Culver City's New Public Wireless Network Stars Vernier Adaptive Security Platform

A Vernier Networks Case Study

Vernier Networks, Inc.
465 National Avenue
Mountain View, California 94043

www.verniernetworks.com

Challenge: Adaptive Network Security and User Management for a Busy Downtown

Culver City, a city of 40,000 on the west side of Los Angeles, has long been known as the "Heart of Screenland," because of its central role in the history of Hollywood. Movie studios have been located here since 1915 when Harold Ince founded Triangles Studios, which later became Metro-Goldwyn-Mayer. Today Culver City is home to Sony Pictures Entertainment World Headquarters, several theaters including the new Kirk Douglas Theatre, and a host of thriving businesses.

As of September 9, 2004, there's a new screen that people can watch in Culver City—the screen of any Wi-Fi enabled computer. As a free service to residents, workers, and visitors, Culver City has launched a free broadband Wi-Fi hot spot covering roughly a square mile of downtown streets. The coverage zone includes an outdoor performance and gathering spot; a public park, the Culver Hotel, and numerous outdoor cafes, retail stores, and offices. Culver City's network is the first public broadband Internet hot spot on the west side of Los Angeles. Within the coverage zone, free Internet access is available to anyone with an 802.11b-compliant computer.

Culver City has launched a free broadband Wi-Fi hot spot covering roughly a square mile of downtown streets. Within the coverage zone, free Internet access is available to anyone with an 802.11b-compliant computer.

The Culver City Wi-Fi hot spot is the brainchild of two city organizations, the Redevelopment Agency and the Information Technology department. Early in the project, the project's organizers recognized that network security and manageability would be critical to the project's success. The city government needed to protect its own network and internal communications from viruses, worms, and any intrusions introduced through the public network. The wireless network would have to secure enough to protect the information assets of a busy city government, while remaining accessible enough for coffee drinkers surfing the Internet in a nearby park.

Proprietary security solutions were ruled out. The city could not ask the public to install special software or hardware in order to keep the network safe. Instead, the hot spot would have to work with whatever computers that the public cared to use, even if those computers were infected with malware. Network security would be assured by technology that automatically detected security threats such as worms and viruses and removed them from the network in real time. Security would be built into the network, rather than hoped for in network users.

Manageability was another important concern for the city. "I have many responsibilities in addition to the hot spot," explains Carlos Vega, a network manager in the city's IT department. "If I can find a network security solution that saves me time, that's great."

Reducing the time required to manage security products was a critical factor in ruling out solutions such as Cisco VPN concentrators. "I've been online at other hot spots that use WEP and Cisco VPN concentrators for security, so I'm familiar with them," says Vega. "They don't have all the features we need, and I know how hard those systems are to configure. We needed a more practical feature rich solution."

® 2004 Vernier Networks, Inc. All rights reserved.

The Solution: The Vernier Adaptive Security Platform

In the summer of 2004, Culver City deployed a Wi-Fi network secured by the Vernier Adaptive Security Platform (ASP). The Vernier ASP is the first adaptive network security system that enables organizations such as city governments to assure secure business continuity on their wired and wireless networks. The Vernier solution proactively protects networks from increasingly complex malware attacks, automatically removing threats when they appear in the data path. Highly configurable, the Vernier ASP continuously adapts security policy to respond to changing network conditions and to defend against evolving security threats.

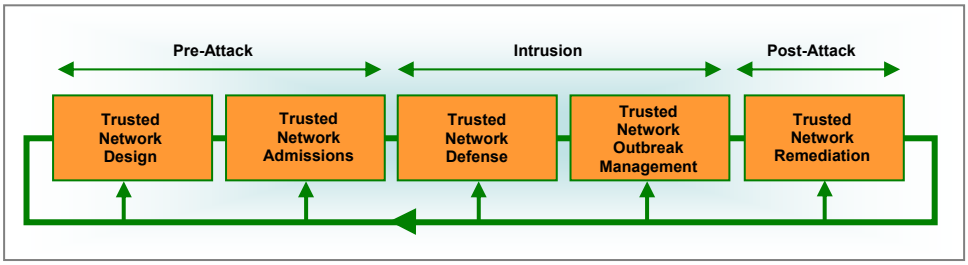
"The Vernier system made security a whole lot easier for us," says Carlos Vega. "The Vernier ASP is at the center of what we're doing. It connects to the public hot zone, the city hall network, and a broadband line to the Internet."

A registration and login solution for the hot spot was created using the Vernier ASP's authentication and redirection features. Now when a member of the public attempts to access the hot-spot network, the Vernier ASP detects the attempt and serves the user a login and registration page. "We collect basic information such as the user's name and zip code," says Vega. "The zip code enables us to track how many users are visitors to the area. The hot spot is conveniently located by two major freeways, so we're hoping to attract people who will drop by to surf. The Vernier system lets us identify demographic trends and usage patterns."

Once users are logged in, the Vernier ASP monitors their traffic for viruses, worms, and other malware. The Vernier ASP automatically removes malicious traffic from the network data path and block malicious traffic from attacking network infrastructure assets such as routers. If a user's computer is infected, the Vernier ASP quarantines the computer until it has been cleaned. If a user has been idle for 5 hours, the Vernier ASP automatically logs the user out.

