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/

SOLUTION OVERVIEW

ALERT LOGIC CLOUD DEFENDER FOR PCI COMPLIANCE

MAINTAIN CONTINUOUS PCI DSS COMPLIANCE

Organizations that process, store or transmit credit card data face tremendous pressure to comply with the comprehensive set of requirements outlined in the Payment Card Industry Data Security Standard (PCI DSS). Business fines up to $500,000, expensive litigation costs, damage to brand and loss of consumer confidence are just a few of the consequences of non-compliance. Because the PCI DSS mandates that security operations adequately protect customer information, organizations must embrace new policies and implement changes to network configurations while also ensuring that there is technology in place to protect cardholder data.

Alert Logic Cloud Defender provides an organization with the easiest and most affordable means to secure their networks and comply with the PCI DSS. As the security industry's only cloud-powered vulnerability assessment, intrusion detection, log management, and web application security solution, Alert Logic services help organizations eliminate the burden of PCI compliance in ways traditional security solutions cannot.

In addition, Alert Logic is a PCI Security Standards Council Approved Scanning Vendor (ASV) and maintains Level-2 SAQ Attestation of Compliance status. Cloud Defender also includes advanced risk reporting capabilities, including CVS risk scoring and "audit-ready" reports and dashboards for PCI QSAs.

DETAILED VULNERABILITY ASSESSMENT AND REMEDIATION GUIDANCE

To achieve PCI DSS compliance, you must identify and remediate all critical vulnerabilities detected during PCI scans. Cloud Defender streamlines this process by providing simple, actionable reports that detail vulnerabilities and recommendations. There is also a Dispute Wizard that helps document compensating controls that are in place to remediate specific vulnerabilities. PCI scans include the following reports:

Executive Summary: Overview of scan results and a statement of compliance or non-compliance.

Vulnerability Details: Provides a detailed description, list of impacted hosts, risk level and remediation tips for each vulnerability found.

Attestation of Scan Compliance: Overall summary of network posture, compliance status and assertion that the scan complies with PCI requirements.

PCI DSS 3.0 SOLUTIONS MAPPING

The integrated products and services that make up Cloud Defender meet specific PCI DSS requirements.

SOLUTION	REQUIREMENT	
NETWORK PROTECTION THREAT MANAGER & ACTIVEWATCH	5.1.1	Monitor zero day attacks not covered by anti-virus
	6.1	Identify newly discovered security vulnerabilities
	11.2	Perform network vulnerability scans by an ASV at least quarterly or after any significant network change (Includes 11.2.1, 11.2.2 and 11.2.3)
	11.4	Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network
LOG MANAGEMENT LOG MANAGER & ACTIVEWATCH OR LOGREVIEW	10.2	Automated audit trails
	10.3	Capture audit trails
	10.5	Secure logs
	10.6	Review logs at least daily
	10.7	Maintain logs online for three months
	10.7	Retain audit trail for at least one year
WEB APPLICATION FIREWALL WEB SECURITY MANAGER & ACTIVEWATCH	6.5.d	Have processes in place to protect applications from common vulnerabilities such as injection flaws, buffer overflows and others
	6.6	Address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks

ALERTLOGIC Security Compliance Cloud

U.S. 877.484.8383 | U.K. +44 (0) 203 011 5533 | www.alertlogic.com

PRODUCTS AND SERVICES

ALERT LOGIC THREAT MANAGER	• Threat Manager is a vulnerability assessment and intrusion detection solution. With Threat Manager and ActiveWatch, you can cost-effectively defend and protect your network against internal and external threats across centralized and distributed environments. • Cloud Defender's ActiveAnalytics expert system, purpose-built grid computing infrastructure, and the automatic aggregation and correlation of anomalous behavior patterns quickly identify threats and attacks.
ALERT LOGIC LOG MANAGER	• Log Manager automates log collection, aggregation and normalization, simplifying log searches, forensic analysis and report creation through real-time or scheduled analysis. Once logs are transferred to Alert Logic's secure cloud, Log Manager protects and stores the data to preserve against unauthorized loss, access or modification.
ALERT LOGIC WEB SECURITY MANAGER	• Web Security Manager provides active protection against web application attacks, one of the more prevalent threats to business-critical applications. Proactively blocking unauthorized activity, Web Security Manager effectively protects against the most dangerous attacks, such as SQL Injection and Cross-Site Scripting.
ACTIVEWATCH AND LOGREVIEW SERVICES	• Alert Logic products are backed by ActiveWatch services, fully managed intrusion detection, vulnerability scanning, log management and web application firewall solutions. • LogReview provides daily event log monitoring and review, and is designed to help you meet PCI DSS requirement 10.6. A team of certified security analysts acts as an extension of your team to expertly review your log data daily and alert you whenever suspicious activity or possible security breaches are detected. • Services are managed from Alert Logic's state-of-the-art, 24x7 Security OperationCenters (SOCs) in the United States and the United Kingdom, which are staffed by, which is staffed by security professionals with Global Information Assurance Certification (GIAC) from the SANS Institute.

EXPERT SECURITY SERVICES

By providing both products and expert services, Alert Logic Cloud Defender helps you fully meet PCI DSS requirements. For example, to meet requirement 10.6 (daily log review), either on an going basis (with ActiveWatch) or daily (with LogReview), our security analysts analyze event log data, track and escalate incidents, send notifications, and assess the health of your log collection. With either service, you'll meet the following PCI DSS requirements:

- Analyzes event log data for potential security incidents such as account lockouts, failed logins, new user accounts and improper access attempts
- Identifies incidents that warrant investigation and sends notifications for review
- Creates an incident audit trail for auditors and regulators
- Monitors log collection activities and alerts you when logs are not being collected
- Provides daily reports mapped to the PCI standard

ABOUT ALERT LOGIC

Alert Logic, the leader in security and compliance solutions for the cloud, provides Security-as-a-Service for on-premises, cloud, and hybrid infrastructures, delivering deep security insight and continuous protection for customers at a lower cost than traditional security solutions. Fully managed by a team of experts, the Alert Logic Security-as-a-Service solution provides network, system and web application protection immediately, wherever your IT infrastructure resides. Alert Logic partners with the leading cloud platforms and hosting providers to protect over 2,700 organizations worldwide. Built for cloud scale, our patented platform stores petabytes of data, analyzes over 400 million events and identifies over 50,000 security incidents each month, which are managed by our 24x7 Security Operations Center. Alert Logic, founded in 2002, is headquartered in Houston, Texas, with offices in Seattle, Cardiff, and London. For more information, please visit www.alertlogic.com .