



Organization

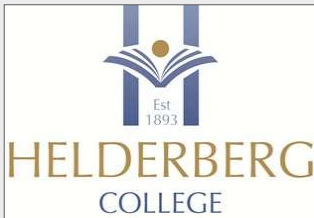
Helderberg College

Country

Cape Town
South Africa

Industry/ Vertical

Education



The network covered sensitive information which was under constant threat from spyware and DoS attacks. So they needed a strong Firewall and IPS solution.

- Mr. Lyndon Bender
IT Director
Helderberg College

Cyberoam Provides Cast-Iron Network Security to Helderberg College

About Helderberg College

Helderberg College is a private higher education institution situated in Somerset West, South Africa. It was established in 1893 - the first Seventh-day Adventist College established outside of North America under the name "Union College".

There are more than 60 buildings on campus including the church, administration and lecture buildings, library, auditorium, gymnasium and cafeteria, student centre, three-storey student residences, married students' flats, staff flats and homes, and separate church-operated primary and high schools.

The growth of the College is probably best reflected in the number of graduates which has increased from 8 in 1929 to an average of 40-60 a year.

The Helderberg College Challenge

According to Mr. Lyndon Bender, IT Director at Helderberg College, the institute was facing the following security and connectivity challenges related to its business activities.

Firewall and IPS

The Helderberg's network basically comprised of web and mail servers with no focused doorway security sketch. The outside of the DMZ is under constant attack. The inside is limited to the traffic that is routed to it. As an educational organization, Helderberg strives to facilitate the open exchange of information. Students, instructors, and librarians all need access to the Internet. Students rely on access to the web for vital course information and research purposes.

However, at the same time, Helderberg has a responsibility to protect users from network threats, and keep the network up and running. A top security priority was to establish a private network to keep confidential information safe from unauthorized users, hackers, and other threats. The college, therefore, needed a gateway firewall to regulate user authentication and access control.

Also, the sensitive servers were under constant threat from spyware, DoS attacks, fragmented and malformed packets, blended threats and more. Therefore, they needed a strong IPS solution which would be capable in retorting these threats.

Malignant Malware Attacks

For Helderberg College, a virus attack in the network would translate into a bunch of unwelcome problems – corrupt files, information theft, network anomalies, huge downtime and more. This would result into network crash. Helderberg was looking for a better option to combat blended threats lurking in the Internet.

Keep an eye on Website Access

The college wanted to monitor and restrict its users from accessing unproductive sites such as Music, Video, Social networking & Streaming media. Phishing, Pharming and nasty Websites also needed to be plugged away. Content filtering was needed to protect the users from accessing futile or deceitful websites. In case of blended threats, Mr. Bender was looking for a solution that could block all illicit download over the Internet.



Frequent downtime, virus and adware, were the chief security concerns faced by Helderberg College.

The Cyberoam Solution

Helderberg looked into a number of security products including Sonicwall and Astaro in order to address their business challenges, but they have limitations with Data Transfer Quota. The search was on for an appliance which would take care of their all above requirements. After going through a trial demo of Cyberoam by Xepa, they felt that Cyberoam was the apparent choice. The college then deployed One (1) CR 200ia and One (1) Cr35ia at their headoffice in Gateway mode.

The business benefits were as follows:

Access and Application Control

Cyberoam's Dual certified firewall – Checkmark and ICSA, provides access control over all the Internet traffic. Stateful inspection firewall and Intrusion Prevention solution guard the LAN and the DMZ network from unauthorized access and intrusion attempts.

All applications that tried to access Internet were logged and any un-productive application was blocked. If required, Mr. Bender can create custom signatures for custom applications. This gave him an unparallel control over all the network activities happening in the college.

Gateway level Antivirus

Cyberoam's gateway anti virus pickets all the web and mail traffic – SMTP, IMAP, POP3, HTTP, HTTPS and FTP-o-HTTP protocols and makes sure that no malware or spyware creeps through the boundary and the network is fully safe and sound against malware including root-kits, viruses, worms, Trojans, spyware, backdoors, key-loggers and more.

Each and every file going through gateway is scanned against antivirus engine that is powered by more than 4 million signatures.

Browsing Check Accomplished

Cyberoam UTM's web content filtering feature controls Internet access in the entire college network by blocking inappropriate and unsafe Web content, including phishing and other malware-laden sites. This is done through a constantly updated database of millions of sites divided into 82+ categories including pornography, P2P, entertainment and job search. Moreover, Cyberoam's identity-based filtering allows sets individual user Internet access policy, surfing quota, time limits and bandwidth restrictions.

By customizing students' identity-based policies, the administrator provides selective Internet access and surfing rights based on the staff and students working needs. "I can now prioritize the college's bandwidth usage as per academic requirements with more effective controls on which user consumes how much bandwidth (upload and download limits) during any time of the day", said. Mr. Bender. This helped the college in controlling the student's behavior on the Internet.

Reporting

Mr. Bender said, "The reporting capabilities are an essential component of the Cyberoam appliance. We consult the activity logs and reports on a weekly basis to ensure that the students and staff are using the Internet appropriately and have the information on hand when dealing with students who abuse our Internet Usage Policy."

Cyberoam ICSA and Checkmark certified firewall - provides granular access controls over Internet traffic and the network resources.

"The activity logs and reports on a weekly basis ensure that the students and staff are using the Internet appropriately", said Mr. Bender

Toll Free Numbers

USA : +1-877-777-0368 | India : 1-800-301-00013

APAC/MEA : +1-877-777-0368 | Europe : +44-808-120-3958

Copyright © 1999-2010 Elitecore Technologies Ltd. All Rights Reserved. Cyberoam and Cyberoam logo are registered trademark of Elitecore Technologies Ltd. Although Elitecore has attempted to provide accurate information, Elitecore assumes no responsibility for accuracy or completeness of information neither is this a legally binding representation. Elitecore has the right to change, modify, transfer or otherwise revise the publication without notice.

