Pulse Secure®

Secure Access in a Zero Trust World

Demystifying Zero Trust NAC

WHITE PAPER

www.pulsesecure.net

Table of Contents

Secure Access in a Zero Trust World 3

Zero Trust NAC Drivers 3

Influx of Endpoints 3

Regulations and Compliance 3

Mobility and Cloud Initiatives 3

Shortage of Skilled Security Professionals 4

Evolution to Zero Trust NAC 4

Core NAC Capabilities 5

Visibility 5

Onboarding 5

Security Automation and Orchestration 5

Implementation 6

Phases 6

Visibility 6

Enforcement 7

Integrations 7

802.1X for True Zero Trust 7

Agent or Agentless 7

Other Deployment Considerations 8

Pulse Policy Secure: Zero Trust NAC 8

Conclusion 9

Secure Access in a Zero Trust World

The influx of BYOD and IoT endpoints, combined with the transformation to hybrid IT and increased mobility, have complicated the task for security professionals to limit the risk of compromised endpoints.

Modern enterprises require secure access solutions based on a Zero Trust model of continuous verification and authorization. Network Access Control (NAC) is an integral piece of Zero Trust access security. Zero Trust NAC ensures that only authenticated users and compliant devices can connect to the network. Organizations benefit from automatically enforcing their endpoint security compliance policies, which limits overall security risk, reduces the burden of security auditing and enables the limited security staff to focus on strategic projects.

However, confusion continues to surround the best practices on why, where, and how to best apply a Zero Trust NAC solution. This White Paper provides an overview of Zero Trust NAC technology, the dynamics that drive solution innovation, and best practices for NAC implementation.

Zero Trust NAC Drivers

Influx of Endpoints

The Internet of Things (IoT) is exploding and organizations want to increase efficiency by merging Industrial IoT devices (IIoT) in the Operational Technology (OT) environment, with the IT realm. OT environments typically operate in strict isolation. Extending connectivity for such devices, reduces downtime because administrators don't have to go on-site anymore for maintenance and troubleshooting. However, IoT devices are inherently insecure, creating a significant risk of enabling access for an attacker deeper into the network.

Meanwhile, BYOD is a de-facto standard. Workers expect to be able to perform their duties using the tools of their choice. All these trends result in a huge variety of endpoints, each with varying Operating Systems and supporting apps. Enterprises looking to enable secure access for all these endpoints, need to ensure they are validated, profiled, controlled and monitored to minimize risk.

Regulations and Compliance

Compliance requirements including FISMA, PCI-DSS, NERC, ISO/IEC 27001 and GDPR and CCPA 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. Automated policy enforcement ensures continuous compliance and aids in avoiding costly regulatory violations.

Mobility and Cloud Initiatives

Worker mobility and cloud adoption is taking place at an ever-accelerating rate. The downside of the clear business advantages of this increase in flexibility and efficiency, is the new risk it creates. Security and Network administrators must now deal with endpoints connecting from a very fluid set of locations. Organizations need to extend visibility into remote endpoints and public cloud infrastructures. NAC centralizes management and enables secure access for mobile and cloud devices through visibility and uniform policies across a diverse landscape.

Shortage of Skilled Security Professionals

Most IT organizations are continuously mandated to do more, with fewer resources. The severe shortage of security professionals drive management to look for better security tools with better value and automate systems so the core security teams can focus on strategic projects. Zero Trust NAC ensures access policies are automated and enforced on all endpoints, from a central location, even across the wide variety of endpoints and decentralized access infrastructure.

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 cloud endpoints

Automated policy enforcement frees up resources for security personnel and lowers overall risk

IoT and IIoT-enabled devices increase exposure to attack

Evolution to Zero Trust NAC

NAC solutions started in the early 2000's with a focus on very strict Authentication, Authorization and Accounting (AAA) based enforcement. Early adoption rates suffered, as these solutions were difficult to deploy, often operationally disruptive and low on investment return to IT management.

