this through the following actions:

- Regularly audit our AI models and datasets to identify and address potential biases
- Implement robust security measures to protect user data and prevent unauthorized access
- Implement internal training on the ethical implications of AI and best practices for responsible development and deployment
- Be transparent about how we use AI in our solutions and explain AI-driven recommendations clearly
- Continuously improve our AI practices by staying informed of the latest research and developments in ethical AI.

Visit https://conga.com/ethical-ai-statement for more information.

2 Customer data protection

2.1 Access controls

Conga protects its customers' data through a combination of access controls deployed at Conga and controls that customers can configure when using Conga's products.

Access to Conga infrastructure supporting customers is restricted to appropriate personnel at Conga. Access is role-based and only the least privileges are assigned to the personnel to complete job duties. Conga users must satisfy strong authentication methods to access infrastructure, including passwordless and multifactor authentication (MFA).

Conga builds strong access controls into its products and encourages its customers to deploy these controls to protect themselves when using Conga's products. Specifically, Conga's products support MFA and Single Sign-On (SSO). Customers can also develop custom roles with varying functional and data access within Conga's products to achieve role-based access that aligns with customer policies. These configurations and controls are managed by designated administrators in the customer environment.

2.2 Data protection

Conga prioritizes protecting customer data as the highest priority. Data at rest is encrypted with AES-256, and data in transit is encrypted via TLS 1.3. Data is saved in encrypted (AES-256) S3 storage buckets and each customer is provided with a unique storage bucket. Customer data is never co-mingled.

Code execution occurs in a private subnet, and we use an in-memory cache to improve the data merge process. This cache is encrypted, and the data held inside is transient and not saved or serialized to disk during processing.

Additionally, only select Conga Cloud Operations team members who pass background checks and complete privacy and security training can access environments for maintenance. Conga's access controls also ensure that authorized personnel are granted the least privileged access. We recertify access quarterly.

2.3 Network protection

Conga utilizes web application firewalls (WAFs) as one component of a layered approach to application infrastructure security. WAFs control access and allow only authorized traffic to Conga infrastructure. Additionally, traffic is restricted between resources, and public access is managed via Network Security Groups and Access Control Lists. Security groups are configured to use only the required ports and are opened based on business requirements.

In addition, Conga employs security policies to manage the ingress and egress of data based on protocol, port, source, and destination within the environment. Conga applications or APIs accessible through WAF are configured with various rules to protect the ports and traffic flow to the Elastic Load Balancer (ELB). The ELB passes the traffic to the respected resource, typically a microservice deployed in a VM, and can expand horizontally. Any traffic not adhering to these strict access controls is discarded at the internet boundary. Internally, host-based intrusion detection and monitoring systems are deployed at the server and network layers. Events in these systems are captured in logs, which are fed into a Security Information and Event Management (SIEM) system, which has 24/7 human and AI monitoring for aberrant behavior.

3 Conga corporate security

3.1 Access controls

Access to Conga systems is restricted through passwordless authentication. This form of authentication offers several key security advantages for organizations, including support for Zero Trust Security and enhanced security, which eliminates passwords to reduce the risk of common attacks such as phishing, credential stuffing, and brute force attacks. At Conga, passwordless authentication is combined with MFA methods like biometrics or hardware tokens, which are much harder for attackers to compromise.

Within Conga's systems, users are assigned role-based access that adheres to least privilege principles. User access is reviewed quarterly, and inappropriate access is removed as part of the review process.

3.2 Endpoint security

Conga protects all end-user endpoints from viruses and malware with an industry-recognized endpoint protection product. Additionally, Conga employs standardized system hardening practices across devices, including restricting protocol access, removing or turning off unnecessary software and services, removing unnecessary user accounts, changing default passwords, patch management, and logging. All devices utilize full disk encryption.