Results: Network Security and Business Continuity

"I like the Vernier product a lot," says Vega. "It gives us the security we need, as well as control over a large user population. It's a very granular system. You can pretty much do whatever you want with it. It's been performing very well for us."



REDUCING THE TIME REQUIRED TO MANAGE SECURITY PRODUCTS WAS A CRITICAL FACTOR IN RULING OUT SOLUTIONS SUCH AS CISCO VPN CONCENTRATORS. "I'VE BEEN ONLINE AT OTHER HOT SPOTS THAT USE WEP AND CISCO VPN CONCENTRATORS FOR SECURITY, SO I'M FAMILIAR WITH THEM," *SAYS CARLOS VEGA, A NETWORK MANAGER IN THE CITY'S IT DEPARTMENT.* "THEY DON'T HAVE ALL THE FEATURES WE NEED, AND I KNOW HOW HARD THOSE SYSTEMS ARE TO CONFIGURE. WE NEEDED A MORE PRACTICAL FEATURE RICH SOLUTION."

® 2004 Vernier Networks, Inc. All rights reserved.

The Vernier ASP protects the Culver City network with five layers of security:

Trusted Network Design: Using the Vernier ASP, the city's IT team can define access policies that meet the needs of various user groups while minimizing the risk of intrusion. For example, Vernier ASP can be configured to prevent laptops from communicating directly with a network router, eliminating the risk of these devices launching a Denial of Service (DoS) attack on the router.

Trusted Network Admission: Through an automated screening system managed by the Vernier ASP, Culver City can ensure that only users whose computers are in compliance with campus security policies can gain access to the network. The Vernier ASP authenticates users against the city's authentication system and ensures that users access only those resources for which they have authorization.

Trusted Network Defense: The Vernier ASP offers in-line intrusion detection and protection and provides real-time defense against viruses and worms. The system recognizes attack patterns and blocks attacks from spreading to the rest of the network. The Vernier ASP's fine-grained policy controls enable the city's IT department to automatically enforce user- and location-specific security policies, such as requiring internal users to connect with a VPN when working in City Hall.

Trusted Network Outbreak Management: The Vernier ASP enables the city's IT department to respond effectively to any virus and worm outbreaks that occur, minimizing productivity losses and downtime. Infected nodes are immediately identified, quarantined, and blocked from attacking the network or infecting others. The Vernier ASP takes action automatically and requires minimal policy changes or human intervention.

Trusted Network Remediation: The Vernier ASP enables the city's IT department to analyze attack patterns and to adapt security policies to prevent future attacks.

"I like the fact that Vernier is brand-independent (non-proprietary)," says Vega. "I have access points from three different vendors connected to the Vernier system. I can roam from one coverage zone to another without interruption. Everything just works."

The City plans to expand the city's use of the Vernier ASP. Soon, the Vernier system will provide network security for PDA, Tablet PC, and Laptop users in the city's police department, fire department, and permitting office. The Vernier's built-in Guest account will provide controlled network access for contractors and others visiting the city offices.

Vega expects use of the hot spot to increase, as word spreads about the free service and its attractive setting in parks and public areas. "People love the new hot spot," says Vega. "They're comments are extremely positive."

As this latest offering from the "Heart of Screenland" becomes more popular, the Vernier ASP will ensure that Culver City network remains secure, always available to give its best performance.

® 2004 Vernier Networks, Inc. All rights reserved.

At a Glance

Challenge: Culver City needed to protect its city hall network from malicious intrusions and malware, while delivering free, convenient broadband Internet service to the general public in a downtown Wi-Fi hot spot.

Solution: To secure the network, Culver City deployed Vernier Networks' Adaptive Security Platform (ASP), a multi-layer security solution that continually adapts security policies to changing threat levels and network conditions. Through its adaptive security controls, the Vernier ASP assures business continuity on wired and wireless networks.

Results: Culver City is realizing these benefits from the Vernier ASP:

Trusted Network Design: The Vernier ASP provides a comprehensive security layer for defending and managing access to the city network. The Vernier ASP eliminates threats that exploit network access, such as DoS attacks directed at routers.

Trusted Network Admission: Through an automated screening system managed by the Vernier ASP, the City of Culver City is assured that only users whose computers are in compliance with the city's security policies can gain access to the network. The Vernier ASP authenticates users and ensures that they access only the resources for which they are authorized.

Trusted Network Defense: The Vernier ASP enforces authentication and access policies in real time, ensuring that users access only the resources for which they have authorization. The Vernier ASP automatically removes threats from the data path.

Trusted Network Outbreak Management: The Vernier ASP automatically quarantines computers not known to be safe and computers harboring viruses or worms. Users regain access to the network only after their computers have passed rigorous screening.

Trusted Network Remediation: The Vernier ASP enables the Culver City IT department to analyze attack patterns and to adapt security policies to prevent future attacks.

® 2004 Vernier Networks, Inc. All rights reserved.