

Security Overview

Background

The Kaplan EduNeering Platform is offered via the Cloud Computing or Software as a Service model. This widely used outsourcing model allows us to design and maintain the computer hardware, software, security, and personnel we need to deliver our solutions, without our clients incurring excessive capital investments and operational commitments.

Our expert IT staff is responsible for creating, managing, and supporting our technology-based solutions, to assure that all systems run smoothly and securely in our wholly-owned data center facility.

Physical Security

All security begins with physical security. Kaplan EduNeering's primary datacenter in Houston (shown to the right) is inside a office building with 24x7x365 on-site security. The building contains a back-up electrical generator capacity, and other equipment designed to keep servers up and continually running.

Once inside, a separate system validates the badge of an employee prior to entering the Houston office, and again before entering the datacenter. Logs of all entries into the data center are checked on a regular basis to ensure that only properly authorized personnel have access.

Similarly, Kaplan EduNeering's back-up datacenter in Princeton requires a badge to obtain access to the office, and a separate authorization to obtain access to the datacenter.

Network Access Security

Networks are protected by multiple state-of-the-art firewall systems. The data center network is automatically monitored for intrusion detection and other malicious activity including viruses.

To obtain remote access to the Kaplan EduNeering network over the Internet, an employee must be granted VPN access (placed into a VPN group within Active Directory).

Access is granted using standard Microsoft Active Directory credentials, including standard industry best practices on passwords. Kaplan EduNeering uses wireless access in our both our Houston and Princeton offices. That wireless access is secured by WPA2 RADIUS which also authenticates against Microsoft Active Directory.



Guest Access Security

Both the Houston and Princeton offices receive guests on a regular basis. Each office has a network for guest access. This will permit the guests to get internet access but will block them from making a connection to any of our resources.

While conference rooms and guest offices tend to be the most likely places which will be set for this guest network, any ethernet port within Kaplan EduNeering's network can be set for guest access if necessary.

Inbound Web Security

All Kaplan EduNeering uses multiple layers of security to protect inbound web traffic. All traffic must pass through a redundant cluster of Juniper/Netscreen SSG550M firewalls. Those firewalls perform industry standard port filtering and stateful packet inspection to prevent connections on any port except those which are used for standard business connections.

Packets which are destined for permitted ports are then inspected by Juniper's deep packet inspection technology. Any malicious packets that it sees are discarded. Packets destined for our production web servers then move to our Juniper Load Balancers (redundant model DX3250s). The load balancers open up each packet, decrypt the SSL packets, and then multiplex those packets into a single connection to our web servers. Malicious packets that are not properly formed will be dropped during this process. Those packets then are forwarded onto our web servers.

(continued on next page)

Inbound Web Security *(continued)*

All of our web servers have Trendmicro Client Security Agent installed on them. This includes a software based firewall with a second intrusion prevention system. Since this IPS comes from a separate vendor than the one that is installed in the Juniper firewall, it will have a higher likelihood of being able to prevent an attack that gets past the Juniper's defenses.

Inbound File Transfers

Kaplan EduNeering receives files from customers on a regular basis in order to facilitate things such as adding new employees into a client's list of users. The majority of these incoming transfers are encrypted with public key encryption, specifically PGP.

Since those incoming files can only be decrypted with our private key, any transmission that an attacker may be able to intercept will not be decryptable.

Some of our customers use SFTP in order to transfer files up to Kaplan EduNeering. Those transfers are being put on a Linux server running the OpenSSH SFTP server, an industry standard for securely transferring files. Transfers are authenticated using RSA keypairs.

Site-to-site VPN Security

All site-to-site VPN connections terminate on our Juniper/Netscreen SSG550M firewalls.

All of our site-to-site VPNs use either 3DES or AES encryption. Packets are authenticated using either MD5 or SHA1 header authentication.

Disaster Recovery Infrastructure

We have comprehensive policies, procedures and investment in hardware and communications capabilities, all of which protect against significant disruption to our systems and data within those systems.

We have redundant T-3 communication lines in Houston, TX, a T-3 line for the data center in Princeton, NJ, as well as hardware at the Princeton, NJ facility that is designed to support client activities if there were to be a catastrophic failure at the main data center in Houston, TX.

Additionally, we perform backups of our production systems so that no more than 15 minutes of data would be lost in the event of a disaster. These backups reside at the main data center in Houston, TX, and are also transmitted to our backup data center in Princeton, NJ. In addition, every 24 hours the data is written to a magnetic tape and sent off site for an additional level of backup protection.

In the Event of Close of Business due to Force Majeure (Natural Disaster)

We have structured our computing resources across our two main locations in New Jersey and Texas. In the event of a truly catastrophic disaster or complete loss of our main Texas data center facility, we maintain adequate computing and network resources in New Jersey to restore our systems for customer use within four hours.

