Pulse Secure®

Demystifying NAC 3.0

Network Visibility, Access Compliance and Threat Response

Intro

Network Access Control (NAC) solutions have come of age, driven by the need for dynamic network visibility and automated threat reduction, wide-scale use of mobile device for Bring-Your-Own Device (BYOD) and guest networking, and the rise of the Internet of Things (IoT). IT organizations are rapidly implementing NAC as an integral piece of their business compliance measures and overall security strategy. However, confusion continues to surround the best practices on why, where, and how to best apply a next-generation NAC solution.

The purpose of this document is to provide an overview of NAC technology, the dynamics that drive solution innovation, and best practices for NAC implementation.

NAC Defined

Network Access Control solutions are designed to control user and device access to the enterprise network based on corporate security access policies. NAC solutions discover and profile network endpoints, control access to corporate and guest network resources and enforce security compliance for wired or wireless, endpoints including BYO, and IoT devices.

State of the Art

NAC technologies have evolved from solutions that simply focused on authentication and authorization of managed endpoints to now delivering an array of endpoint discovery, classification, assessment, remediation and monitoring services such as identifying and applying policy to BYOD, guest-access networks, and IoT devices. Adoption by organizations continues to expand and the technology is understood, accepted, and deployed globally.

NAC solutions are installed across all industry verticals. Financial services and health care have the highest usage rates, with installations also present in government, education, IT, telecom, energy and manufacturing companies. Adoption has fueled a $1 billion-dollar market in 2017, and the analyst firm Quadrant Knowledge predicts growth will accelerate five times by 2023.

Technology Drivers

Several major contributing factors are spurring adoption and expansion of NAC solutions:

1. Regulatory and Compliance.
   Compliance requirements including FISMA, PCI-DSS, NERC, ISO/IEC 27001 and GDPR continue to drive demands for greater network visibility and threat reduction. A key component of this is personal and corporate data privacy. Security noncompliance results in higher risk of information theft, heavy financial penalties, and loss of trust and revenue due to negative publicity. Global regulations continue to grow in complexity and drive IT teams to build smarter and automated security infrastructure that ensures employees and contractors conform to security policies and aids in avoiding costly regulatory violations.

2. Mobility and Bring Your Own Device (BYOD)
   Security of BYOD and WYOD (Wear Your Own Device) devices that access corporate resources and cloud applications are also a catalyst for NAC solutions. Mobile device business use-cases and WiFi-enabled technologies are driving companies to new levels of worker productivity. Management and access-control of a variety of mobile devices, each with different versions of software and potential security vulnerabilities, further stimulates risk. NAC centralizes management and secures mobile devices through visibility and enablement of policies across a diverse landscape that includes BYOD, guest and contractor access, and shared corporate-owned devices.

3. Explosion of Smart IoT devices
   IoT device usage has significantly increased in both the corporate and industrial operations areas. IoT technology has expanded from simple entry-order and tracking functionalities to a complex inter-connected network utilizing data analytics to make predictive business decisions. Widespread IoT use has increased exposure to vulnerabilities and expanded the attack surface making NAC an essential tool to help harness the IoT for business use.

NAC Adoption and Growth

Market Drivers

Global Regulations: FISMA, PCI-DSS, NERC, ISO/IEC 27001, and the GDPR

NAC solutions enforce organizational security policies

Need to Secure Mobility, BYOD, and WYOD

Growing awareness of NAC benefits in improving organization security measures

IoT and IIoT-enabled devices increase exposure to attack

NAC Evolution

NAC 1.0

The first concept of NAC originated in the early 2000's as an authentication onboarding technology of corporate owned devices. Organizations recognized a security requirement to identify and authorize these endpoints prior to connecting to the network and to help fend off virus attacks. This became known as NAC 1.0, or the first generation of NAC products. Early adoption rates suffered, as these solutions were difficult to deploy, often operationally disruptive and low on investment return to IT management.

NAC 2.0

In 2008, NAC 2.0 introduced visibility and access-control features that aided management in planning and implementing security policy. As a result, large organizations began to uncover unmanaged endpoints on the network and began to see the value-proposition of NAC.

By 2012, a new wave of IT technologies emerged. The era of enterprise mobility, BYOD, IoT, and wireless corporate and guest-access networks began, as such, organizations adopted the mindset of requiring broader compliance requirements. As adoption grew, so did the exposure to a new generation of cyberattacks. Typified by browser attacks and email phishing, these new network attacks targeted users with the end goal of compromising endpoints and installing stealthy malware for greater hacker access. A recent report states ransomware damage costs exceeded $5 billion in 2017, up more than 15x from 2015. It is predicted that ransomware will attack a business every 14 seconds by the end of 2019[1].

