

*How do I best protect against Day-Zero  
Viruses and Worms?*

*Deploy a pre-emptive  
Outbreak Protection Solution.*



### **A Major Texas University**

#### **Situation**

A major Texas university recently invited Accudata Systems and NetScreen to present to it the latest in intrusion prevention technologies. The university also requested, as part of its invitation, that Accudata install a trial version of the NetScreen Intrusion Detection and Prevention Solution between two of its schools to evaluate its effectiveness.

#### **Solution**

Accudata and NetScreen installed the solution in passive mode, after flushing the logs. While Accudata and NetScreen presented the features and benefits of the NetScreen IDP Solution and firewall appliances, the product logged but did not filter out all detected intrusion attempts. The product was in place only for little more than an hour, yet it detected a significant number of worms and intrusion attempts – approximately 40,000 concurrent connections!

Upon reviewing the findings of the trial IDP Solution and seeing the number of issues detected, the university staff requested that the NetScreen solution be enabled for active prevention. The number of concurrent connections was reduced to 3,000! The NetScreen IDP Solution prevented all active worm and manual intrusion attempts.

#### **Resolution**

After purchasing the solution and putting it into production, the university has experienced a dramatic improvement in network performance, having all but eliminated worm outbreaks and malicious intrusion attempts. Its value proven, the NetScreen IDP Solution is planned for deployment throughout other university networks.

### **A Texas Based Utility Company**

#### **Situation**

Utility companies have a lot at risk. Security breaches can potentially impact millions of lives and cause significant outages. With concern for the security of its production SCADA systems, a Texas based utility company asked Accudata Systems to provide a solution that would proactively detect and notify the administration team when rogue behavior occurred.

#### **Solution**

Accudata Systems recommended a solution that combined network and host-based intrusion prevention solutions. By monitoring the network traffic and local systems services, the utility company's administrative team is now better informed of potential worm activity and intentional malicious behavior. In addition to increased awareness, the solution provided tools that are capable of proactively terminating the potentially harmful activity.

#### **Resolution**

After installing the IP solution, the utility company was able to confirm that its current firewall and network design was effective in preventing intrusion. Regular monitoring of log data and testing of the detection ability also confirmed that the production segments were secure and free from intrusion.