3.3 Third-party risk management

Conga engages with third-party vendors to support its objectives. Before commencing a business relationship with a vendor, Conga performs regular vendor security reviews to ensure the vendor has a strong security posture and appropriate data protection measures. Conga does not engage with vendors that do not meet its security and data protection standards.

3.4 Security benchmarks

Conga measures, monitors, and benchmarks its outward-facing perimeter for weaknesses using a third-party solution called SecurityScorecard. As seen in our Conga Community, where we publish our current standing and performance, Conga has regularly maintained an "A" rating.

For our internal systems, Conga uses the Microsoft SecureScore scoring system. Under this system, Conga regularly scores above 90% while Conga's competitors average a score in the 40-50% range.

4 Vulnerability and patch management

Conga patches all systems, network devices, and applications following our Vulnerability Management Policies and Procedures, which define patching requirements based on industry best practices.

Conga uses industry-standard tools to perform real-time vulnerability scans. Conga assesses the risk level in addition to the classification (Critical, High, Medium) for any identified vulnerabilities and prioritizes remediation for critical software issues. Conga has SLAs with various issue types, classifications, and targets for vulnerabilities.

Conga measures the emergency patch development and release process in days while measuring critical infrastructure patch implementation in hours. We use an automated patch deployment system, which allows for efficiencies during the patch deployment process.

4.1 Bug bounty

Conga has developed and currently manages a bug bounty program for our applications, infrastructure, and external facing websites. This process is an extension of Conga's vulnerability management process, as it allows external testers to find and report issues in Conga's production environments. Conga's security team works with the relevant team internally to triage reported findings, raise relevant tickets for remediation, and then work with the initial reporter to re-test an item to confirm successful fix/remediation in place. In the last 12 months, Conga received 31 security reports and paid a bounty on eight of them.

5 Incident response

Conga has a rigorous incident management process for security events that may affect systems or data confidentiality, integrity, or availability. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Conga will utilize personnel with forensics experience and training as part of the incident response process when applicable. To help ensure the swift resolution of security incidents, the Conga security team has 24/7 monitoring for security issues. It has communication procedures to notify Conga security personnel to respond to security incidents. If an incident involves customer data, the Conga security team will investigate the incident and work alongside the appropriate Conga teams to inform the customer.

Conga performs bi-monthly tabletop exercises to practice and obtain feedback on incident response procedures. All relevant scenarios are incorporated into tabletops to obtain a wide variety of knowledge and feedback. Functional teams across Conga are invited to familiarize themselves with the incident response process and provide input as part of the incident response tabletop when relevant.

6 Business continuity (BC) and disaster recovery (DR)

Conga maintains robust business continuity and disaster recovery (BC/DR) plans, including risk assessments, disruption strategies, and procedures to sustain critical IT operations. Its geographically distributed data centers use near-seamless failover technologies, enabling uninterrupted service even if one site is disrupted.

The company ensures data resilience through high availability, real-time replication, and disaster recovery. An active-active architecture spans multiple availability zones within each region with independent power and network connectivity, allowing automatic workload redistribution during failures. Across regions, an active-passive model replicates customer data to a standby environment in real-time, supporting a Recovery Time Objective (RTO) under 30 minutes and a near-zero Recovery Point Objective (RPO). Daily backups are retained for 30 days for added protection.

BC/DR plans are regularly tested through failovers, resilience drills, and tabletop exercises. All data centers are active and clustered by region, with automated systems rerouting traffic during failures. Cloud partners maintain disaster recovery facilities at separate geographic sites to ensure continuity if primary data centers become unavailable.

We provide transparency around service availability and performance for Conga products here: https://status.conga.com.

7 Conga trust and assurance activities

7.1 Conga compliance

Conga is committed to earning and maintaining customer trust and confidence. Its dedicated security and privacy teams play a key role in this mission by helping customers meet global compliance, data protection, and regulatory requirements.