> "It is predicted that ransomware will attack a business every 14 seconds by the end of 2019"

NAC 2.0's core capabilities of network endpoint visibility, access control, and endpoint compliance with enforcement provided new measures to combat modern network attacks. Guest access security to the corporate network, secure management of removable storage, malware prevention and endpoint compliance are valuable examples of this generation's capabilities.

NAC 3.0

Personal IoT use in corporate environments and mechanical use in industrial operations are disrupting conventional network security strategies. IoT technologies connect workforce services and invigorate operational functions such as tracking customer behavior and delivering inventory alerts as part of an entry-order system.

IoT is further empowering Shadow IT. The majority of IoT devices are devoid of human interaction and employ operating systems and applications that are not easily maintained by IT. The sheer numbers, diversity, and widespread geographic dispersion of these devices widens exposure to new vectors of cyberattack.

Expansion of NAC 3.0 counters the new risk of IoT with advanced Security Automation and Orchestration (SAO) capabilities. SOA automates the access to and management of IoT requirements, such as self-service or contractor-based installation, updating, and remediation. NAC 3.0 further automates threat response by sharing contextual information with other network infrastructure. Through integrations with security vendors, organizations can leverage their investments and improve the capacity of security teams and minimize time to mitigate threats.

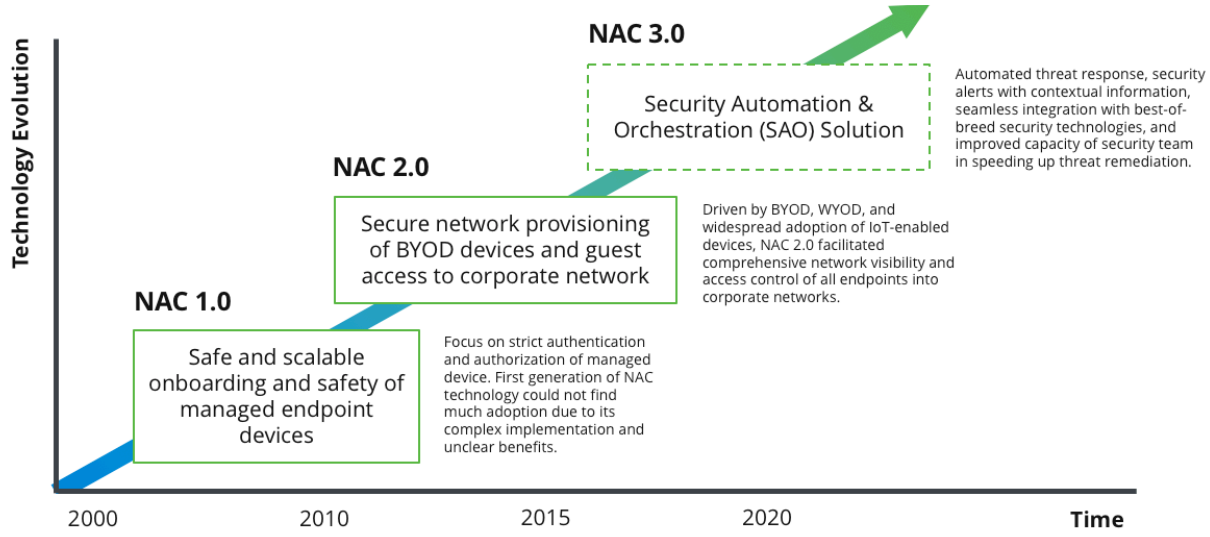


Figure 1: Evolution of Network Access Control (NAC)

[1]Morgan, Steve. 2017 Cybercrime Report, PDF file, 2017, https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf

Core NAC Capabilities

Visibility

Visibility is the comprehensive discovery of network connected endpoints, both managed and unmanaged. Network profiling enables discovery and classification of endpoints while also tracking corporate and guest user access to the wired and wireless network. Visibility delivers wide amounts of contextual security data, including user role, device type, device configuration, location, time, date, access request, application or network resource used and network activity.

> "97% of organizations have experienced a breach; of those breached, the breach went undetected for an average of 134 days"
>
> — Addressing the Threat Within: Rethinking Network Security Deployment, 2016

Onboarding

Automated onboarding allows for self-registration of BYOD and IoT devices. Through security policy, the correct level of access is allowed or denied to corporate resources. As part of the onboarding process, NAC performs device risk-assessment analysis and quarantines suspect devices. Auto-provisioning frees IT from onboarding task and helps scale BYOD and IoT deployments.