Then, NAC solutions introduced visibility and access-control features that aided management in planning and implementing security policy to combat modern network attacks from all endpoints including IoT, BYOD or guest devices. As a result, large organizations began to uncover unmanaged endpoints on the network and began to see the value-proposition of NAC.

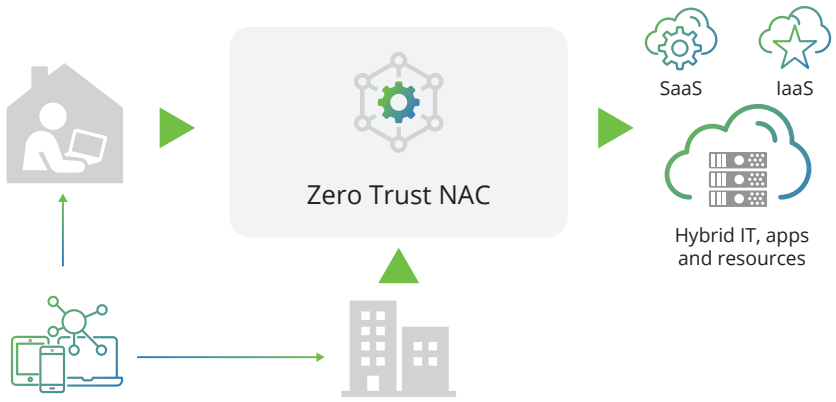
Now, NAC counters risk with advanced Security Automation and Orchestration (SAO) capabilities. SAO automates threat response on endpoints by sharing contextual information with other security and network solutions. Bidirectional integration with SIEMs, NGFWs, MDM/EMM enhances overall security efficacy and offloads Security and Networking administrators from doing repetitive tasks.

The concept of a Zero Trust Architecture has been around for about a decade. Zero Trust Networking (ZTN) is a principle or overall strategy to prevent unauthorized access, contain breaches, and reduce the risk of an attacker's lateral movement through a network. NAC is a foundational security defense, and a pillar to deploy Zero Trust.

Core NAC Capabilities

Visibility

In order to protect and control network access, you need to know what endpoints are connected, 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.



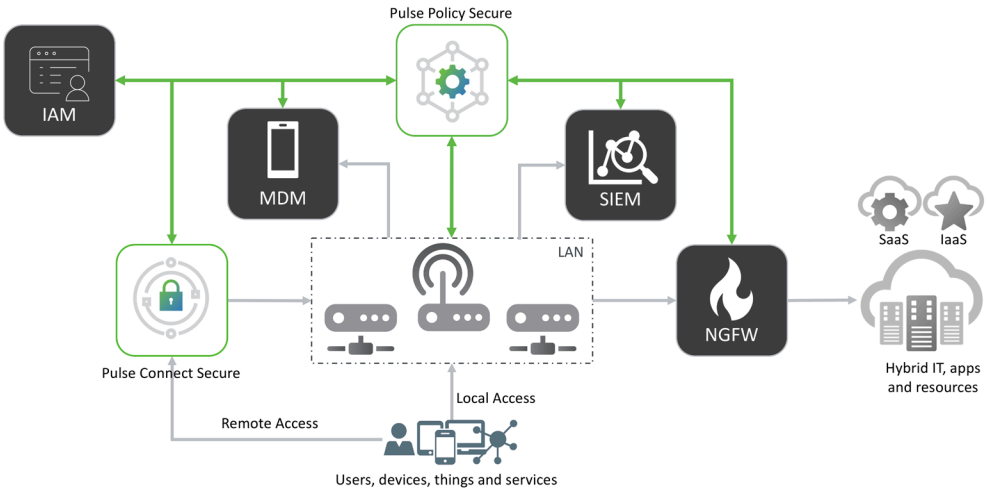
Zero Trust NAC policies treats all connections the same, remote or local

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 tasks and helps scale BYOD and IoT deployments.

