

Mi5 Kicks Botnets Off Campus at Santa Clara University

Mi5 pinpoints bots with unprecedented accuracy

It's an IT manager's worst nightmare: thousands of laptops that go home every night and may bring fresh malware back to school in the morning. Maria Gallagher, electronic security officer at Santa Clara University, describes the challenges of keeping her school's network safe:

"We have, potentially, over 14,000 systems on the campus at a given time, with more than 1,000 university-owned laptops used by the faculty and staff, plus student machines, and servers. So there are always lots of infected machines on the network, and there always will be, with new threats being introduced daily."

Before Mi5, Maria used ACLs (Access Control Lists) on her firewalls and desktop software to block threats. However, she knew there were threats that were being missed, but couldn't prove it.. She didn't know what the threats were or what laptops, desktops or servers they were on. Maria tells how the Mi5 appliance helps her do her job:

"We've always had a firewall with robust policies, but as our bandwidth grew, we found it wasn't keeping up. Before, I could only tell there was a problem if something bad crossed the firewall, but with the Mi5 reports I can pinpoint the problems because Mi5 looks at traffic flowing both in and out of the network, as well as inside the campus."

"I'm basically checking the Mi5 reports all day long. With other systems, I may not be able to track the problem to the specific building and machines, but with Mi5 I can immediately see if there's a machine with spyware on it or bots scanning inside our network."

"The Mi5 appliance gives our helpdesk a level of visibility that they can't get elsewhere. Whenever my other devices allow something to slip through, Mi5 tells us what it is, and points us in the right direction for cleanup."

– Maria Gallagher, Chief Security Officer, Santa Clara University



Organization

Santa Clara University
Santa Clara, California
www.scu.edu

Industry

Education

Challenge

Large educational institutions like Santa Clara University face special challenges, the most formidable being a highly mobile population. Santa Clara has thousands of day students and hundreds of faculty who may take their laptops home at night and return with fresh infections.

Solution

Mi5 helps the IT staff reduce their workload from a single location in the network, by removing guesswork and pinpointing infected machines on the network.

The Results

“With Mi5, we are able to detect bots with amazing accuracy, and remove them from our campus. Sometimes users have a false sense of security because an attack disabled the antivirus engine’s functionality. You can’t see the infection, so you feel good about things, and you figure everything’s fine. But the Mi5 reports lets the end user see right there on the screen that they’ve got a problem. They say ‘Wow, look at all of that.’”

About Santa Clara University

Santa Clara University, a comprehensive Jesuit, Catholic university located in California’s Silicon Valley, offers its students rigorous undergraduate curricula in arts and sciences, business, and engineering, plus master’s, Ph.D., and law degrees. Distinguished nationally by the fourth-highest graduation rate among all U.S. master’s universities, California’s oldest operating higher-education institution demonstrates faith-inspired values of ethics and social justice.

About Mi5 Networks

Mi5 Networks enables organizations to defend their web perimeter, and eliminate lost employee productivity, PC clean-up costs, and data theft associated with undetected malware. The company’s Webgate security appliances protect organizations against web-based threats, including malicious URLs, spyware, crimeware, botnets and viruses, while providing control over web use. Mi5 Networks was named a visionary by research firm Gartner for its innovative malware detection and protection capabilities, and low latency architecture. Mi5 Networks is privately held and based in Sunnyvale, California. For more information visit: www.mi5networks.com.



Why Mi5?

“I do a weekly report on all types of security systems, and I use the Mi5 reports to identify the types of infections or security risks we’re seeing in the network. The reports tell me what infections exist on each machine, including active bots, and identifies the machine name, location in the network, and user group. They have been very accurate. It is very helpful.”

Implementation, Ease Of Use

“When there’s a new exploit, but there’s no signature available yet from the anti-spyware and antivirus vendors, Mi5 gives me insight into what might be going on.”

Support Experience

“Very responsive. It’s been a pleasure to work with them. When I’ve sent them specific questions, I’ve gotten back a very good analysis about exactly what I’m seeing on my machine.”

Benefits Realized

“I like the constant updating, and the fact that I can get a level of detail right down to the machine. In other words, it doesn’t just show me addresses that have problems, it actually shows us really good detail about the individual system.”