Integrations

Because most large companies have multiple versions of security products, interoperability is a key NAC 3.0 capability. When combined with third-party network security, vulnerability and risk assessment and systems management solutions, NAC contextual data expands the effectiveness of endpoint intelligence and network enforcement.

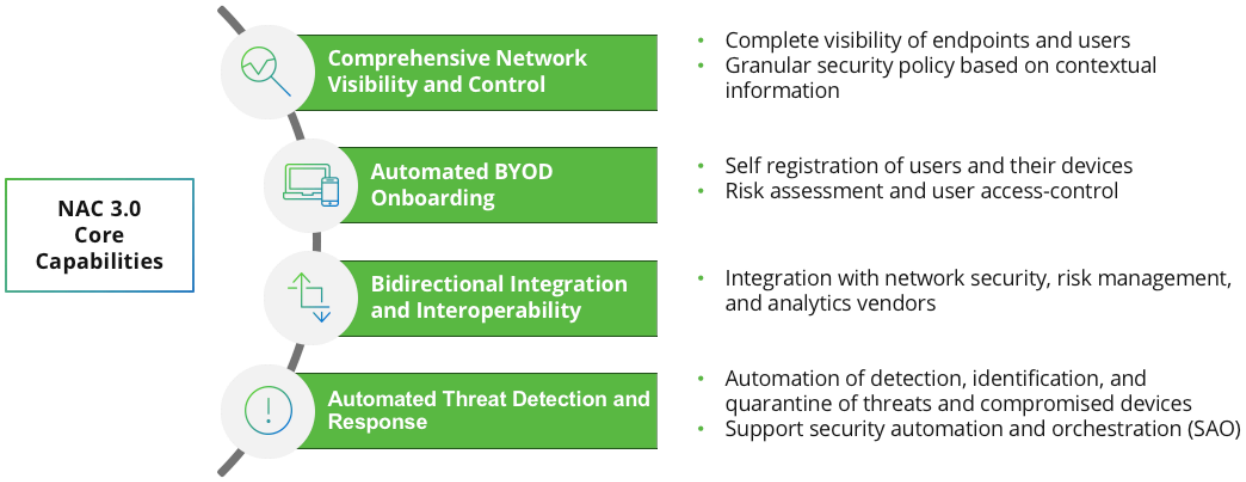
Bi-directional alert-based or API integration functions further enhance NAC 3.0 benefits and can be used to fortify the effectiveness of zero-trust networks.

Threat Detection and Response

The threat of breaches remaining undetected for extended periods is growing. According to a Gigamon report, 97% of organizations have experienced a breach; of those breached, the breach went undetected for an average of 134[2] days. NAC automatically detects the presence of IoT and BYOD devices and reduces the complexity of handling thousands of security alerts daily. Without automation, security incidents may be lost in the daily deluge of alerts and overlooked. Automated threat detection and response addresses this issue and is a key trend for 2018 and NAC 3.0.

[2]Addressing the Threat Within: Rethinking Network Security Deployment, PDF file, 2016, https://www.gigamon.com/content/dam/resource-library/english/white-paper/wp-rethinking-network-security-deployment.pdf

NAC Core Capabilities



- NAC technology capabilities vary between different vendors' offerings. Also, requirements of NAC features vary between SMB, large, and enterprise organizations.
- User organizations should conduct a detailed technology evaluation with the analysis of specific features required as per their own organization-specific and industry-specific requirements.

Implementation

Deploying a NAC platform requires careful thought and planning. NAC solutions provide full visibility of endpoints and enforce security policies. Dissimilar to common security products—Anti-Malware, Next-Generation Firewall and VPN—NAC can be deployed to satisfy a variety of different use cases.

Phases

IT teams leverage NAC to solve a variety of access challenges for the corporate network, often in a phased manner. With a plethora of IP and Wi-Fi enabled technologies capable of connecting to the network, IT organizations view endpoint visibility of managed, unmanaged and IoT devices as table stakes for a NAC strategy.

Next, NAC addresses change within the workforce, providing contractors and partners with guest access and enabling BYOD for workers. NAC technology empowers automated management of network use by guests and contractors while reducing threats from unauthorized users and compromised devices.

With a comprehensive and dynamic view of network devices, organizations can phase in granular policy enforcement to secure devices (managed and unmanaged including IoT devices) and users on the network, ensuring compliance with industry regulations and corporate policies. In this phase, enterprises can leverage existing security infrastructure investments for enhanced identity and device context and to enable automated mitigation of incidents.

