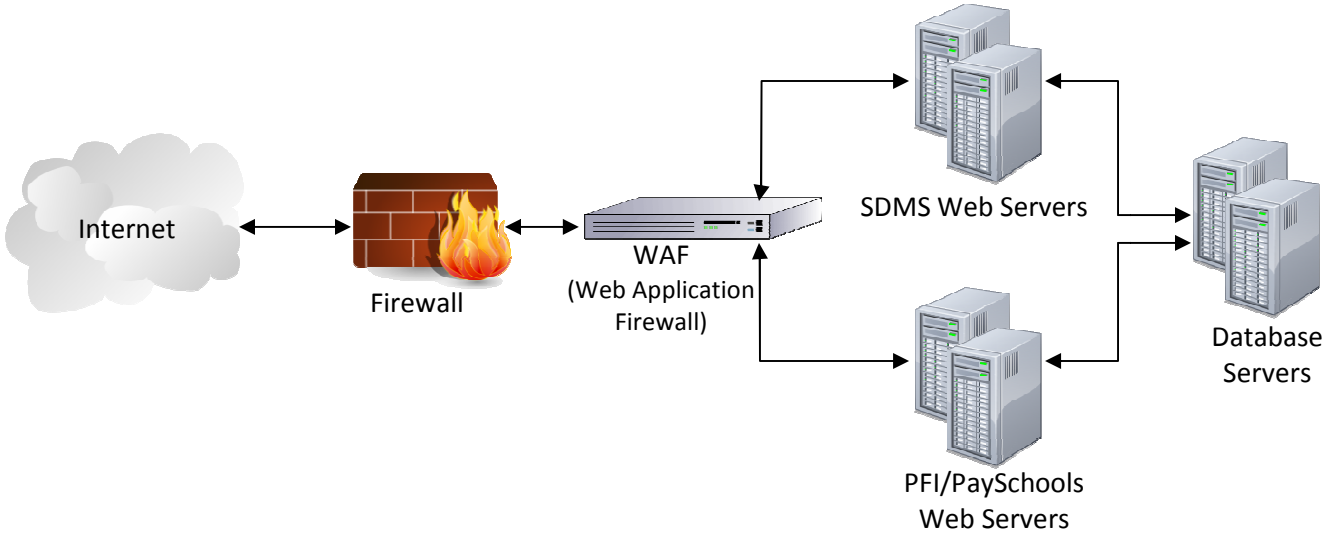
Data Business System Internet Security and Reliability

Data Business Systems understands your data is private and takes every step to ensure it is protected from unauthorized access and your data is secure and protected from loss and our systems are reliable:



PCI Compliance: All DBS servers reside inside a PCI Compliant environment. The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that data is maintained in a secure environment. PCI Compliance requires periodic review of business practices, software, network, and data vulnerability. Data Business Systems is required to maintain the highest level of PCI Compliance.

SSL Certificates: External communication is protected with 2048 bit SSL certificates issues by well known providers such as DigiCert Inc. The SSL protocol secures and authenticates the connection between the customer's browser and the server ensuring all data transmitted is encrypted.

Vulnerability Assessment: Alert Logic's Threat manager is a cloud powered vulnerability assessment and intrusion detection service to defend and protect systems against internal and external threats. All servers and network appliances are scanned periodically by Alert Logics Threat Manager to identify and address any potential vulnerabilities.

Managed Firewall: Managed firewalls provide the highest level of security earning ICSA Firewall and IPsec certification and Common Criteria EAL4 evaluation status. The firewall limits access to specific applications protecting internal services from the outside.

Threat Management: The Web Application Firewall (WAF) leverages industry-leading SecureSphere & ThreadRadar technology from Imperva, the leader in web application security. The WAF actively monitors the content of inbound traffic looking for possible hacking attempts and irregular traffic. Common threats are blocked automatically and are reported to network management.

Two-Factor Authentication: Remote access to the servers is protected by Two-factor Authentication backed by industry-leading RSA SecurID technology, with a 20 year history of outstanding performance and innovation and a team of CCSP and RSA certified professionals to fully manage the dedicated RSA SecurID appliances and tokens. Each RSA Authenticator token automatically generates a unique password every 60 seconds. Two-factor authentication using a unique PIN and authenticator password offers a more reliable level of user authentication than reusable passwords alone. Remote access is limited to a small group of internal employees that perform operations that necessitate access to the server environment.

Data Center Security: The data center is PCI-DSS and Safe harbor compliant in addition to having SSAE16 TYPE II, SOC1, SOC2 (Security and availability only), and SOC3 audits on file for all data center facilities. Specific policies exist to both prevent unauthorized physical access, damage and interference to the premises and information and to confirm that only approved users are granted access to appropriate systems and resources.

Track and monitor all access to network resources: Log Management: The Alert Logic Log Manager automatically aggregates, normalizes and stores log data from the hosting environment to simplify log searches, forensic analysis and report creation though real time or scheduled analysis. Alert Logic reviews logs daily to identify any potential security risks or system issues.

Anti-Virus: Fully managed anti-virus software provides proactive sustained protection against viruses, worms, Trojans, spyware and other malware on all windows and Linux servers. Advanced features include Behavioral Genotype Protection for zero-day protection by proactively identifying malicious code on file servers and deleting it before it executes or reaches endpoint computers on the network.

Redundancy: Uptime is important to DBS. The entire systems and networking infrastructure is redundant. Redundant web servers and failover database servers increase both the speed and availability of system services. Should one server fail for any reason or should it be taken off line for maintenance, redundant servers will take over its tasks. Power, environmental controls, data storage, and network infrastructure components are all redundant to provide nearly 100% uptime.

Backups: Data is hard if not impossible to replace, therefore servers are backed up on a daily basis and all databases are backed up every 12 hours. Data is stored on high speed RAID arrays and accessed over a Fiber Channel Fabric that ensures the best performance and the highest protection against data loss due to hardware or network failures.

Web Software: The web software was built from the ground up with security in mind. Access is limited by user and critical data is encrypted when stored in the database. Access to the software may be limited by IP address, so it's possible to set up SDMS so that it is only accessible inside a district.