CASE STUDY

Webroot® Spy Sweeper® Enterprise Helps University of California, San Diego Medical Center Protect Patient Data and Secure Network against Online Threats

The University of California San Diego Medical Center recently chose Webroot Spy Sweeper Enterprise over competing antispyware solutions based on product effectiveness and centralized management capabilities.

Overview
Webroot Software was recently selected by the University of California, San Diego (UC-San Diego) Medical Center to protect and secure approximately 3,700 desktops and workstations throughout its medical campus. After a thorough testing phase, the UC-San Diego Medical Center selected Webroot Spy Sweeper Enterprise over Microsoft® Windows Defender, Sunbelt CounterSpy™ and PC Tools’ Spyware Doctor™ to provide comprehensive and proactive network protection against spyware and other malicious malware threats. In doing so, Webroot will protect medical data for a facility that has more than 21,000 admissions and more than 454,000 outpatient visits annually.

Despite having existing enterprise class antivirus and content filtering capabilities installed on its network, the installation of Webroot Spy Sweeper Enterprise immediately found and removed over 4,000 potentially unwanted items located on UC-San Diego Medical Center workstations. In addition, Webroot’s centrally managed administration console allowed the UC-San Diego Medical Center IT staff to establish a stronger security policy and to proactively manage and report on every individual workstation deployed throughout its network.

The following case study describes the UC-San Diego Medical Center’s situation prior to installing Webroot Spy Sweeper Enterprise, what key factors led to the decision to select Webroot, and how Webroot Spy Sweeper Enterprise has performed since installation.

About the UC-San Diego Medical Center
The UC-San Diego Medical Center is part of the renowned University of California system, one of the most respected education and research institutions in the world. U.S. News & World Report rankings have consistently recognized the UC-San Diego School of Medicine as one of the top medical schools in the country for its clinical and research excellence in a wide range of specialties, including cancer care, orthopedics, respiratory care and gynecology. UC-San Diego physicians have also been honored consistently by publications listing “The Best Doctors in America,” “America’s Top Doctors” and “San Diego’s Best Doctors.”

Situation
As a major medical center in the region, comprising two hospitals, a cancer center and affiliated outpatient and specialty clinics, the UC-San Diego Medical Center handles more than 21,000 admissions and more than 454,000 outpatient visits annually. Connecting this large medical center is a network of approximately 3,700 workstations and kiosks used by staff, faculty, and patients. While the UC-San Diego Medical Center did have a comprehensive security policy, including enterprise class antivirus and content filtering solutions, the Medical Center IT staff began to notice decreased performance and an increasing number of pop-up ads on Medical Center workstations. Pop-up blockers were installed on campus workstations but had to be disabled to support medical software being used throughout the UC-San Diego Medical Center network environment.
Case Study: UC-San Diego Medical Center

Initial attempts by Medical Center IT staff to restore performance and remove any potentially unwanted items were accomplished by reimaging infected workstations. However, after witnessing its operational costs rise due to increased demand for workstation reimages, IT staff soon realized that despite its efforts and existing security policy, there was a more serious malware problem that needed to be addressed.

Solution

The UC-San Diego Medical Center quickly sought antispyware software recommendations from its peers within the University of California system. After a successful installation at the University of California, Los Angeles (UCLA), Webroot Spy Sweeper Enterprise made the short list of antispyware products to be tested. Other products selected included Microsoft Windows Defender, Sunbelt CounterSpy and PC Tools’ Spyware Doctor.

After a comprehensive analysis, the UC-San Diego Medical Center selected Webroot Spy Sweeper Enterprise over the competing solutions based on its effectiveness at identifying, blocking and removing potentially unwanted items, its centrally managed administrative console, its reporting capabilities and its value when compared to the other solutions. Additionally, the UC-San Diego Medical Center IT staff liked Webroot’s ability to lock down client workstation settings to prevent users from tampering or uninstalling the antispyware client.

Results

After an initial pilot to test configuration and network compatibility, Webroot Spy Sweeper Enterprise was quickly and easily deployed across the UC-San Diego Medical Center’s network of 3,700 workstations. Upon installing the administration console and updating all workstation clients with the latest spyware definitions, the UC-San Diego Medical Center began to analyze its network for existing spyware and malware threats.

The initial scan of its network yielded impressive results by identifying and removing over 4,000 potentially unwanted items from campus workstations.

In addition, Medical Center IT staff also reported improvements in workstation performance as a result of the malware removal.

Since its initial deployment and workstation scans, the UC-San Diego Medical Center IT staff reports that Webroot Spy Sweeper Enterprise continues to detect and remove potentially unwanted items, a testament not only to the health of the UC-San Diego Medical Center’s network, but also to the proactive real-time security capabilities of Webroot’s powerful Smart Shields. These shields proactively block spyware and other malware threats that exhibit spyware behavioral characteristics including some Trojans, keyloggers, and rootkits.

The ability of Webroot Spy Sweeper Enterprise to successfully identify, block and remove potentially unwanted items from a network environment with existing antivirus and content filtering capabilities validates the necessity for an enterprise class antispyware solution to protect and secure company assets and customer data. In addition, the installation of Webroot Spy Sweeper Enterprise at the UC-San Diego Medical Center has not only removed annoying and performance robbing items from its network environment, but has also served to proactively protect patients’ online data through Webroot’s real-time protection capabilities. IT administrators have also been pleased with Webroot’s centrally managed administrative console, providing the ability to efficiently manage a networked workstation environment, saving IT staff resources, time and money.

For More Information

For more information about the UC-San Diego Medical Center please visit http://health.ucsd.edu/

For more information about Webroot Software, Spy Sweeper Enterprise and Webroot’s other award-winning corporate security products, please visit www.webroot.com/business or call 1-800-870-8102 to speak with a sales representative.