Customer Case Study

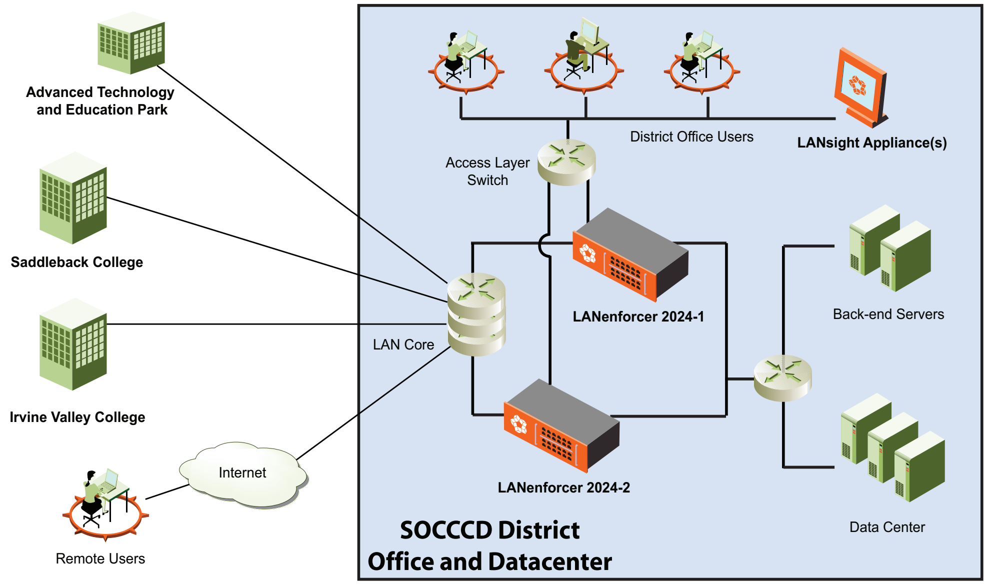
The South Orange County Community College District (SOCCCD) Selects Nevis to Monitor User Activity and Secure Critical Data and Applications

> *"We needed the (access control) solution to be as transparent as possible and Nevis has definitely delivered on this. Once we deployed Nevis, we could bring up a list and see who the active users are and, in most instances those users didn't know they were even behind Nevis, or protected by Nevis. That was a tremendous benefit for us, that the end user impact was minimal. Beyond that, we have one central location we can go to to look for anomalies in the network traffic. We can look at network traffic to see if malicious activity is occurring, either originating at the district or with the district as a target, so it's a great dashboard to look at to see the security infrastructure of the network."*
>
> — Jeff Dorsz, Telecommunications and Network Security Manager, SOCCCD

The South Orange County Community College District (SOCCCD) needed to secure sensitive data and applications, largely consisting of student's and staff's personal information, within the datacenter at their district office. The users on the district network consist of roughly 38,000 students and over 2,500 faculty and staff spread over two main campuses, as well as the district office. Access to the sensitive systems needed to be granted according to a user's role, such as "administrator". In addition, SOCCCD wanted to improve network access controls for systems connecting to the network, as well as user monitoring once the users were allowed on the network.

Jeff Dorsz, the telecommunications and network security manager at SOCCCD and the project lead, originally considered a firewall-based access control solution, but quickly realized that he needed an "identity-based" solution that could align with his role-based access policies. Managing access control lists (ACLs) or segmenting his LAN to control access was not feasible given the nature of his user base and the distributed campus network.

Internal firewalls would also not be able to enforce network access controls (NAC), nor would they provide logging and reporting of user activity like an identity-based solution would. At that point, Jeff decided to deploy Nevis LANenforcer™ and realized he could combine his NAC and access control initiatives.



Deploying Nevis at SOCCCD

SOCCCD ended up deploying two LANenforcer 2024 security appliances on parallel redundant paths between the core of the network and the servers in the datacenter. In the initial phase of the deployment, all district office users connect through an access switch which feeds traffic to one or both of the LANenforcers so that a secure, fault-tolerant network path is maintained. Remote campus users, including the bulk of the student population, are also effectively shielded from accessing the datacenter since all their traffic must go through the LANenforcers as well.

SOCCCD takes advantage of the Nevis “cloaking” feature which essentially makes the data resource invisible to unauthorized network users. This increases security over solutions that rely solely on proper access credentials to access the server, since any traffic that would scan the network or try and reach that destination is dropped within the Nevis LAN security appliance according to pre-defined role-based access policies. This effectively blocks a wide range of potential attacks, including denial of service attacks, or vulnerability scans, where the potential attacker otherwise does not need access credentials to launch the attack.

The Resulting Benefits for SOCCCD of the Nevis Deployment

- **Role-based Access Control and Policy Enforcement** — SOCCCD now has a network security solution that can enforce access control policies based on the role of the many users on the campus LAN. Other access control solutions, such as firewalls, can not make these identity-based solutions, which would require either an unmanageable mapping of identities to machine addresses, or a new policy model.
- **Transparent User Activity Monitoring** — Through the Nevis LANenforcer appliance, SOCCCD can now generate reports on compliance and activity on a user id by user id basis. It is now readily apparent what each individual is doing, without having to map machine addresses to user names. This saves time in tracing back problems to specific users and their systems, which is critical for student-owned laptops. Users are not impacted and generally do not know they are protected by Nevis.
- **Reduced User Administration Costs** — Because the access control solution is identity-aware, it is a simple process to manage users and policies through the existing user directories, predominantly Active Directory, and have that be the primary driver of creating user access policies. Since SOCCCD has automated their user creation process, policy changes are enforced automatically.
- **Single console dashboard for network-wide activity** — Nevis has also delivered a single dashboard to detect and analyze threats arising from within the district, as well as targeting the district, in addition to showing all user activity, greatly reducing time and costs to remediate threats.

About SOCCCD

The South Orange County Community College District, founded in 1967, is one of 72 community college districts in the state of California. The district's two colleges, Irvine Valley College in Irvine, and Saddleback College in Mission Viejo, CA are fully accredited and offer quality transfer courses, vocational education programs, and continuing education and cultural opportunities. The SOCCCD currently serves over 38,000 students and employs more than 2,500 faculty and staff. For more information, please visit http://www.socccd.org.

Nevis NETWORKS

Nevis Networks, Inc.
295 Bernardo Ave., Suite 100
Mountain View, CA 94043
www.nevisnetworks.com
(650) 254-2500

Nevis Networks
International HQ
Delegate House
30 Hart Street
Henley on Thames,
RG9 2AL, United Kingdom
Tel: +44 1491 635 339

Nevis Networks India
C301 Pune IT Park
Bhau Patil Marg
34 Aundh Road
Pune 411020, India
Tel: +91 98450-05047