How NAC Meets the Basic CIS Controls

Introduction

With the sheer volume of products on the market vying for your organization's IT budget, how can you be sure your investments of time, money and resources are well spent on the right technology for your needs?

A logical starting point, Cybersecurity is paramount to the defense of your organization's data. The truth is, there is no single product that can do it all. The need to adopt a *Defense in Depth* approach has been illustrated time and again with each new report of another large-scale data breach. But where do you start?

The Center for Internet Security's (CIS) **Critical Security Controls for Effective Cyber Defense** were developed as a recommended set of 20 specific, prioritized actions that an organization can take to mitigate today's most pervasive attacks. Enforced and used by the U.S. Government, the European Telecommunications Standards Institute, and diverse organizations globally, the CIS Controls should be your first stop on a cybersecurity journey.

The most crucial "must-do's" to eliminate vulnerability in your organization are in the 6 Basic CIS Controls, all of which can be addressed by implementing a Network Access Control solution.

NAC Mapping to Basic CIS Controls

Focusing your cybersecurity efforts on these top controls helps your organization address the largest vulnerabilities facing your network with the least amount of effort; the biggest 'bang for your buck' as far as network security spend goes.

CIS Control 1: Inventory and Control of Hardware Assets

Actively manage (inventory, track and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

NAC Coverage: A NAC solution sits in-line on the network, giving an administrator comprehensive visibility on all connected hardware devices. Policy-based access is granted to authorized devices used by authenticated users, and any devices found to be unauthorized is prevented from gaining access to critical network resources and data.

CIS Control 2: Inventory and Control of Software Assets

Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized software is found and prevented from installation or execution.

NAC Coverage: An optional feature, NAC solutions assess an endpoint to determine software that is installed and running on that endpoint. Based on an organization's security compliance policy, the NAC can take action on that device, either by warning the end user that the device is in violation of the Acceptable Use Policy, or place the endpoint into a quarantine VLAN and force the end user to self-remediate by ceasing use of unauthorized software.

CIS Control 3: Continuous Vulnerability Management

Continuously acquire, assess, and act on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for hackers.

NAC Coverage: On its own or integrated with a 3rd party security tool like a Next-Generation Firewall, SIEM, IDS/IPS or Advanced Threat Detection tool, a NAC can continuously assess endpoint devices on the network to identify vulnerabilities and act on those devices. When integrated with a 3rd party product, the NAC can receive threat alerts and act by quarantining a device flagged as posing a risk to the network.

CIS Control 4: Controlled Use of Administrative Privileges

The processes and tools used to track/control/prevent/correct the use, assignment and configuration of administrative privileges on computers, networks and applications.

NAC Coverage: Integration of the context NAC naturally has, that other portions of your security ecosystem lack, can be published to other network devices to more granularly control access based on a user's role in your Identity Access Management system. For example, leveraging a Next-Generation Firewall (NGFW) to contextually block users from the management interfaces of devices.

CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

NAC Coverage: Based on the policies established for the various device types, NAC can continuously monitor their security posture with respect to those policies and alert the user and/or IT of the non-compliance. Moreover, based on the policy for that device, the device can be immediately removed from the network and optionally quarantined while the user brings it in line with the established policies.

CIS Control 6: Maintenance, Monitoring and Analysis of Audit Logs

Collect, manage and analyze audit logs of events that could help detect, understand, or recover from an attack.

NAC Coverage: Supporting documentation and reports on various metrics related to network authentication and policy adherence can be produced by a NAC solution to aid an organization in meeting regulatory compliance requirements. These reports can be used to identify both known and unknown users as they attempt to gain access to the network and are kept as part of an audit log to help organizations detect potential vulnerability points that could leave them open to an attack.

NAC Value-Adds for Cybersecurity Controls

Implementing a NAC solution as part of your cybersecurity best practices can have the following benefits to your organization:

- **Greater Device Visibility** - By automatically recognizing when devices attempt to connect to wired, wireless or VPN networks, a NAC can provide device type profiling, integration with directory services to facilitate authentication, guest self-enrollment options and real-time contextual intelligence reporting -- all with the goal of letting an administrator see across the expanse of the network, easily and automatically.
- **Granular Control** - Crafting policy-based access to the critical resources on the network and automated enforcement of compliance with an organization's Acceptable Use Policies in real-time, continuously as a device traverses the network - all without the involvement of a help desk staff member.
- **Network Security Orchestration** - Automate policy enforcement based upon the risk levels reported by 3rd party security solutions like Next-Generation Firewalls, SIEM providers and IDS/IPS systems, and publish real-time contextual intelligence information to these 3rd party security solutions that they can't glean on their own, by virtue of where they sit on the network.

- **BYOD, COPE and IoT Management** - Track, assess and enforce compliance of devices in multiple user communities on the network outside of traditionally domain-managed devices, including employee-owned "Bring-Your-Own-Device", "Corporately-Owned, Personally-Enabled" and browserless "Internet of Things" devices
- **Helps Address Regulatory Compliance** - The foundation of meeting most regulatory compliance mandates is accounting for who is on the network, and reporting on what levels of access those users have. Complying with cross-industry standards like PCI-DSS, HIPAA and SOX by way of audit trails, authentication logs and historical reporting is something with which a centrally-managed NAC can assist.

Conclusion

Network Access Control is not just about controlling access. The value it brings to an organization's cybersecurity posture transcends the simplicity that the name implies. Mobility and the advent of the Internet of Things has brought with its tremendous productivity but with it, more security risk than ever. A set of prioritized activities that provide real impact on an organization's overall security posture is the goal of the CIS Controls, with the Basic Controls being the most easily undertaken with the largest impact. The foundation of these Basic controls is the identification of what's on the network, security of the endpoints connected, granular control of access privileges and comprehensive reporting and auditing of authentications. By deploying a Network Access Control solution, an organization can address these Basic Controls and help mitigate their cybersecurity risk.