CUSTOMER STORY *(Cybersecurity)*

University Deploys Core Security Network Insight

To Fight Botnets and Cyber Threats

The Challenge

Securing campus networks is a unique challenge for Universities. The abundance of personal laptops and mobile devices entering the network makes it more difficult to lock down computing resources or enforce standardized configurations. At universities today, the young, tech-savvy population demands unfettered access to Internet resources and social networking sites, providing unlimited infection vectors for botnet operators and cyber criminals.

Protecting its student and faculty population has always been a top priority for one large urban research University that serves traditional and nontraditional students at both the graduate and undergraduate levels. This University's network is accessed by over 40,000 students and faculty.

The Approach

"Cyber criminals today are getting more and more sophisticated, and the threat landscape is rapidly changing," said the University's chief information security officer (CISO). "With the growing use of personal devices within our network, comes increased risk. We needed a solution to automate the process of finding the botnet threats. Core Security Network Insight was chosen based on its auto-detection capability and its ability to easily pinpoint infected assets."

The University had been using manually intensive processes to correlate data from a variety of security solutions in an effort to identify botnets and malware infections. But the CISO quickly realized that the existing procedures did not scale to the current threat level, was not identifying all the threats, and consumed precious security resources. After reviewing several alternatives, the University selected Core Security.The Approach

Large university sees dramatic results using Core Network Insight to detect botnet and other cyber threats that rely on advanced malware and network-based command-and-control (CnC).

The Result

By implementing Core Security Network Insight, the University has been able to offload first-level remediation response to its data center operations,freeing up information security resources for other initiatives.

"With Core Security Network Insight, we can more rapidly detect and remove infected users from the network before their infection can do harm to University resources or expose the user to identity theft or fraud," said the CISO. "Using Network Insight, we can identify threats as they emerge and more quickly remediate the user's machine. Core Security provides us with an easy-to-use solution to defend against the silent threat of botnets and advanced malware."

"This University is on the forefront of educational institutions addressing the advanced nature of today's cyber threats," said Core Security. "Universities have the added challenge of operating a borderless network with student and faculty bringing personal laptops and a wide variety of devices with various operating systems and applications in and out of the network. They understand that today's advanced malware is elusive and will defeat even the best prevention technology. Core Security is uniquely positioned to detect and terminate these threats before they can do harm. We are pleased to have this University join our growing list of higher education customers."

> ***"With the growing use of personal devices within our network, comes increased risk. We needed a solution to automate the process of finding the botnet threats. Core Security Network Insight was chosen based on its auto-detection capability and its ability to easily pinpoint infected assets."***

coresecurity
by HelpSystems

www.coresecurity.com

About HelpSystems

HelpSystems is a people-first software company focused on helping exceptional organizations Build a Better IT™. Our holistic suite of security and automation solutions create a simpler, smarter, and more powerful IT. With customers in over 100 countries and across all industries, organizations everywhere trust HelpSystems to provide peace of mind. Learn more at www.helpsystems.com.