Security Automation and Orchestration

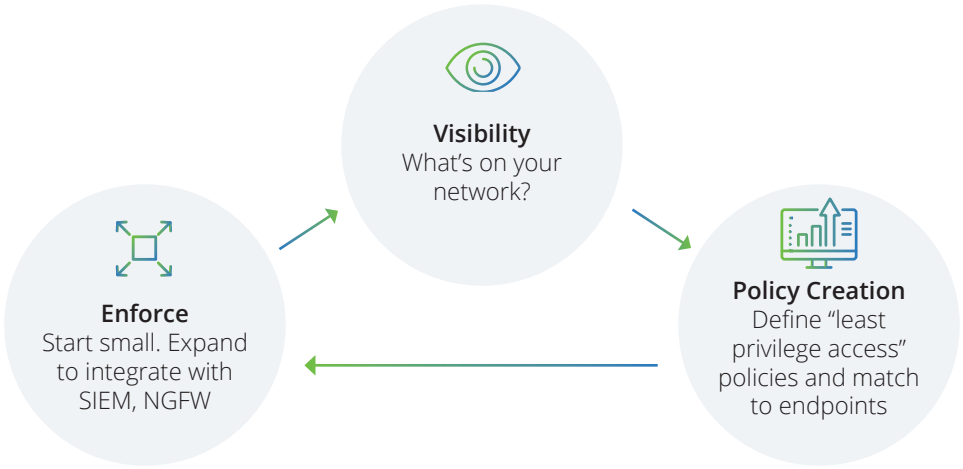
The threat of breaches remaining undetected for extended periods is growing. Without automation, security incidents may be lost in the daily deluge of alerts and overlooked. When combined with third-party network security, vulnerability and risk assessment and systems management solutions, NAC contextual data expands the efficacy of endpoint intelligence and provides fast, automated threat response.



Bidirectional integration of Pulse Policy Secure NAC with Access and Security infrastructure enables immediate threat response at endpoint level

Implementation

Deploying a NAC platform requires careful thought and planning. NAC solutions provide full visibility of endpoints and enforce security policies. There are several considerations how to use the available features to best matches your organization's needs.



Implement NAC in phases for frictionless transitions

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.

802.1X for True Zero Trust

802.1X is a proven, widely supported technology for dynamic access control on network edge devices such as switches and wireless LAN controllers. It is perceived as challenging to implement. However, a phased deployment ensures a smooth migration. And once implemented, it's very easy to maintain; a lasting payoff that frees up IT and security team resources. 802.1X technology holds true to the Zero Trust principle of 'validate before connect' and holds continuous and direct communication with the authentication servers. It tracks all endpoints that connect on a port to prevent extra, unsanctioned devices "piggybacking" via a switch or WiFi router on the established connection of a validated endpoint.

Alternative technologies to control edge network devices are SNMP or CLI access (over SSH). MAC authentication, in combination with a granular visibility and profiling solution, ensures headless devices such as printers, IP phones, cameras and so on, can connect securely.

Agent or Agentless

The security posture of an endpoint may consist of many variables such as AV definitions, OS or other software update status, active apps, and so on. There are different ways to assess this. The most secure, granular and responsive option is to install an agent on the endpoint. The agent can provide 802.1X functionality, but today's Operating Systems provide this supplicant too. Agents from vendors such as Pulse Secure that provide additional secure access products such as VPN or SDP, the agent can serve all solutions.

To avoid the complexity of rolling out an agent on all endpoints, "agentless" 802.1X deployments can be an alternative. However, there are quite some concessions when opting for this approach. First, for the endpoint to communicate with the NAC controller, it requires initial network connectivity. "Allowing, then evaluating" defies the essence of Zero Trust. Inside this shared network environment and timespan to assess the security posture, threats can spread freely. Another complication is the discovery phase; how the NAC learns that a new endpoint is connecting. One way is to glean this information from the DHCP server. Some vendors promote the use of SPAN Ports for device detection and classification, which increases network complexity and cost. Once the user is connected, WMI/RPC/SSH protocols can also convey endpoint contextual information and then enforce role-based access policies. This defies the core principal of Zero Trust implementation and provides a poor end-user experience. Other drawbacks of using agentless posture checks are that posture changes go undetected until next polling interval, which can be several hours. In addition, agentless requires full administrative access to all Windows systems.

