



## University of Dayton Blocks Cyber Attacks and Increases Bandwidth with TippingPoint

Founded in 1850, the University of Dayton is the largest, private university in Ohio and one of the top ten largest Catholic universities in the United States. The University of Dayton has over 70 academic programs for its 10,000 students, and is one of the most wired campuses in the country. All university housing is wired for high-speed internet access, and all students are required to own computers.

### The\_Problem

Like most universities, the University of Dayton needed to provide open network access to students, faculty and staff. The university was unable to stop attacks, such as Code Red and Nimda, that bypassed the firewall on Port 80 and other well-known ports. According to the university, approximately five Code Red infected machines can overwhelm the core campus router. Until the university implemented the TippingPoint, the only valid strategy was to apply patches before a server or workstation was allowed on the network, a labor-intensive process. The university also had no way to measure or assess if the network was infected or under attack.

Illegal file sharing is prevalent with students using peer-to-peer applications to download copyrighted music and video files. This can lead to legal ramifications, security issues and bandwidth abuse. The University of Dayton estimates that they received a dozen letters per month threatening legal action for piracy.

### The\_Solution

The University of Dayton installed the TippingPoint Intrusion Prevention System and immediately viewed attacks being blocked on the security management console's attack log. Since implementing TippingPoint in early 2003, the university estimates that over one million worms, viruses and attacks have been blocked each month. The Digital Vaccine® service allows administrators to download new security filters to the TippingPoint to protect against the latest vulnerabilities, and alleviates administrators' pain of patching systems individually.

TippingPoint enables customers to block peer-to-peer traffic uni-directionally or bidirectionally. The University of Dayton chose to allow students to retrieve shared files from outside the university network, but blocked people outside the university network from retrieving shared files located within the university. After implementing TippingPoint, reports show over one million shared files are blocked per month, augmenting the organization's bandwidth

*"TippingPoint gives me peace of mind. I am no longer comfortable with the idea of running our perimeter defense without it."*

**Ronnie Wagers**  
Network Systems and  
Security Officer  
University of Dayton

availability. Results from the University of Dayton show that the peak rate of bandwidth consumption without blocking peer-to-peer traffic or using bandwidth management tools was approximately 30 Mbps. After blocking peer-to-peer traffic uni-directionally with TippingPoint, bandwidth consumption dropped to a low of 17 Mbps within the first 30 minutes, giving a 43 percent increase in bandwidth availability.

## Value Proposition

Organizations can greatly increase their security and bandwidth availability while reducing the legal risk of piracy by blocking peer-to-peer file sharing applications. TippingPoint's Peer-to-Peer Piracy Prevention feature is included in all TippingPoint Intrusion Prevention Appliances and Systems. TippingPoint performs deep packet inspection through Layer 7, providing immediate protection against known threats and vulnerabilities.

**Corporate\_Headquarters:** 7501B North Capital of Texas Hwy. > Austin, Texas 78731 USA > +1 512 681 8000 > +1 888 TRUE IPS

**European\_Headquarters:** Herengracht 466, 2nd Floor > 1017 CA Amsterdam, The Netherlands > +31 20 521 0450

**Asia\_Pacific\_Headquarters:** 47 Scotts Road #11-03 Goldbell Towers > Singapore 228233 > +65 6213 5999