Cold Spring Harbor Laboratory

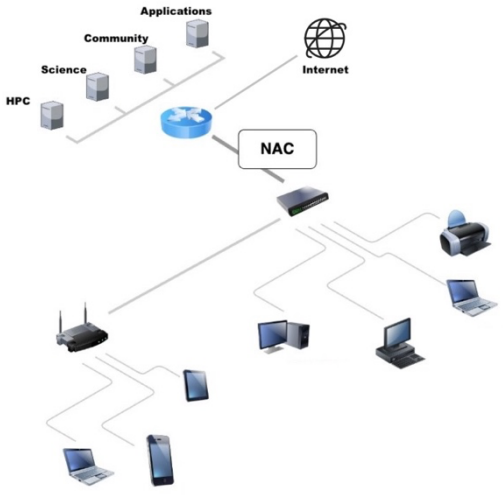
Cybersecurity Management Office

It's National Cybersecurity Awareness Month!

This year we're spotlighting a major upgrade to our network security: the deployment of a Network Access Controller. This deployment significantly strengthens our defenses against cyber threats while aligning with regulatory cybersecurity requirements. Our institution thrives on collaboration - across labs, disciplines, and even borders. But this openness also creates risk.

Scientific environments often include legacy systems that can't be patched, devices not managed by IT, and external collaborators with varying security postures and access needs. This makes CSHL a high-value target for cybercriminals and nation-state actors. And we're not alone. According to the Zscaler ThreatLabz 2024 Ransomware Report, educational institutions face mounting pressure as the fourth-most affected sector by ransomware. Between April 2023 and April 2024, educational organizations were hit by 217 ransomware attacks, marking a year-over-year increase of more than 25%. This highlights the need for proactive, layered defenses.

The Network Access Controller (NAC) will allow us to segment access based on device type and trust level, ensuring that only compliant systems can reach sensitive resources. The NAC continuously monitors posture compliance - checking for antivirus status, patch levels, and other security indicators - and integrates with our threat detection systems to identify and respond to risks in real time. If a device is compromised or fails to meet security standards, the NAC can automatically segregate it from the network providing only interet access.



For example, if someone brings in a laptop without IT installed protections, that device may be granted basic internet access but will be restricted from core systems such as HPC and shared file servers. Once the required agents are installed and the device passes posture checks, it can be reassigned to a trusted network segment by the NAC. This approach balances operational flexibility with strong, policy-driven protection, allowing the important work that we do to continue without disruption.

As cyber threats continue to evolve, we remain committed to strengthening our defenses. The NAC deployment is an important step in our broader cybersecurity strategy and a critical part of our journey toward full compliance with NIH requirements. While compliance is essential for continued funding, it's not just about checking boxes. It's about building a security posture that's resilient, adaptive, and strong. By aligning our infrastructure with best practices and regulatory expectations, we're not only protecting our community, networks, and data - we're empowering our research to thrive in a secure, trusted environment.

If you have any questions or concerns, please reach out to cybersecurity@cshl.edu. Thank you!