Case Study

Lane County Head Start

Project:
» Network access control
» Prevent unauthorized devices

Major challenges:
» Large network with 19 subnets and renters
» Linux and Windows

The background

The Head Start program is widely recognized as the most successful, longest-running national school readiness program in the country. For more than 40 years, Head Start has delivered education and health services to low-income families.

The Head Start organization of Lane County, Oregon provides comprehensive developmental services to the county's low-income preschool children, ages three to five, and social services for their families. Lane County Head Start focuses on key areas like education, socio-emotional development, physical and mental health, and nutrition.

With a population of nearly 350,000, Lane County covers almost 5000 square miles and contains the second-largest urban area in Oregon. To provide its vital services to families all across the county, Lane County Head Start maintains 19 separate facilities. The IT network connecting all these sites is large and complex, with more than 250 nodes, 19 firewalls, and numerous servers and routers, including some that belong to third-party Internet service providers (ISPs) like Comcast.

A formidable challenge

Mel Stiner, the information services manager for Lane County Head Start, is responsible for managing this complicated network, including all the hardware and software that comprise its infrastructure, and ensuring that it's always up and running smoothly. He's also responsible for network security at all 19 sites, which presents a formidable challenge.

"The staff at all of our facilities relies on our network and the applications that run on it to do their jobs, so keeping the network secure is critical," explained Stiner. "An unauthorized device plugging into the network can wreak havoc. For example, someone plugged in an unauthorized router that issued its own IP addresses to different nodes, which brought down all of the printers on the network."

According to Stiner, it usually took hours of searching to find the source of a problem like this and fix it. "We were completely in the dark. We could see on the firewall that something unauthorized was there, but we had no insight into the nature of the security problem or where it was occurring. It could be a simple device issue, a rogue desktop or router plugging in, or someone infiltrating the network from outside. We literally had to search through the entire network for the physical item causing the security breach."

Over time, the problems were becoming more frequent and harder to trace. All of Lane County Head Start's 19 sites are networked together to a main switch. Some of its facilities rent out unused office space to other groups, which opens new security risks. Even though renters are told to provide their own network and Internet connections, people were just plugging their own laptops into any open port and going on-line. This gave them open access and the freedom to probe within the network.

Reducing vulnerability and controlling network access with Veri-NAC.

Increasingly concerned about network vulnerability, Stiner decided to look for a solution to help his IT team manage network access

> *"I can't say enough good things about Veri-NAC. We haven't found anything yet that Veri-NAC can't do when it comes to ensuring network security. It's a fantastic product."*
>
> *Mel Stiner, Information Services Manager, Lane County Head Start*

Lane County Head Start

control and minimize security risks. Going into the evaluation process, he identified several key selection criteria.

First, he needed a solution that could handle a mix of Linux® and Windows® boxes equally well. It had to be easy for his team to learn and use. Most important, it had to free his people from the endless hours of tedious troubleshooting. They needed a solution that would provide them with real-time actionable information and instantly pinpoint anomalies, incursions, and unauthorized access.

Stiner chose Veri-NAC network access control appliances from Black Box, initially implementing one 5400 model and two 5250 models. The Veri-NAC appliances now allow only authorized devices to access the Lane County network. Veri-NAC validates that each connected machine complies with requirements specified by Stiner's team, including operating system and configuration. It also provides the IT team with much-needed real-time insight into everything that is happening on the Veri-NAC monitored network.

According to Stiner, the installation was simple, straightforward, and fast, with no disruption of network operations. The Black Box support group walked Lane County's IT team through the configuration and system menus over the phone, and the team was good to go.

Delivering tangible benefits every day

"Veri-NAC is easy and intuitive to use, and it gives us everything we need in a single product. It tells us when a node is plugged into the net, it alerts us to vulnerabilities so we can solve the problem proactively, and —one of the biggest time savers—it weeds out false positives, so we can concentrate on addressing the real issues that arise," commented Stiner.

Each Lane County site on the network has its own sub-net with its own IP address schema. Now, if an untrusted device tries to plug into the network, Veri-NAC automatically locks it out, whether it's a server, router, desktop, laptop, or wireless device. Veri-NAC also identifies the exact IP address and location of the access attempt, so the IT team can tell at a glance that there's a problem, know precisely where it's occurring, and instantly zero in on the source. As a result, for a staff of 300 people, all network security is now easily handled by just three IT people.

One of the first things Stiner did with Veri-NAC was run an audit of Head Start's critical servers. He was stunned when Veri-NAC discovered that anyone could log into any server with a null login, giving them free reign to access the network resources and even steal data -– a critical hole in security that had to be plugged immediately.

Veri-NAC also uncovered vulnerabilities in the Linux platforms that, upon investigation, turned out to be flaws in the Linux server software from Red Hat. Stiner alerted Red Hat to the problem, and they corrected it and issued the fix to all Linux users.

Locking out unauthorized devices that can jeopardize network operations is vitally important, but there's more to network security for Lane County Head Start. It deals with families and young children, and as a result, it has a lot of sensitive personal data in its systems that must be protected.

"I can't say enough good things about Veri-NAC. We haven't found anything yet that Veri-NAC can't do when it comes to ensuring network security. It's a fantastic product," concluded Stiner.