Blackboard ASP Services

An Overview of ASP Security Measures – North America

The purpose of this document is to review the security measures taken by Blackboard ASP Services. In order to protect client data, this will be a general overview. However, this information should be sufficient to understand the extent to which client data is protected. This particular document is specific to Blackboard ASP’s datacenters in the United States. A separate document can be obtained that details the International datacenters.

Physical Security

Blackboard ASP Services are hosted in two physically separate AboveNet facilities referred to as VA1 and VA2 in the United States. The VA1 facility is located in Tyson’s Corner, Virginia. The VA2 facility is located in Reston, Virginia. A third facility, known as VA3, will be opened in Chantilly, VA, and will replace the current VA1 facility.

AboveNet is an Enterprise – Class provider with a high performance global optical network. AboveNet has six datacenter facilities located in North America as well as a London facility. Each data center is connected directly to AboveNet’s global all-optical IP architecture over a dedicated fiber optic network that reaches across the globe. With a commitment to providing uninterrupted service to its customers, AboveNet uses the highest standards for building and designing each data center to withstand natural disasters, security breaches (physical and cyber), power outages, and networking and computing failures.

Comprehensive security measures include 24/7 monitoring by on-site AboveNet staff including a guarded single point of entry. All employees and guests to the datacenter must wear identification badges at all times. In addition, Blackboard’s servers are stored in locked cages and vaults that are monitored using full-motion surveillance cameras.

Power redundancy includes a Continuous Power Supply (CPS) that protects against degraded commercial power and interruptions through the use of flywheel online generators and diesel backup generators that have enabled AboveNet to have 100% power availability. These state-of-the-art generators are part of an overall power system that clean and condition commercial electrical power to remove any irregularities in the signal. The CPS flywheel generators also eliminate the operational time restraints and unreliability of legacy battery-powered UPS (uninterruptible power supply) systems—which are often the cause of power failures in co-location facilities. According to analysts, the use of flywheel generators is also more environmentally friendly. All power is run through the CPS generators before
being passed into the facility; this builds up momentum in high-efficiency turbines. In the event of a loss of power from the grid, the momentum in the turbine ensures continuous power while the back-up generators come online. The back-up diesel generator can power the facilities at full power for several days before fuel re-supply is necessary.

In addition, AboveNet supplies a superior cooling system that ensures climate temperatures do not affect computing power; a Very Early Smoke Detection Alarm (VESDA) that constantly samples the air for dangerous particles; as well as state of the art fire suppression.

Blackboard ASP owns and operates all of network appliances and systems within Blackboard ASP network environment inside the AboveNet facilities.

**Network Security & Storage Equipment**

**NetScreen 500 Firewalls**
The NetScreen-500 is a purpose-built, security system designed to provide a flexible, high performance solution for large enterprise central sites and service providers. The NetScreen-500 security system integrates firewall, DoS, VPN, and traffic management functionality in a low-profile, modular chassis. It provides high levels of total throughput for firewall and VPN plus support for virtual systems and security zones. With a flexible and resilient hardware architecture that incorporates modular physical interfaces, redundant power supplies, fans, and high availability interfaces, the NetScreen-500 capacity by far exceeds Blackboard’s typical traffic conditions.

**Tipping Point UnityOne Intrusion Prevention System**
Tipping Point’s UnityOne Intrusion Prevention System (IPS) delivers the most powerful network protection in the world. The UnityOne is an in-line device that is inserted seamlessly and transparently into the network. As packets pass through the IPS, they are fully inspected to determine whether they are legitimate or malicious. This instantaneous form of protection is the most effective means of preventing attacks from ever reaching their targets.

The system is built upon TippingPoint’s Threat Suppression Engine - a highly specialized hardware-based intrusion prevention platform consisting of state-of-the-art network processor technology and TippingPoint’s own set of custom ASICs.

The UnityOne ASIC-based Threat Suppression Engine is the underlying technology that has revolutionized network protection. Through a combination of pipelined and massively parallel processing hardware, the TSE is able to perform thousands of checks on each packet flow simultaneously. The TSE architecture utilizes custom ASICs, a 20 Gbps backplane and high-performance network processors to perform total packet flow inspection at Layers 2-7. Parallel processing ensures that packet flows continue to move through the IPS with a latency of less than 215 microseconds, independent of the number of filters that are applied.

An integral part of the UnityOne solution is the Digital Vaccine Service that delivers new filters on a weekly or even daily basis to maintain evergreen protection for the latest vulnerabilities, exploits, viruses and rogue applications. TippingPoint’s Intrusion Prevention System is the first and only product to win the coveted NSS Gold Award in the IPS space.
**NetApp Network Attached Storage (NAS) Filers**

Blackboard’s ASP hosted clients application data resides on NetApp Filers. NetApp filers are reliable, fast, and scalable systems that simplify and unify enterprise data storage. Key features that enhance the reliability and availability of NetApp storage systems include:

- Built-in RAID for protection from data loss due to disk failures
- Hot spare disks for fast failure recovery
- Redundant hot-pluggable power supplies and cooling fans
- Battery-backed NonVolatile RAM (NVRAM) for guaranteed writes and improved performance

The newest filers in use by Blackboard ASP deliver industry-leading throughput and quick response times to meet the needs of even the most demanding applications. With the ability to scale up to 64TB (cluster model), the newest model can support an enormous amount of enterprise data and is the perfect storage system for storage consolidation.

**Server Access and Security Policies**

Blackboard ASP Operations Team uses the SSH2 protocol for restricted access to each hosted server. Only Blackboard ASP personnel, and, when authorized in a case-by-case basis, Blackboard Global Services technical developers, can have command-line access to ASP servers. ASP also locks down all unnecessary ports to further prevent intrusion. Parties outside Blackboard (including clients) are never given command-line access to ASP servers. Blackboard also runs an intrusion detection monitoring software on the network (Tipping Point Intrusion Protection System, see above) to constantly check for any potential intruders, and has hired a third party vulnerability assessment company to try to hack into the Blackboard network and provide audit reports.

**Data Backup Policies and Process**

ASP’s standard data retention window is 30 days. If a situation arises where an ASP client needs us to restore lost data, the client should contact ASP Support. ASP Services will complete four restore requests per license year at no charge. Beyond four restore requests, ASP will charge a fee of approximately $800 per incident for Enterprise clients. The fee covers the dedicated hardware required to perform these restores, as well as a few hours of labor for these time-intensive tasks. Implementing the fee (beyond four) also helps prevent frivolous requests from clients (some clients ask for restores every few weeks, without understanding the required effort).

Blackboard implements three levels of backups. First, blackboard takes advantage of a Snapshot utility that stores read-only versions of a file system and provides the ability to recover lost or deleted files without assistance or recovery from tape. Snapshots are performed daily. Blackboard also performs daily backups of all databases. Both the file system snapshots and the database backups are stored on disk with specific retention periods for more efficient recovery.

The second layer of backups utilizes a separate set of high-availability filers in a separate datacenter (except in the Amsterdam Datacenter where the redundant filers are located within the same datacenter). This second set of filers, which are also referred to as
Nearstore destination filers, mirror the same data and retention from the source. This added layer protects data in the event of site disasters. The third layer of backups uses a tape system. Each week, production file system and database backups are transferred to tape media and stored for 30 days. Since 30 days of backups (our standard data retention window) are stored in the first and second layers of backup architecture, the tapes should not be required unless a true disaster occurs.

All relevant data on the Blackboard network is backed up including application files, databases and operating system environments where needed.