



Pulse Policy Secure



Overview

Visibility of all devices connecting to the network is a primary driver for prospects seeking out NAC solutions. You can't protect what you cannot see. Automated profiling, monitoring and tracking of devices help administrators in their daily activities as well as providing meaningful metrics for management.

Network Access Control (NAC) solutions help to enforce policies during pre- and post-admission control to achieve zero trust network security. This security posture is a list of software that is active or installed on an endpoint, such as Antivirus solutions, the operating system itself and any other apps. The posture also informs about the current software versions and software updates. NAC solutions can enforce policies where an endpoint's security posture must meet criteria such as how current the OS updates or virus definitions need to be, before allowed on the network. Defining foundational security policies, and automatically enforcing them, helps organizations always stay within compliance of the relevant regulations, making the auditing process much easier.

Access privilege policies are also under scrutiny by foundational security principles. Role Based Access Control (RBAC) leverages the least privilege access model, which means a user only has a minimal set of privileges and access that are strictly required for their role and responsibilities.

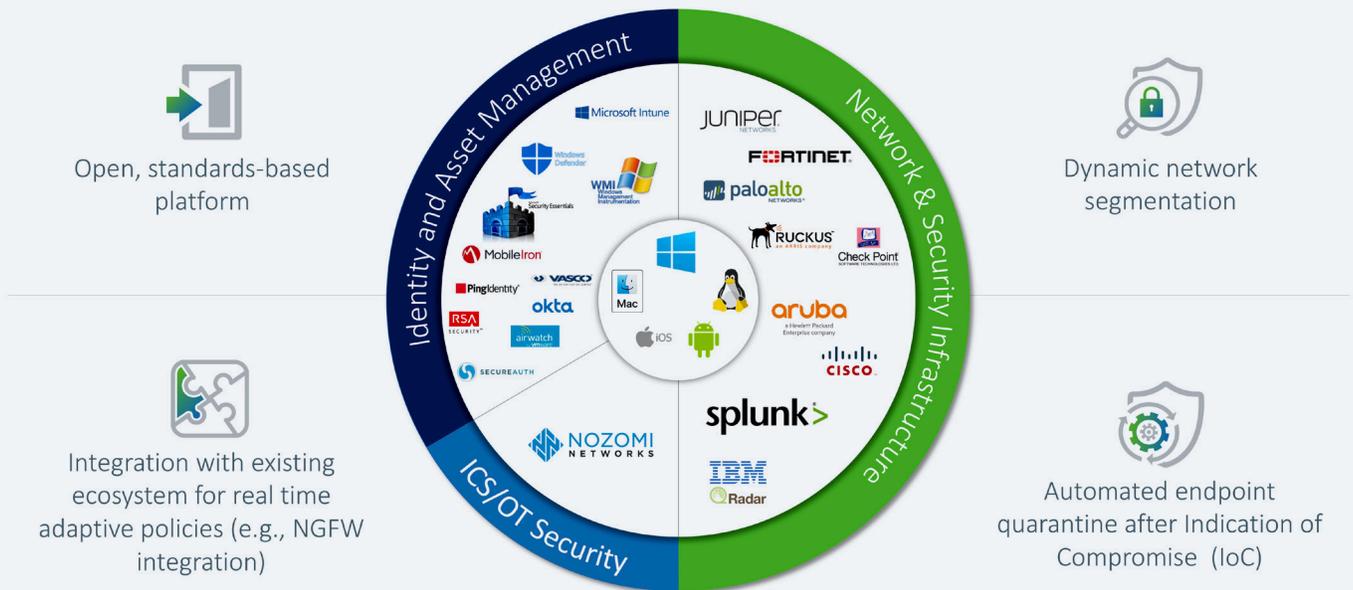
Network segmentation means that classes of users and/or devices, stay within their lane. If an endpoint is compromised, the threat is contained within a segment, limiting the risk of threats spreading laterally to segments with higher access privileges. Automating the onboarding of devices and users and dynamically provisioning the network and firewalls, also aids in compliance and audits

Key Functionality

- Pulse Secure Profiler: Collect endpoint device profiling information and maintain dynamic, contextual inventory of networked devices including IoT devices.
- RADIUS/802.1X support: Integrated, high-performance RADIUS system provides authentication of devices and users attempting to connect to wired and wireless LANs so that only authorized connections are allowed.
- Automated patch assessment checks and remediation: Can tie access directly to the presence or absence of specific hot fixes for defined operating systems and applications, and performs role-based, predefined patch management checks according to the severity level of vulnerabilities.
- Session Federation: Federation of user sessions between Pulse Connect Secure and the Pulse Policy Secure enables seamless provisioning of remote access user sessions into LAN access user sessions upon login, or alternatively LAN access user sessions into remote access user sessions at login.
- UEBA Analytics: Correlation of user access, device data, and system logs in a new analytics engine

- Identity-based admission control: Combines identity-aware capabilities of Pulse Policy Secure with the robust networking and security services of Fortinet, Palo Alto Networks, Checkpoint, and Juniper SRX Series Firewalls, enabling each to be employed as policy enforcement points.
- Automated Threat Response: Leverages next-generation firewall's intelligence driven threat detection to take automated actions by Pulse Policy Secure at the device and user level. PPS policy engine and rich contextual information allows it to take different actions based on threat severity and mitigate security risk further.
- Captive portal: Provides network access control for guests and contractors
- Self-service Guest access support: Enhances and simplifies an organization's ability to provide secure, differentiated guest user access to its network and resources.
- Wizard-based configuration: Aides administrators in navigating and familiarizing themselves with configuration tasks in Pulse Policy Secure admin UI.
- Granular auditing and logging: Provide auditing and logging capabilities delivered in a clear, easy to understand format.
- Centralized policy management: Saves administrative time and cost and a superior user experience by delivering common remote and local access control policy implementation and enforcement across a distributed enterprise.

