

A Drastic Reduction in Malware Infections Across a Large Research University

Overview

Vanderbilt University, located in Nashville, Tenn., is a private research university and medical center offering a full-range of undergraduate, graduate and professional degrees. More than 12,500 full and part-time students attend the university. Their faculty numbers 3,300 and the university employees more than 20,000 full and part-time staff.

The Challenge

Serving Multiple Constituents

Vanderbilt is simultaneously a large research university, undergraduate college and thriving medical center. In many ways, it operates more like a small city than a traditional university. Director of Information Security Salvador Ortega said one of the biggest challenges for his department is balancing the needs of the various constituents the university serves.

Faculty researchers at Vanderbilt have research guidelines about what they can and can't do with data online. Additionally, they need to protect the intellectual property and research they are conducting for both Vanderbilt and the United States. Students view the Internet provided by the university as similar to that as provided by an ISP. For them, there are no restrictions on what's accessible — as long as the law does not restrict it, they can access the content of their choosing.

Finally, the staff population at Vanderbilt has various regulatory policies imposed on them. Staff members must comply with a Web use policy as outlined by human resources, while other groups are not required to comply. "These are policies similar to what you would expect in corporate America," explained Ortega.

A Flexible Solution Needed

Vanderbilt is a blend of centralized and distributed computer support. Several core computing infrastructure services are centrally managed, while desktop support is offered by both central IT and departmental IT services. Consumerization and innovation create a wide range of products, devices and set-ups. "We needed a service that we could offer that was flexible, yet non-intrusive, that didn't involve agent installs," explained Ortega. With such a wide range of needs from those using the Internet Vanderbilt provides, Ortega needed to find a solution that would support the customization and consumerization of the devices that connect to their network.

Malware Infections in the Student Population

Historically, students at Vanderbilt were offered a free anti-malware service they could install on their machines. The service wasn't comprehensive however, and student computers still experienced infections. With the way the student network was set up, once their computer was infected, they would be removed from the network, and responsible for cleaning their machine and removing any malware. This process was both time-consuming and expensive for students, who sometimes needed to take their machines off-campus to get the malware infection removed.



Organization Snapshot

Website:
<http://www.vanderbilt.edu>

Industry:
Higher Education

The Challenge

Provide security services across a university that functions much like a small city; provide Web content filtering to those areas that require it, while giving unfettered Internet access to those that don't.

The Solution

Deploy OpenDNS Professional as an opt-in service for the university with two different options: A malware, botnet and phishing service for students and faculty, and a service that also includes Web content filtering so staff can comply with Web use policies.

The Solution

A cloud-based solution that offers easily customized Web content filtering, best-in-class malware protection and does not require an agent install, OpenDNS Professional was the perfect choice for Vanderbilt University. Ortega and his team offer OpenDNS Professional as an opt-in service to any department at the university who would like to use it. They offer two pre-configured services: one that blocks only malware, phishing and botnets, and another that additionally offers Web content filtering used to enforce staff policies.

No Appliances, No Agent Installs

“The allure that we didn’t have to install an agent was very important to us,” said Ortega. “Everyone uses our DNS, so that’s a common thing enabling us to enforce safer Web surfing.” When researching solutions, Ortega looked at a different option for Web content filtering, but it was more complicated than Vanderbilt wanted. This alternative performed redirections to port 80 and other various Web ports, and required a firewall. In comparison, OpenDNS was cost-competitive, and didn’t require a new infrastructure in order to implement. In contrast to other options considered, minimal staff time is required to maintain OpenDNS Professional. Ortega estimates that managing OpenDNS Professional for Vanderbilt in its entirety is only 20–30 percent of one full time employee’s time.

Student Adoption Key

Since OpenDNS Professional was introduced to the Vanderbilt community as an opt-in service, Ortega and his team first targeted those areas that had the biggest pain points with regard to malware infections. The first target area was the student population. They were experiencing many malware infections on an ongoing basis. Ortega and Matthew Jett Hall, associate vice chancellor for ITS and enterprise infrastructure, met with Vanderbilt Student Government (VSG) demonstrated OpenDNS and the value of this malware prevention tool. After a short discussion, VSG members voted unanimously to adopt the malware, botnet and phishing protection tool for deployment across the entire undergraduate population.

Ortega said it’s been “extremely successful” with students and most importantly, the number of malware infections on the network dropped dramatically.

Speedy Adoption Campus Wide

It isn’t only the student network that’s now protected with OpenDNS. Other departments and divisions have since opted into the service, including the entire Division of Administration. Other departments also utilizing the Web content filtering statistics and reporting, which helped address “cyber slacking” among some staff members and found new ways to increase employee productivity. Ortega’s hope is that once there’s a critical mass, OpenDNS can be deployed across the entire university, including the university medical center hospitals and clinics.

As of January 2011, Vanderbilt prevented 1 million malware attempts from hitting their network by leveraging OpenDNS. The service also helped students avoid infections on their PCs, prevented university staff from wasting workplace hours on non-work related content, and gave Ortega and his team hours of productivity back in their work week to devote to other projects.