

Corero's IPS provides University of Westminster with Advanced Degree of Security

Summary

Industry: Education

Challenge: To protect the university networks and end users from threats such as worms, zero-day exploits and distributed denial-of-service attacks, maintaining the freedom and flexibility required in a higher learning environment without impacting network availability or degrading performance.

Solution: Corero's IPS

Results: Corero Network Security prevents successful attacks against the university networks, controlling both the internal environment and Internet-facing perimeter, while maintaining unfettered network performance.

Key Benefits

- Stops advanced threats
- Lowest latency, superior throughput
- Reliable, purpose-built hardware
- Fast, easy deployment
- Blocks botnets, spyware, viruses and other malware
- Compatible with cloud-enabled infrastructure

The University of Westminster is one of the most popular universities in the U.K., with more than 20,000 students, 700 teaching staff and up to 1,000 visiting academics. Spread over four campuses, with a unique size and topology, the network is a real challenge to secure. With the help of Corero Network Security [formerly Top Layer Security] and its Three Dimensional Protection (3DP) technology, the University of Westminster was one of the first organizations in the U.K. to fully embrace network intrusion prevention systems (IPS).

The Challenge

Any security measures at the University of Westminster have to facilitate rather than restrict the university's philosophy of encouraging academic freedom. Hence, only basic firewall protection had been deployed to protect the network and its users. But a rising web presence and dependency made the university vulnerable, both as a target and a source, to an increasing number of threats, such as worms, zero-day exploits, distributed denial-of-service (DDoS) attacks and other sophisticated cyber threats. A initiative to address compliance issues also contributed to the university's decision to consider an IPS solution, which would protect against illegitimate traffic and undesired access and, ultimately, secure the network from the perimeter to the core.

The university specifically required that the IPS would have to be highly accurate in identifying bad traffic, thus preventing false positives and allowing legitimate traffic to flow without restriction, while deploying the best zero-day protection to mitigate any new threat. The university required that this improved protection must not impact availability and performance in its guaranteed 24/7 network environment.

The Solution

Corero Network Security's [formerly Top Layer Security] IPS was chosen because of its low latency, robust, flexible architecture and its high performance, with the ability to comfortably cope with the network's volume of traffic at high speeds. By using Corero's unique Three Dimensional Protection (3DP) technology, it would ensure that the university network would be protected from content-based attacks, such as virulent worm propagation (to which it had been susceptible), as well as DDoS and other rate-based attacks, and undesired internal or external access — all without compromising freedom of access and network performance.

The design plan was modularized to deploy IPS inside the university network to protect the existing firewall, and identify and block the spread of worm-infected hosts and any "creative" students testing their skills by using university resources to attack hosts on the Internet.

The second part of the design was to deploy at the perimeter to protect the network and Internet presence from attacks from the outside, as the university had been experiencing a lot of DDoS attacks, which were taking its firewall offline frequently.

“We are protected from the latest security threats by a dedicated team researching vulnerabilities.”

*Judie Ayoola, University of Westminster
Network Security Officer*

Corero's 3DP technology identifies the “contextual fingerprints” against the three dimensions of cyber threats: rate- and content-based attacks plus undesired access. This enables the university to mitigate attacks by blocking all genuine threats with remarkable accuracy in identifying malicious traffic while eliminating false positives.

Based upon multidimensional analysis of traffic, as opposed to relying on matching binary signatures, the 3DP architecture's flexibility enables Corero's IPS to focus on protecting against vulnerabilities in applications. This gives the university the very best protection against new and evolving threats, such as zero-day attacks on the network.

“The IPS was fast and easy to install without adversely impacting on the network, while company personnel were very accommodating. They worked to our timelines and understood our concerns for a phased-in approach. They took good care of us on this project and helped out with all aspects, including on-site training and help with implementation and tuning,” says Judie Ayoola, Network Security Officer at the University of Westminster.

“The automatic [Threat Update] security advisories service is also essential and comforting”, Ayoola continued, “as we are protected from the latest security threats by a dedicated team

researching vulnerabilities and pushing out policy updates that we have the option of implementing if we feel the threat affects our network.”

The Results

The deployment of the IPS instantly improved network traffic visibility and control, helping the university achieve compliance with data protection guidelines. Crucially, Corero's 3DP technology has given the University of Westminster the confidence that its network is now protected from all forms of attack and cyber threats. It is highly accurate, and the university can be sure it has the solution in place to block and mitigate zero-day attacks. In keeping with the university's goals, user access is guaranteed and network performance and availability have been maintained.

“We are very confident in the stability and accuracy of the IPS,” says Ayoola. “The ability to be protected in the event of a new exploit spreading before the security community has time to address it was crucial.”

“We are very confident in the stability and accuracy of the IPS.”

Judie Ayoola, University of Westminster

About Corero Network Security

Corero Network Security (CNS:LN) is a leading global provider of Network Intrusion Prevention Systems (IPS) and Distributed Denial of Service (DDoS) defense solutions. Enterprises rely on Corero to protect their critical online assets against risks associated with network-borne cyber threats. Corero, formerly Top Layer Security, is headquartered in Massachusetts, U.S. with offices worldwide. www.corero.com.

Corporate Headquarters

1 Cabot Road
Hudson, MA 01749
Phone: +1.978.212.1500
Fax: +1.978.212.1600
www.corero.com

EMEA Headquarters

No.1 Cornhill
London
EC3V 3ND
Phone: +44 (0) 203 427 3407

To purchase Corero Network Security solutions, please contact your Corero representative at **1.978.212.1500** or authorized reseller.