Pulse Policy Secure Integration Into Ecosystem



Ordering Options

Specifications

Pulse Secure client, as the user interface for Pulse Policy Secure, supports Microsoft Windows 10, Windows 8, Windows 8.1, Windows 7, Windows RT and Windows Vista SP2 operating systems. Pulse Secure also supports Apple Mac OS X 10.6 (or higher) operating system software, Apple iOS, and Google Android.

Clientless mode secures devices running Microsoft Windows 10, Windows 8.1, Windows 8.0, Windows 7, and Windows Vista SP2 operating systems, Apple Mac OS, and Linux operating systems and platforms including Fedora, Ubuntu and openSUSE, interoperating with supported browsers which include Microsoft Internet Explorer, Mozilla Firefox, and Apple Safari.

For specific supported operating system software, operating platforms, and browser versions, please refer to the latest version of the Pulse PSA Series Appliance Family document, which may be found at www.pulsesecure.net.

ORDERING NUMBER	DESCRIPTION
Policy Secure Licenses	
POLSEC-xU(-zYR)	Add x simultaneous PPS users to Pulse PSA Appliance (x options: 10, 25, 50, 100, 250, 500, 1000, 2000, 2500, 5000, 7500, 10k, 15k, 20k, or 25k concurrent sessions) Subscription Licenses (z options: 1, 2, or 3 year)
POLSEC-ADD-yU	Add y simultaneous PPS users to Pulse PSA Appliance (y options: 10, 25, 50, 100, 250, 500, 1000, 2000, 2500, 5000, 7500, 10k, 15k, 20k, or 25k concurrent sessions) Perpetual for hardware platform where activated
PS-PROFILER-RADIUS-SM	Pulse Secure Profiler with max 500 devices for PSA 300/3000 Platform - Includes RADIUS Server capability
PS-PROFILER-RADIUS-MD	Pulse Secure Profiler with max 10,000 devices for PSA5000, PSA7000 Platform - Includes RADIUS Server capability
PS-PROFILER-RADIUS-LG	Pulse Secure Profiler with max 50,000 devices for PSA7000 Platform - Includes RADIUS Server capability
PS-PROFILER-RADIUS-SM-HA	Pulse Secure Profiler with max 500 devices for PSA300/3000 Platform - Includes RADIUS Server capability and High Availability
PS-PROFILER-RADIUS-MD-HA	Pulse Secure Profiler with max 10,000 devices for PSA5000 Platform - Includes RADIUS Server capability and High Availability
PS-PROFILER-RADIUS-LG-HA	Pulse Secure Profiler with max 50,000 devices for PSA7000 Platform - Includes RADIUS Server capability and High Availability
PS-PROFILER-RADIUS-SM-1 YR or 2 YR or 3 YR	Pulse Secure Profiler with max 500 devices for PSA300/3000 or Virtual Platforms - Includes RADIUS Server capability and High Availability (Subscription 1 or 2 or 3 Year with GOLD Support)
PS-PROFILER-RADIUS-LG-1 YR or 2 YR or 3 YR	Pulse Secure Profiler with max 50,000 devices for PSA7000 or Virtual Platforms - Includes RADIUS Server capability (Subscription 1 or 2 or 3 Year with GOLD Support)

	Data Center						IaaS	
	Physical Appliance			Virtual Appliance			Cloud	
		VPN	NAC		VPN	NAC		VPN
Models and License Capacity	PSA300/3000 PSA5000 PSA7000	200 2500 25000	500 10000 50000	PSA3000-V PSA5000-V PSA7000-V	200 2500 25000	500 10000 50000	PSA3000-V PSA5000-V PSA7000-V	200 2500 25000
Platforms	Purpose-built			VMware, KVM, Hyper-V			Azure	
Supported Software Services	VPN, NAC			VPN, NAC			VPN	
Software Licensing	Perpetual, Subscription			Subscription			Subscription	
Clustering	Active / Active Active / Passive			Active / Active Active / Passive (Limitations: 2 node, VMware)			Planned	
ICE (In Case of Emergency)	✓			✓			✓	
License Server (on-premises)	✓			✓			✓	

Pulse Secure Services and Support

Pulse Secure is the leader in performance-enabling services that are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to maximize operational efficiency while reducing costs and minimizing risk, achieving a faster time to value for your network. Pulse Secure ensures operational excellence by optimizing the network to maintain required levels of performance, reliability, and availability.



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

ABOUT PULSE SECURE

Pulse Secure, LLC offers software-defined Secure Access solutions that provide visibility and easy, protected connectivity between users, devices, things and services. The company delivers suites that uniquely integrate cloud, mobile, application and network access control for hybrid IT. More than 23,000 enterprises and service providers across every vertical rely on Pulse Secure to empower their mobile workforce to securely access applications and information in the data center and cloud while ensuring business compliance. Learn more at www.pulsesecure.net.

[linkedin.com/company/pulse-secure](https://www.linkedin.com/company/pulse-secure)
twitter.com/PulseSecure

www.facebook.com/pulsesecure1
info@pulsesecure.net