Kollective

Security Overview

Kollective takes our customers security and their data privacy very seriously. The Kollective solution is Secure by Design and Secure in Operation.

The worlds largest brands trust Kollective, including industries requiring the highest security standards such as Banking, Financial Services, Insurance, Healthcare, and Defense.

Secure by Design

- The Kollective solution is Secure by Design. We have architected our solution to use common ports and protocols. The solution uses SSL for all transfers of data and control information.
- All communication is secured within the peering protocols and transfers between nodes. The protocol itself is built on top of trusted and well-defined network protocols including DTLS/SCTP for secure connections between nodes, and TLS with authenticated tokens for connections to cloud services.
- There are no known vulnerabilities within the peering protocol
- The code is scanned for vulnerabilities through a number of industry standard best practices and third-party auditing tools.
- The software loads and runs only in the browser or Teams app which means it doesn't interact with local resources.
- Because the solution runs in the users context no special whitelisting is required.

Secure in Operation

- We validate our operational security every year with the SOC2
- We run penetration testing against our environment weekly
- Kollective follows the same security mechanisms and access controls as Microsoft as part of the deep integration.
- Our cloud architecture is hardened according to industry best practices

"Microsoft Azure provides a secure foundation across physical, infrastructure, and operational security. Customers like Smithfield and Merrill Corporation choose Azure to be their trusted cloud due to its platform security. Microsoft invests over a billion dollars every year into security, including the security of the Azure platform, so that your data and business assets can be protected."

- Avi Ben-Menahem Director of Program Management, Azure Security

To learn more about Azure security, watch Microsofts Azure Essentials video on Azure Security.
https://youtube.com/watch?v=OTGMi0ksjXY

Kollective Technology, Inc. All rights reserved.

Kollective

Compliance

To help you validate our security story we offer easy access to our certifications and compliance offerings, including:

Kollective is GDPR and PII Compliant. There is no Personal Identifiable Information (PII) gathered in the course of using the ECDN.

SOC 2 defines criteria for managing customer data based on five "trust service principles"—security, availability, processing integrity, confidentiality and privacy.

ISO/IEC 27001 is the best-known standard in the family providing requirements for an information security management system (ISMS).

Transparency

- The only data sent to the cloud is session, external ID, transfers, peering, buffering, time, connects, bytes
- Data is archived after 24 months, but still accessible upon request
- Users within your organization who have permission to create live events have access to all event analytics
- All data is encrypted with SHA256 in transit and at rest
- Customer data is sharded against their own primary key which is tied to their account
- The data is located in the secured Azure instance alongside the ECDN itself

Privacy Policy

https://kollective.com/privacy-policy/

Kollective Technology, Inc. All rights reserved.

(408) 215-6400 - kollective.com