# SECURITY///SERVER OVERVIEW

## SECURITY

All data is transferred securely behind an SSL. Once the data reaches our servers, it is behind our firewall with ip filtering (so our database server can only communicate with our webservers). All Front Rush data is backed-up onsite and offsite. All applications are similarly backed-up. In a disaster type situation, Front Rush is simply redeployed to a new environment with
a mirror of the original.

Front Rush uses IP filtering for direct access to the servers. The database server is only accessible through the web server. All connections are monitored and logged. Any breach would be immediately reported to the client base.

Front Rush uses an independent 3rd party, Pivot Point Security http://www.pivotpointsecurity.com, to audit and certify our security. This includes vulnerability scanning and pen testing. From pivot point: "we determined that Front Rush's application is secured in a manner consistent with or exceeding industry best practice and that the application is not vulnerable to the attacks outlined in the OWASP Top 10 (a broad industry consensus of the most critical web application vulnerabilities). Additionally Front Rush utilizes Alert Logic, a cloud-powered vulnerability and intrusion monitoring and log management solution. This 3rd party security service provides threat prevention capabilities and around the clock operations with their SSAE 16 Type II Verified Data Centers and team of security experts, enhancing the fortification of our infrastructure.

## SERVERS & PROVIDERS

Front Rush is hosted by aws.amazon.com. Our email delivery is provided by dyn.com. Our SMS delivery is provided by twillio.com.

Aws.amazon.com :: hosting, dyn.com :: email delivery, twillio.com :: SMS delivery

We back-up all data multiple times daily through AWS (in case of a meteorite type event). The data is accessed through secure connections by coaches (again both online and mobile) through https://frontrush.com or through our mobile apps.

## AWS INFASTRUCTURE

### SECURELY BUILT

The AWS cloud infrastructure is housed in AWS's highly secure data centers, which utilize state-of-the art electronic surveillance and multi-factor access control systems. Data centers are staffed 24x7 by trained security guards, and access is authorized strictly on a least privileged basis. All personnel must be screened when leaving areas that contain customer data. Environmental systems in the data centers are designed to minimize the impact of disruptions to operations. And multiple geographic regions and Availability Zones allow you to remain resilient in the face of most failure modes, including natural disasters or system failures. http://aws.amazon.com/security/

### CONTINUOUSLY MONITORED

The AWS infrastructure is protected by extensive network and security monitoring systems. These systems provide important security measures, such as basic distributed denial of service (DDoS) protection and password brute-force detection on AWS accounts. In addition, AWS infrastructure components are continuously scanned and tested. While some organizations perform vulnerability scanning on their resources once a quarter or once a month, we scan multiple times a day. And we scan from every possible angle— from within the same region as the resources being scanned as well as across AZs and regions.

### CONSTANTLY UPGRADED

We're not only replacing failed hardware on a continuous basis, we're always improving our infrastructure. We replace end-of-life hardware with the latest processors that not only improve performance, but also include security technologies such as the latest instructions for speeding up crypto operations (for example, Intel AES-NI instruction for AES algorithm, Intel RDRAND for random number generation) and the Trusted Platform Module chip for enabling hardware-based security features like secure storage and host software verification.

### HIGHLY AVAILABLE

AWS builds its data centers in multiple geographic regions as well as across multiple availability zones within each region. Each availability zone is designed as an independent failure zone. This means that availability zones are physically separated within a region and are located in lower risk areas. They are each fed via different grids from independent utilities to further reduce single points of failure. Availability zones are all redundantly connected to multiple tier-1 transit providers.

In the unlikely case of failure, automated processes move customer data traffic away from the affected area. Core applications are deployed in an N+1 configuration, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.

### FULLY COMPLIANT

For customers who must meet specific security standards or regulations, AWS provides certification reports that describe how the AWS cloud infrastructure meets the controls required by these standards. AWS has achieved compliance with an extensive list of global security standards, including ISO 27001, SOC, the PCI Data Security Standard, the Australian Signals Directorate (ASD) Information Security Manual, and the Singapore Multi-Tier Cloud Security Standard (MTCS SS 584). We have been granted two separate FedRAMP Agency ATOs: one for the AWS GovCloud (US) Region, and the other covering the AWS US East/West regions. We are also one of the only public cloud service providers to have been granted a provisional authorization for DoD CSM Levels 1-5. http://aws.amazon.com/compliance/