Visibility

Consider using NAC visibility features for continuous endpoint profiling. Profiling can be implemented with or without an agent. A variety of polling methods can be used to discover devices include DHCP, SNMP, NMAP, WMI, SSH, EMM, and HTTP session details. In addition, profilers can automatically classify devices, profile endpoints assigned with static IP addresses, and actively scan open ports to detect MAC spoofing.

Enforcement

Upon achieving full visibility, use NAC for granular policy enforcement to secure devices (managed and unmanaged including IoT devices) and users on the network. This will ensure compliance with industry regulations and corporate policies. Customers can leverage existing security infrastructure investments to achieve enhanced identity and device context or to enable automated mitigation.

NAC solutions have a broad range of built-in and extensible policy templates. Categories to consider when building policies include:

- User roles
- Quarantine options
- Acceptable endpoint devices
- Time-of-Day
- Network segmentation

Integrations

Consider integrating NAC with third-party security solutions via API, Syslog, and IF-MAP protocol. Implement a NAC solution with an alert-based or API-based framework that can work with popular firewalls, SIEM, Enterprise Mobility Management (EMM) and other systems to share identity, network and configuration contextual information. IF-MAP protocol can be useful to interoperate with existing IF-MAP supported infrastructure.

Other Deployment Considerations

There are a variety of other deployment considerations for NAC 3.0 solutions.

Understand the network and supporting network infrastructure. While NAC solutions typically identify upwards to 30 percent of unmanned and unknown network endpoints, proper NAC deployment requires a thorough understanding of network locations, segments and interconnects and existing network and endpoint security systems of which NAC will interoperate with.

Over-communicate on areas concerning the roll-out of NAC, as the introduction of new network access policies, notification and enforcement controls should and will impact respective IT divisions and user constituents. Multiple avenues of communication (email, intranet site, FAQ, etc.), interaction with change management, open

dialogue tech support, interaction with business and application owners that may be affected, and discussions with executive management are just a few communications vital to success.

Pre-connect NAC takes a "guilty until proven innocent" approach by quarantining devices on a separate VLAN until they are deemed compliant and authorized. Post-connect NAC takes an opposite approach by granting network access while applying policy to take an action if a device is or becomes non-compliant or unauthorized.

Before considering pre-connect NAC, it is recommended to review key use-cases and security policies to gauge potential user and device impact, agent management concerns, and infrastructure support requirements. A hybrid combination of both pre- and post-connect NAC deployment should be considered to cover any outage scenario.

Use a phased approach to implement NAC enforcement. It is suggested to begin with notification of policy violations prior to implementing enforcement. This method serves to change end user behavior. The introduction of new NAC policies with strong enforcement can impact user experience.

Endpoint visibility allows IT staff to understand the ramifications of policy changes on end-users. Guest management typically requires strong enforcement. Areas of the network exist which require strong enforcement, such as notifying on new or unknown devices in PCI-DSS designated computing zones and wireless guest management.

Defining rollback processes, key contact personnel, and outage communication protocols should be on the rollback plan in case the rollout causes an interruption to business. A phased approach can be by region, business case, and interoperability.

Avoid the temptation to immediately integrate multiple products with NAC. The core integrations NAC deployments are firewall, SIEM and mobility management. Integrating with third-party security vendors adds security contextual awareness and strengthens security posture and time to remediation. Integrate slowly, as a larger amount than the IT organization can readily support. The path to integration can be difficult and require in-depth knowledge of API and product features.

Documentation is essential for both installation and support of any NAC rollout. Success criteria should be clearly established at specific steps of the process, as well as when the installation is completed. Project next steps, value for users, customers, or the business, third-party integrations, network architecture, security ramifications, support personnel and contact information, and possible business impact scenarios are all elements recommended for documentation.

Once initially deployed and fine-tuned, consider an open-ended NAC extension plan that support last-minute developments throughout the course of business. Although it is prudent to assign project tasks, develop date milestones, and keep project task owners accountable, reality dictates business requirements will always take precedence over all IT projects.

Pulse Secure: Next Generation NAC

Pulse Policy Secure (PPS)

Pulse Policy Secure is a Network Access Control solution that provides 360-degree network visibility and security enforcement for managed and unmanaged endpoints, BYOD, and mobile endpoints. Pulse Policy Secure can be flexibly deployed and scaled using multi-purpose physical (PSA series) or virtual (VMware, Hyper-V & KVM) appliances. The solution consists of three primary elements: Pulse Secure Profiler, Policy Secure and the Pulse Client.

