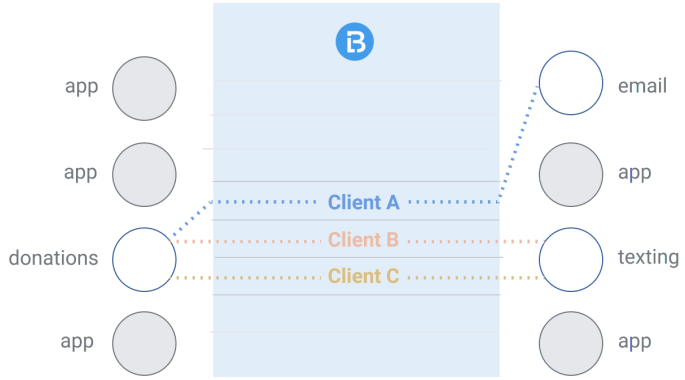
BLUELINK

Security Overview

Security is a key consideration for technology companies in general. The world of political tech brings unique security challenges. We at Bluelink understand this well and thus security is a high priority built into everything we do.

Encryption Everywhere

Bluelink encrypts data both in transit and at rest using strong, industry-standard encryption protocols (TLS 1.2+). Lightrail data pipelines are always run in their own isolated environments. Therefore, it is not possible for an organization's data to ever touch anyone else's data and even multiple pipelines run for the same customer remain separate.



Further, any third party credentials or keys placed within our system are encrypted both at the database and application layer, with each customer having their own keys. And should a customer wish to leave us, we ensure that all relevant data is purged from our system.

Continuous Evaluation

Security is a process, not a state of being, and so all systems at Bluelink are continuously evaluated for security concerns by both our internal engineering teams and external security professionals. We further provide a way for the public at large to notify us by sending any concerns to security@bluelink.org. Any potential vulnerabilities in the system that are uncovered are quickly triaged, analyzed and then mitigated as appropriate. We further employ robust monitoring systems which allow us to quickly detect outages and anomalies across our services, and then alert customers of anything that might impact them.

Leveraging Industry Standards

Bluelink systems are built on top of the same industry standard infrastructure used by companies all over the world. We use Google Cloud Platform (GCP) as our primary infrastructure provider, which brings with it an array of world class security features, in addition to high availability and scalability. GCP is compliant with ISO 27001, SOC 2 and SOC 3 standards and PCI DSS, among others. Read more about their certifications here.
We also apply industry best practices to our process and policies, such as adhering to the principle of least privilege when granting access to systems. For customer access, we use Google Auth, which means user credentials are never stored with us.

Our People

Bluelink employs technology professionals from all across the industry, bringing with them deep knowledge including integrating sensitive healthcare data, working on presidential campaigns and more. All employees are provided with an encrypted workstation and hardware multi-factor authentication token to ensure the highest level of security when building our systems. Device encryption and passcodes are required and enforced for all mobile devices with employee level access to Bluelink. Employees receive security training to stay up to date with best practices and are able to identify common threats. We strive to build a culture of transparency so that any employee feels empowered to speak up to identify issues or make suggestions.