The BPR Security Document

Your data security is our top priority. We are committed to safeguarding our customers' information by employing secure architecture, back-up procedures, and encryption. Our policies provide for ongoing monitoring and regular review of our security structure. We perform risk assessments and adapt our approach where necessary.

The BPR Cloud Instance Security

Our instances that customers use to process, store, or transmit data are run on dedicated instances within an Amazon Virtual Private Cloud (VPC). The VPC offers a set of network security features including stateless network access control lists and dynamic reassignment of instances into stateful security groups afford flexibility in protecting the instances from unauthorized network access.

Security is integrated in the design of our product.

AWS Shield includes Distributed Denial of Service (DDoS) protection service that safeguards The BPR running on AWS. It provides always-on detection and automatic inline mitigations that minimize application downtime and latency. It also offers protection against the most common, frequently occurring network and transport layer DDoS attacks like HTTP flood attacks, reflection attacks, etc.

Web Application Firewall (WAF) gives us the ability to allow and block traffic to The BPR. Rules on WAF block attack patterns such as SQL injection, HTTP flood attack, cross-site scripting, etc. Our technical team are notified whenever a request gets blocked. Further we have a sweet trap setup for bad bots that may try to steal information from the BPR application. An IP trying reach a resource which doesn't exist in the BPR app will be directed to the honeypot, with the IP registered in WAF with a bad-bot rule and the IP being permanently blocked.

The BPR Encryption

We utilize military grade AES-256 server side encryption & Secure Sockets Layer (SSL encryption) on the communications between the BPR application and our backend database.

The BPR Redundancy & Business Continuity

Our services provide for auditing capabilities, data back-up procedures, and disaster recovery mechanisms. Various properties are applied on Bucket level including:

- **Logging** tracks every access request to bucket, which is maintained in the bucket as a log file.
- **Versioning** allows you to preserve, retrieve, and restore every version of every object stored in this bucket. This provides an additional level of protection by providing a means of recovery for accidental overwrites or expirations.
- **Cross Region Replication** replicates every upload of every object with proper permissions in a bucket to another bucket. This helps protect data from accidental deletion or data being affected by any disaster.
- **Elastic Load Balancing** provides higher levels of fault tolerance for our application by automatically routing traffic across multiple instances and multiple Availability Zones. We use the Classic Load balancer because all network traffic must be encrypted in transit end-to-end, it also uses an encrypted protocol for connections. This feature enables traffic encryption between the load balancer and the clients that initiate HTTPS sessions, and for connections between the load balancer and customer back-end instances. All sessions are encrypted on both front-end and back-end listeners for transport encryption. Auto-scaling is also enabled which is well suited for applications that have either stable demand patterns or that experience hourly, daily, or weekly variability in usage, it also automatically increases the number of instances during demand spikes to maintain performance.

The BPR Policy and Monitoring

Data Deletion: We have an established life-cycle policy on our primary source bucket which after 60 days permanently removes extra versions of all files and also the files deleted by customers.

We allow only authorized individuals access to information when it's essential to complete tasks that improve our application and enhance security.

We perform regular reviews of our systems to ensure data integrity and security. We monitor our instances constantly for the emergence of new threats and perform risk assessments to ensure that we consider each new threat in the context of our security structure.

Any Questions?

General Inquiries: +1800-305-0493 **Support Ticket**: +1215-600-1538