SETTING UP A HYBRID OFFICE: HOW TO SECURE YOUR NETWORK

It may seem like just yesterday that IT teams worldwide scrambled to set up secure and efficient remote work environments. Now, a little over a year later, we are seeing the beginnings of a return to office work. For some organizations, this may be a return to normalcy in their IT operations, but for others, recent changes to workflow and infrastructure may make for yet another challenging project in terms of managing users and devices. With that in mind, here are some quick tips to ease the transition back to a stable baseline in your network environments.

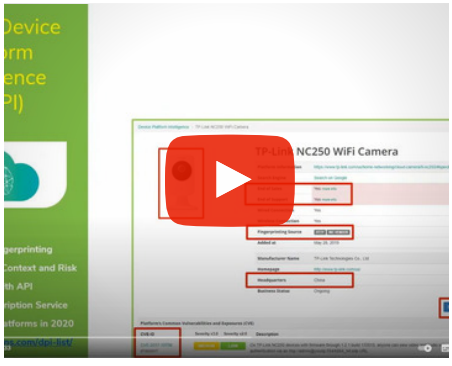
BE MINDFUL OF CHANGING ACCESS METHODS

Many organizations have expanded their remote access options to accommodate + their remote workforces. This often includes a VPN+RADIUS setup. If your organization has configured their infrastructure in such a way, it would be efficient to integrate your on-premise switches and access points into the same network access scheme.

In cases where port-based access control is not used or not supported in your on-premise environment, or if you want to exercise additional control over connected devices, you should review your criteria for determining what devices should be on the network and what their privilege levels should be.

The Genians Network sensor can leverage powerful Device Platform intelligence (Included with Genian NAC or available as a standalone service) and arp enforcement technology to microsegment your networks in real-time based on changing contextual information about the platforms that are detected, which users have authenticated, time of day, and many more factors

Genian NAC RADIUS Authorization Policies



Genian Device Platform Intelligence GDPI Overview

PLAN YOUR ONBOARDING & ENFORCEMENT IN PHASES

As you begin to accept more devices onto on-premise networks, consider using a gradual enforcement approach.

For example, you may start allowing only some devices full network permissions, and allowing most other devices limited access. In most environments, a least privilege approach is best, as it is safer, and it is easier to locate and resolve a false-positive threat, than it is to deal with an undetected threat.

Users whose devices have restricted network access should be allowed the necessary network permissions to contact your IT administrators and request the level of privilege needed, but no more.
With this in mind, be very mindful of which conditions you use to allow broader network access. Using a combination of authentication, MAC addressing, IP addressing and other factors can be a simple way to determine which devices should be allowed to access the network with fewer restrictions.

TAKE NOTE OF CHANGING ATTACK SURFACES

Another important consideration for devices with increased network access is stricter mandatory security software requirements, for things such as antivirus, or making sure that insecure applications are not installed. This can be accomplished with the Genian NAC agent. Since remote users typically log in via a VPN or connect directly to cloud resources, the main threat they face is data leaks including credential loss.
In such an environment, one compromised machine is typically isolated by a firewall filtering traffic in and out of the network, and general account security measures. In an on-premise environment, employee devices are clustered together within a network, further increasing risk, and negating firewall controls.

Using Genian NAC, devices with software related risks can be detected and isolated In the coming months, there will be new devices, new challenges, and new risks.

Despite the abrupt change, the ideal strategy boils back down to basic points.

- Make efficient use of your infrastructure and solutions
- Leverage multiple forms of authentication and identification for security and management
- Aim to implement least-privilege
- Plan your project in phases
- Tailor your approach to the specific environment