gorgias

Security at Gorgias

Security is one of the top priorities for Gorgias because it's fundamental to your experience with the product. Gorgias is committed to securing your application's data, eliminating systems vulnerability, and ensuring continuity of access. Gorgias uses a variety of industry-standard technologies and services to secure your data from unauthorized access, disclosure, use, and loss. All Gorgias employees are trained on security practices during company onboarding and on an annual basis. Security is directed by Gorgias's Chief Technology Officer.

Vulnerability Disclosure

If you would like to report a vulnerability or have any security concerns with a Gorgias product, please contact security@gorgias.com.

You can also report them on our Hackerone program. Currently the program is private, send us an email at security@gorgias.com to receive an invite.

If you want to encrypt sensitive information please read the information on this keybase account here.

Infrastructure and Network Security

Physical Access Control

Gorgias is hosted on Google Cloud Platform. Google data centers feature a layered security model, including extensive safeguards such as:

- Custom-designed electronic access cards
- Alarms
- Vehicle access barriers
- Perimeter fencing
- Metal detectors
- Biometrics

According to the Google Security Whitepaper: “The data center floor features laser beam intrusion detection. Data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are reviewed in case an incident occurs. Data centers are also routinely patrolled by professional security guards who have undergone rigorous background checks and training.”

Gorgias employees do not have physical access to Google data centers, servers, network equipment, or storage.

Network Access Control

Gorgias is the assigned administrator of its infrastructure on Google Cloud Platform, and only designated authorized Gorgias operations team members have access to configure the infrastructure on an as-needed basis behind a two-factor authenticated virtual private network. Specific private keys are required for individual servers, and keys are stored in a secure and encrypted location.

Penetration Testing

Gorgias undergoes black box penetration testing, conducted by an independent, third-party tester, on a continuous basis via our Hackerone vulnerability bounty program. We also did a penetration testing with Cure53 agency. For our enterprise level customers we're happy to provide the results of their findings and the mitigation we applied.

Third-Party Audit

Google Cloud Platform undergoes various third-party independent audits on a regular basis and can provide verification of compliance controls for its data centers, infrastructure, and operations. This includes, but is not limited, to SSAE 16-compliant SOC 2 certification and ISO 27001 certification.

As part of our ongoing commitment to providing you the highest level of security assurance, Gorgias is SOC 2 Type 2 compliant.

Intrustion Detection and Prevention

Unusual network patterns or suspicious behavior are among Gorgias' biggest concerns for infrastructure hosting and management. Google Cloud Platform's intrusion detection and prevention systems (IDS/IPS) rely on both signature-based security and algorithm-based security to identify traffic patterns that are similar to known attack methods. IDS/IPS involves tightly controlling the size and make-up of the attack surface, employing intelligent detection controls at data entry points, and developing and deploying technologies that automatically remedy dangerous situations, as well as preventing known threats from accessing the system in the first place. Gorgias does not provide direct access to security event forensics, but does provide access to the engineering and customer support teams during and after any unscheduled downtime.

Business Continuity and Disaster Recovery

High Availability

Every part of the Gorgias service uses properly-provisioned, redundant servers (e.g., multiple load balancers, web servers, replica databases) in the case of failure. As part of regular maintenance, servers are taken out of operation without impacting availability.

Business Continuity

Gorgias keeps continuous encrypted backups of data in multiple regions on Google Cloud Platform. While never expected, in the case of production data loss (i.e., primary data stores lost), we will restore organizational data from these backups.

Disaster Recovery

In the event of a region-wide outage, Gorgias will bring up a duplicate environment in a different Google Cloud Platform region.

Data transit

Data into servers

All the incoming connections towards our servers are required to be encrypted with industry standard SSL encryption. Latest SSL Labs report can be found here. We also obfuscate (strip) sensitive information such as Credit Cards, IBAN, SSN and others before it reaches our main database.

Data between our servers

Connections between our servers (i.e. web servers ↔ databases) are encrypted via TLS with a AES-256bit encryption method. Secrets such as database password, API secrets are encrypted using the same AES-256bit method.</→

Data out of our servers

Once the request is processed, the response is sent back using the same HTTPs SSL encrypted connection.

Data Security and Privacy

Data Encryption

All data in Gorgias servers is automatically encrypted at rest. Google Cloud Platform stores and manages data cryptography keys in its redundant and globally distributed Key Management Service. So, if an intruder were ever able to access any of the physical storage devices, the Gorgias data contained therein would still be impossible to decrypt without the keys, rendering the information a useless jumble of random characters.

Encryption at rest also enables continuity measures like backup and infrastructure management without compromising data security and privacy.

Gorgias exclusively sends data over HTTPS transport layer security (TLS) encrypted connections for additional security as data transits to and from the application.

Data Retention & Removal

Read more about our data lifecycle policy here.

PII removal

We recommend that users do not send any personally identifiable information (PII) to Gorgias. To mitigate accidents and other security risks, Gorgias offers server-side filtering as a default. We striping and obfuscating the incoming data such as Credit Card numbers, IBAN, SSN, etc...

Security Training

All new employees receive onboarding and systems training, including environment and permissions setup, formal software development training (if pertinent), security policies review, company policies review, and corporate values and ethics training.

All engineers review security policies as part of onboarding and are encouraged to review and contribute to policies via internal documentation. Any change to policy affecting the product is communicated as a pull request, such that all engineers can review and contribute before internal publication. Major updates are communicated via email to all employees.

Disclosure Policy

Gorgias follows the incident handling and response process recommended by SANS, which includes identifying, containing, eradicating, recovering from, communicating, and documenting security events. Gorgias notifies customers of any data breaches within 2 business days via email or phone call, followed by multiple periodic updates throughout each day addressing progress and impact.

Systems status live report

Gorgias maintains a live report of operational uptime and issues on our status page. Anyone can subscribe to updates via email from the status page. Any known incidents are reported there, as well as on our Twitter account.

Incident response plan

In case of a security incident it's best to have a clearly defined plan and responsibilities. Below you will find more details regarding the response plan that Gorgias has in place in the unlikely case of a security breach.

Responsibilities

Level 1: Depending on how the incident is reported/discovered we generally have the first level of technical support that is likely to triage/escalate the issue. Normally that role is reserved for whoever is on the level 1 tech support shift at the time.

Level 2: Is a senior engineer or CTO that classifies the impact of the security incident.

Level 3: CTO or CEO is responsible for the communication with the affected parties regarding the details of the breach.

Triage process

Before escalating the incident to the next level, the person that first finds out about it needs to verify the incident and its initial impact.

Escalation process

Once verified the escalation process should be immediate to level 2 and then level 3 verbally, by phone, email, whatever medium available.

Classification process

Once escalated the rank/severity of the incident must be determined. Does it affect all customers? A single company? An individual? What type of data was affected if any? Was it encrypted? If so, how?

Investigation process

Analyze all elements of the incident in order to identify all the causes or where a failure occurred including the software, hardware, people, and internal processes.

Lessons learned

Based on the result of the investigation, determine what could be done to prevent this attack and what defensive mechanisms failed and take immediate action to re-mediate the cause and improve the future process. This information should also be public and posted on our public blog.

Feedback

If there are any questions regarding this page, please contact us: support@gorgias.com