Other Deployment Considerations

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.

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.

Pulse Policy Secure: Zero Trust NAC

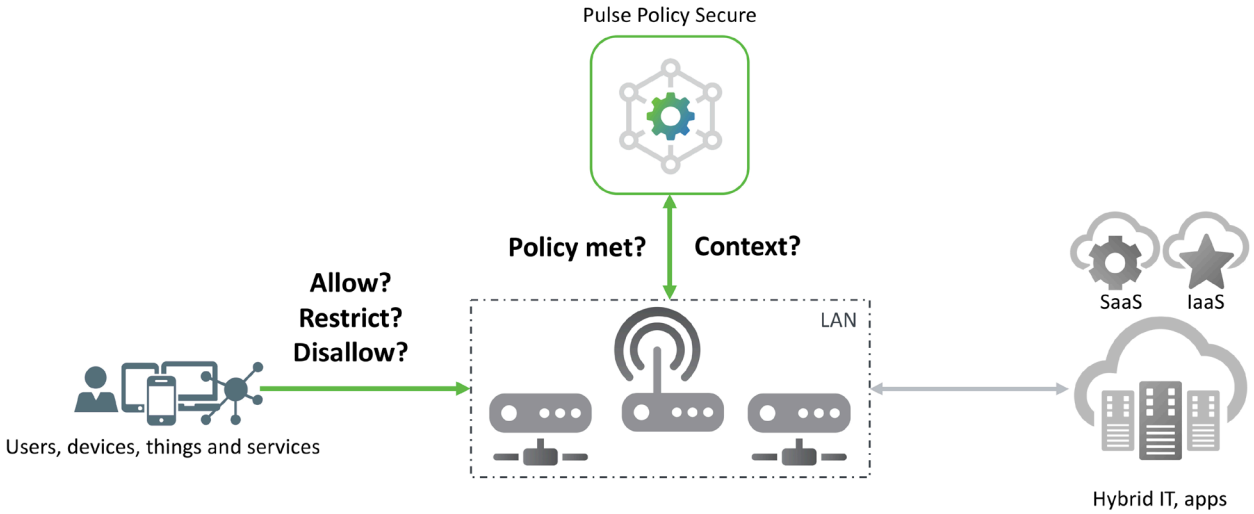
Pulse Policy Secure (PPS) provides complete visibility and Network Access Control (NAC) for all endpoints, regardless of their network location. PPS leverages adaptive authentication and User and Entity Behavioral Analytics (UEBA) functionality to track endpoints, enabling automated threat responses for threats like MAC spoofing, DGA attacks and more. Its open, high-performance design helps small and large organizations to easily enforce endpoint security compliance and Zero Trust security.

Pulse Policy Secure continuously enforces foundational security policies and controls network access for managed, unmanaged, and IoT endpoints. PPS uses Zero Trust principles to manage network access by validating the user, a device's security posture and connects the device with least privilege access policy.

The open platform integrates with a wide range of switching, Wi-Fi and NGFW solutions to enforce access policies. Bidirectional integration with 3rd party security solutions improves overall security efficacy with automated endpoint access enforcement.

Automated responses to Indicators of Compromise (IoC) reduces remediation time and streamlines administrative resources. PPS integrates with a wide range of NGFWs such as Palo Alto Networks, Checkpoint, Juniper and Fortinet, as well as SIEM solutions such as IBM Qradar and Splunk.

Learn more at PulseSecure.net/NAC



Pulse Policy Secure enables secure access for users, devices, things and services

Conclusion

To implement Zero Trust, automate the enforcement of access security policies and reduce risk, a NAC solution is indispensable. 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 real-time threat response against malware and network attacks—is worth the investment.

Corporate and Sales Headquarters
Pulse Secure LLC

2700 Zanker Rd. Suite 200
San Jose, CA 95134

(408) 372-9600

info@pulsesecure.net
www.pulsesecure.net

linkedin.com/company/pulse-secure
www.facebook.com/pulsesecure1
twitter.com/PulseSecure
info@pulsesecure.net