Conga's trust and assurance activities include:

- SOC 1 Type 2 (SSAE 18) report
- SOC 2 Type 2 report
- ISO 27001:2022 certification
- HIPAA
- PCI DSS 4.0
- ISO 27701 certification: Scheduled for October 2025

Conga complies with all applicable laws and regulations, including:

- EU Standard Model Clauses (July 2021): EU Data Processing Requirements
- GDPR: Data Processing Addendum
- Data Privacy Framework Program (EU-U.S. and Swiss-U.S. Privacy Shield): https://www.dataprivacyframework.gov/list (search "Conga")

7.2 Compliance portal

Conga has a dedicated Compliance portal within its Customer Community. Conga's Security and Compliance Team regularly posts security-related alerts and updates, such as responses to zero-day vulnerabilities and results from threat hunts on the portal, so customer security teams understand Conga's actions to address these matters promptly.

Additionally, the Compliance portal is a self-service repository for customers to obtain compliance reports.

7.3 Helpful links

- Conga DPA: https://conga.com/legal-center/dpapresigned
- Conga Privacy Policy: https://conga.com/privacy
- Conga Subprocessors: https://conga.com/privacy/subprocessors
- Conga Customer Community: https://community.conga.com/s/home
  Customers without a login are welcome and encouraged to create an account.

8 Data center security

Data processing and storage occur within our cloud providers (e.g., AWS, Salesforce, Azure). Their data centers are housed in nondescript facilities.

Annually, Conga reviews the SOC reports for all cloud providers to validate the operating effectiveness of controls, including physical access controls.

8.1 Physical access

The Conga Advantage platform and products built on the Conga platform are SaaS offerings that leverage the underlying platform and infrastructure services from cloud providers (e.g., AWS, Salesforce, Azure). Conga does not own any data centers. Cloud providers are responsible for the physical security of their data centers and offer various compliance certifications to meet industry requirements. As a SaaS provider, Conga does not require or have access to the cloud provider's infrastructure. Please contact us and we can direct you to the relevant cloud provider's compliance certifications.

Physical access to the cloud provider's data centers is tightly controlled. The cloud provider's security staff monitor perimeter and entry points using video surveillance, intrusion detection systems, and other electronic methods. Authorized personnel must complete two-factor authentication to access data center floors. Visitors and contractors must present identification, sign in, and be escorted by authorized staff. Access to the cloud provider is granted only to individuals with a legitimate business need and is revoked immediately when no longer required, regardless of employment status. Cloud providers log and regularly audit all physical access by employees.

8.2 Operational support systems

Operational support systems in the cloud provider's data centers are designed to ensure resilience and reliability. These include redundant power systems with dual feeds and backup supplies to maintain continuous operation and precise climate and humidity controls to prevent overheating. Redundant cooling systems provide backup in case of failure, while automatic fire detection and suppression mechanisms enhance safety. Additionally, leakage detection systems are in place to identify and mitigate water-related risks, ensuring overall operational integrity.

Cloud providers ensure continuity of internet connectivity by utilizing multiple providers of Internet connectivity, which are frequently provided by a separate route into the building further helping avoid potential outage due to, for example, physical excavation of the road/paths outside the building or damage to overhead cables.

About Conga

The Conga Advantage Platform is chosen worldwide to accelerate the journey to become a more connected, intelligent business. Conga brings Configure, Price, Quote, Contract Lifecycle Management, and Document Automation capabilities together on a single open platform that works with any ERP, any CRM, and any Cloud. Powered by a unified data model and purpose-built AI, Conga helps companies achieve a unique advantage—one built on seamless connection, actionable intelligence, and scalable growth.

Conga delivers an advantage to over 10,000 customers and 6.4 million users around the globe. More than 6 million contracts and 21 million quotes are generated annually with Conga. Founded in 2006, the company is headquartered in Broomfield, Colorado and has global operations in North America, Europe, Asia and Australia. Visit conga.com for more information.

For more information

Email info@conga.com or visit conga.com