Pulse Secure Profiler dynamically identifies and enables automatic and custom classification of both managed and unmanaged endpoint devices, to provide operational visibility, reporting and policy-based controlled access to networks and resources based on the user, device, applications and other attributes.

Policy Secure is a context-aware policy engine that applies granular policies for reporting and enforcement based on user, role, device, location, time, network, and application. The solution provides automated, self-service onboarding of laptops, smartphones, and tablets independent of user location or device ownership.

Pulse Client includes Host Checker functionality enabling the activation of predefined or custom policies to scan devices attempting to connect to network resources. Host Checker continually monitors endpoint security compliance through the Pulse Client (agent or agentless) and optionally from third-party EMM solutions.

Core PPS Features

802.1x port security is a key method for NAC layer two (L2) enforcement and is predominantly used by security-conscious customers in enterprise and government networks because it provides a trusted approach for both pre-connect and post-connect access control. A proven, high-performance RADIUS server is embedded within Policy Secure, and enables rapid deployment at a lower cost.

Figure 2: Pulse Secure delivers complete access control.

Policy Secure uses a combined solution of 802.1x and NAC to deliver additional visibility not available using 802.1x alone, including device type, wireless SSID, physical location, and time of access. Policy Secure uses this information to maximize security compliance and network resource access on endpoints. Policy Secure also features layer three (L3) enhanced contextual security and control through integrations with next-generation firewalls for application and IoT security.

For scenarios where 802.1x supplicant client downloads are not feasible, Pulse Policy Secure supports a clientless mode using SNMP (Simple Network Management Protocol) for device visibility and policy enforcement. Clientless endpoint visibility is achieved via MAC address discovery via SNMP traps and DHCP fingerprinting. A client-based and clientless hybrid NAC deployment can be used for complete endpoint visibility and enforcement.

Core PPS Features

A Secure Access solution benefits organization with boosts to worker productivity and enabling user access to resources from any location from any device type. At the same time, the solution must deliver visibility and enforcement to secure the network from unauthorized access, malware, and other cyber threats.

Pulse Secure provides an access security solution that couples both remote and local connectivity with NAC visibility and enforcement. Customers can import existing policy configurations from Pulse Connect Secure (VPN) to Pulse Policy Secure (NAC) for quick deployment, consistent security policies, and simplified administration.

A unified Pulse Client makes it simple for users to access applications and data remotely via VPN or locally via the Wi-Fi network. This is attractive for customers using the Pulse Connect Secure VPN a simple method to add NAC capabilities. When deployed with Pulse One Centralized management, the solution can scale to 20M endpoints.

The user experience is enhanced by seamless roaming between remote and local access. Pulse Policy Secure enables the federation—or sharing— of user session data with Pulse Connect Secure (SSL VPN), transitioning remote access user sessions to LAN user sessions at login, or alternatively local LAN user sessions into remote access sessions. The federation of LAN access and remote access session data is a vital part of the context awareness and session migration capabilities of Pulse Secure. This enables a remote access user connected via SSL VPN to Pulse Policy Secure to be granted access to the LAN through the same or different Pulse Policy Secure instances, without re-authentication. No re-authentication is required, enabling "follow-me" policies regardless of the user's device or worldwide location.

Summary

Choosing to implement a next-generation NAC solution dramatically improves an organization's network security posture. Comprehensive visibility of managed, unmanaged and unknown endpoints teamed with policy-based enforcement of device accessibility to the network, ensure appropriate user and device network resource access while enabling guest and IOT device risk management. By effectively quarantining untrusted parties, suspect endpoints who fail security compliancy checks, or IOT devices into specific network segments, or by blocking their access altogether, the risk of an intentional or accidental introduction of malware, network breach, or sensitive data exfiltration can be reduced.

Keep in mind that implementing NAC, like many other IT initiatives, requires adequate policy and deployment planning and support from management. It also represents an ongoing investment in licenses, training, alert monitoring, and support of the NAC system. Many IT practitioners consider the main benefits of NAC—such as greater control over BYOD and IoT, endpoint visibility, granular access to network shares, the means to segmented zero-trust networks, and added protection against malware and network attacks—is worth the investment.

Lastly, NAC boosts your security posture and optimizes resource utilization by working harmoniously with existing IT and security systems. Integrations with existing firewall, SIEM and EMM security solutions enable greater contextual intelligence and the potential for automated network threat response value above core NAC solution capabilities.

For more information about Pulse Secure Access solutions including Next-Gen NAC, please visit us at https://www.pulsesecure.net.