Clari

Clari 2023

CLARI SECURITY

CLARI AND PROSPECT CONFIDENTIAL

CONTENTS

02 TABLE OF CONTENTS

03 INTRODUCTION & CLARI ORGANIZATIONAL SECURITY

04 CLARI'S PROTECTION OF CUSTOMER DATA
- Secure software development lifecycle
- Encryption
  - Data in transit
  - Data at rest

05
- Server Hardening
- Network Security
- Endpoint Security
- External Validation

06 SECURITY AND PRIVACY COMPLIANCE & CONCLUSION

INTRODUCTION

Clari's mission is to help our customers realize their fullest potential by transforming their revenue operations to be more connected, efficient, and predictable. We believe that we need to secure your data and that protecting it is one of our most important responsibilities. We're committed to being transparent about our security practices and helping you understand our approach.

CLARI ORGANIZATIONAL SECURITY

Clari's industry-leading security program is based on the concepts of zero trust principles and defense in depth: securing your data at every layer. Our security program is aligned with ISO 27000, NIST Standards and AICPA principles. We are continuously evaluating the threat ecosystem and evolving our program with industry insights and best practices. With our commitment to transparency, you can see all of Clari's 3rd party attestations in our online portal.

CLARI’S PROTECTION OF CUSTOMER DATA

The focus of Clari’s security program is to prevent unauthorized access to customer data. Our team of dedicated security personnel, work in partnership with key stakeholders across the company, to identify and mitigate security risks as well as improve our overall security posture and controls.

SECURE SOFTWARE DEVELOPMENT LIFECYCLE

Clari’s product security team works closely with our Product Development Engineering organization and has built out a robust framework for ensuring secure development. Clari security has integrations in multiple phases of the development cycle to catch bugs and vulnerabilities throughout the pipeline. Additionally the Security team maintains production workload protection and manages multiple bug bounty programs throughout the year to allow the world’s best security researchers to facilitate responsible disclosure of potential security vulnerabilities. All identified vulnerabilities are validated for accuracy, triaged, and tracked to resolution.

ENCRYPTION

DATA IN TRANSIT

Data transmitted within the Clari web application, mobile application, and API, as well as with Clari backend services, are consistently protected by robust encryption protocols. Clari ensures the use of up-to-date, recommended secure cipher suites to encrypt all data during transit. This includes the adoption of TLS 1.2+ protocols, AES256 encryption, and SHA2 signatures whenever supported by our clients.

DATA AT REST

In Clari’s production network, data at rest is safeguarded through encryption using hardware backed key material that complies with the FIPS 140-2 standard. This encryption protocol applies to all forms of data that reside within Clari systems, including relational databases, object stores, and database backups. The management of encryption keys is governed by stringent resource-based policies. Clari has implemented comprehensive measures to ensure the secure handling of sensitive information, such as encryption keys and service account credentials, throughout their lifecycle, including creation, storage, retrieval, and destruction.

Clari’s customer’s data is hosted in our shared infrastructure and logically separated from other customers’ data. We use a combination of storage technologies to ensure customer data is protected from hardware failures and returns quickly when requested. The Clari service is hosted in public cloud and is configured for high availability, fault tolerance, and data integrity.

SERVER HARDENING

Every instance, container, and pod in our production fleet undergoes hardening procedures, including the disabling unnecessary ports and removing default passwords, to enhance security. Additionally, a standardized base configuration image is applied to maintain uniformity throughout the environment. Clari's production fleet is equipped with workload protection, audit logs, and stringent access control measures to ensure robust security measures are consistently upheld.

NETWORK SECURITY

Clari employs a network segmentation strategy to enhance the security of sensitive data. The systems that facilitate testing and development activities are segregated into a distinct network, separate from the one housing Clari's production infrastructure. Access to Clari's production environment is tightly controlled, and services and applications are governed by a zero trust model to ensure stringent security measures are in place.

ENDPOINT SECURITY

Clari ensures that all workstations assigned to its personnel adhere to our stringent security standards. These standards mandate proper configuration, regular updates, and continuous monitoring through Clari's endpoint management solutions. By default, Clari-configured workstations include features like data encryption at rest, robust password policies, and automatic locking when idle. These workstations also run up-to-date monitoring software to detect and report potential malware, unauthorized software installations, and mobile storage devices. Moreover, any mobile devices used for company-related activities must be enrolled in the designated mobile device management system to guarantee compliance with Clari's security criteria.

EXTERNAL VALIDATION

In addition to our Compliance audits, Clari also works with 3rd parties to independently perform snetwork, infrastructure and application penetration tests. The findings from these engagements are communicated to senior leadership, and accessed for severity and prioritization. Clari also maintains a Bug bounty program where independent security researchers can assess our platform and hunt for potential security weaknesses. Customers have the option to request executive summaries of these activities.

SECURITY AND PRIVACY COMPLIANCE

Clari maintains a continuous cycle of monitoring, auditing, and enhancing the design and operational efficiency of our security controls. This comprehensive approach involves routine assessments conducted by third-party accredited assessors and Clari's internal risk and compliance team. The results of these audits are transparently communicated to senior management, and any identified issues are tracked and resolved in a timely fashion. For more details, you can access our collection of certificates by following this link.

CONCLUSION

Safeguarding your data is of paramount importance to us, as it aligns with our core values and mission. We firmly believe that every individual, team, and organization deserves the assurance of data security and confidentiality. This commitment to protecting your data is a fundamental responsibility we uphold for our customers. We are unwavering in our efforts to earn and maintain your trust. If you have any questions or concerns, please don't hesitate to reach out to your dedicated account team.