aruba
a Hewlett Packard Enterprise company

SOLUTION OVERVIEW

SECURITY CONSIDERATIONS FOR NEXT GENERATION NETWORK ACCESS AND ENDPOINT COMPLIANCE

The dangers of endpoints connecting to the network before scanning for device health

INTRODUCTION

Endpoint compliance assessments are critical for today's mobile workforce environment. Employees, contractors, and guests treat IT-issued laptops as if they own them. Meanwhile, bring your own device (BYOD) has become popular due to convenience, cost savings and IT offload. Unfortunately, user behavior and connecting these devices to enterprise networks is a growing concern that adds potential threats.

Legacy network access control (NAC) required IT to install supplicants and agents on IT-issued computers to ensure the latest A/V software was updated and scanned. Next generation endpoint compliance allows for the automation of configuring devices, with little IT hassle, with improved policy creation and enforcement. Endpoint type will include laptops and desktops, smart phones, and tablets.

In this paper, we'll discuss how and where new generation endpoint compliance should be enforced as well as additional considerations that are critical for ensuring a secure network.

NAC RE-INVENTED

Early issues with deploying NAC are a thing of the past — in fact, there's no longer a need to distribute supplicants. Devices come with usable supplicants and the distribution of agents is automated today.

Next generation endpoint compliance is "IT lite" because agents can be automatically pushed to the client. Today's NAC solutions are typically used to distribute agents to computers and enterprise mobile management (EMM) solutions are used for distributing agents to smart phones and tablets. In both scenarios, the policy management component within a NAC solution will be used to enforce network access privileges. The goal is to perform the assessment before full access privileges are granted.

This ease of deployment has lifted a significant burden off of IT that otherwise would have hampered implementation. More importantly, today there are many features that are available within a NAC solution that solve the security implications of a mobile workforce.

BASIC FEATURES OF AN ENDPOINT COMPLIANCE SOLUTION

Today, endpoint compliance means much more than just checking for traditional anti-virus and firewall status. IT can now require and control the use of many more variables that have been implicated in breaches. This can include controlling USB ports, P2P file share blocking, spyware updates, patch/hotfix management, and more.

Additionally, today's NAC solutions can be configured so that features run in the background. Real-time assessments can trigger auto-remediation to change the status of an endpoint that makes it non-compliant. When auto-remediation is not an option, the NAC solution can also communicate instructions to the end user on how to resolve non-compliance issues via SMS, email, or a service desk call.

Tying these features together with the AAA capabilities of a policy solution allows for much more granular and robust policies that can leverage the detailed user and device context that's available today. Device fingerprinting, the status of a certificate or credentials and user location data can now be collected and used to determine if a device should be connected to a network.

This simplifies IT involvement and improves the end user experience as self-management of their devices makes it easier to comply with changing policy requirements.

DIFFERENCES BETWEEN NAC SOLUTIONS

Not all NAC solutions are equal. Most importantly, when approaching access control with a security mindset, when device health checks occur is often the most overlooked gap.

From a security standpoint, the strength of your defenses is inversely proportional to end user and/or IT convenience. Sometimes a "good enough" approach is fine – for example, some websites do not require lengthy or complicated passwords, but more important accounts, such as brokerage accounts, may require strong passwords and two-factor authentication. However, in the case of endpoint compliance and health checks in the mobile world, slightly more involved challenges are needed considering the implications of a large breach, data loss, or infected network.

The convenience first, security second school of thought for some vendors is to let the device onto the network before doing a policy or health check. And instead of using 802.1X, RADIUS and other authentication and enforcement protocols, they attempt to scan devices after they've been granted a connection to the network. This way, elements of the device can be scanned faster than if an agent were issued to a device and securely scanned and authenticated first.

Although the time increment may be small before detecting a threat in this model, it can be just enough time to expose your network to malicious code or data loss than if enforcing an assessment and authorization before the device acquires an IP address. In other words, merely allowing a device to acquire an IP address first and then scan packets, still allows for enough time to compromise your network.

Furthermore, the speed with which a device can be scanned before acquiring an IP address is negated by the intrusive performance hit a device will take while the end user is working on an application. The size of an organization is another consideration. Devices farther away from where the NAC solution sits, will have access to resources longer than may be desired.

Trusting the device before enforcing compliance policies is akin to locking your front door when you leave for work in the morning — after leaving the door open overnight. You are leaving yourself vulnerable at the most critical and vulnerable time. The same is true for endpoint control. It makes sense to enforce a policy before allowing untrusted devices onto the network. Just because devices are known does not mean that they should be trusted.

IMPLICATIONS OF THE PRE-ENFORCEMENT ACCESS MODEL

Stories about breaches and corporate data loss are increasingly all over the news feeds. Some of the largest companies in the world have had to disclose devastating breaches because someone brought a device onto the network that was not IT issued and logged into the network without a health check. Once malicious code is injected into the network in the fraction of a second that the user logs in, there is virtually no way to stop the propagation of the infection throughout the network – the damage has already been done. And now with laws requiring public disclosure and notification of breaches, the costs are staggering – not to mention the potentially personal legal implications for C-level executives.

PRE-HEALTH CHECK VS. POST-HEALTH CHECK

Although accessing the network after checking for device health policy is critical from a security standpoint, both pre and post assessment and enforcement is ideal for strong security. Say you have a pre-enforcement solution and policy in place and a remote employee wants to use their personal laptop on the network. They are required to download an agent which then scans for a policy. If the device is clean, they are allowed onto the network. If there is an anti-virus program that is outdated, it can be auto-remediated.

But, what if a user does something after they are on the network? Say they click on a malicious link that circumvents their current anti-virus application by turning off their firewall. A persistent agent will continue to check the device and will either auto-remediate or block the user from the network if a firewall is a component of the IT policy. If there was no persistent agent, there would be no way to auto-remediate or flag and block any changes to the device post device health check.

ARUBA CLEARPASS — A SECURITY CENTRIC ENDPOINT COMPLIANCE SOLUTION

Aruba ClearPass OnGuard, a component of the Aruba ClearPass Policy Management Platform can be used to perform device assessments on any computer or laptop connecting to the network. The Policy Manager is also capable of pulling attributes from an EMM system to ensure that only compliant smartphones and tablets are connected to Wi-Fi and wired networks.

With the use of a persistent agent, IT can check for anti-virus, spyware, firewalls, hot fixes and more in real time before granting authorization privileges onto the network. If there is a service or requirement that can't be auto-remediated, for example, if disk encryption must be enabled, the user can be notified that they can't access the network and must restore their encryption before they will be connected to the network.

Not only will ClearPass ensure non-IT issued laptops and computers are compliant before they are allowed network access, but they can do so in an "IT lite" fashion on both the wired and wireless network before an IP address is issued.

A lightweight dissolvable web based agent is also available for users segmented on a less critical segment of the network, for instance, a guest network. Personal devices do not allow agents to be permanently installed in most cases and would connect through a captive portal that uses a native dissolvable agent. The dissolvable agent is completely removed from the device once the browser is closed.

More importantly, users and devices are authenticated and authorized for access before being given network access. Learn more about ClearPass OnGuard.

aruba
a Hewlett Packard Enterprise company

1344 CROSSMAN AVE | SUNNYVALE, CA 94089
1.866.55.ARUBA | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com