DATASHEET

Pulse Policy Secure

Uncomplicated Device Discovery and Control for Zero Trust Networks

Highlights

- End to end visibility into what's connecting on your network on-premises or remote
- Enhanced assessment of endpoint device health and security posture before allowing access
- Standards-based open API for easy integration with security and network ecosystem
- Discovers and profiles all network connected devices
- Detects anomalous device behavior for potential malware and domain generation algorithm (DGA) attacks

Benefits

- Seamless, end-to-end Zero Trust access security
- Device discovery, profiling and security enforcement for all devices (corp owned, BYOD and IoT)
- Insightful behavioral analytics detects anomalies and protects against threats such as DGA attacks and MAC spoofing
- Seamless user experience for guest access
- Comprehensive access management from endpoint to datacenter identifies unauthorized devices, users and applications while remediating on demand.

While external malicious threats continue to terrorize the enterprise network, network access control (NAC) solutions are also challenged by IT transformations like "bring your own device" (BYOD), cloud services, and the Internet of Things (IoT). As the last line of defense in network security, enterprises must adapt NAC for a borderless network that services an increasing number and type of endpoints.

Today's solutions empower IT administrators to implement zero trust security with the ability to define, implement, and enforce granular access polices for connecting endpoints based on contextual information (e.g., user ID, role, device type, security posture, location).

Pulse Policy Secure (PPS) is an easy, flexible and interoperable NAC solution that provides visibility with security enforcement, to control managed, unknown, and IoT devices connecting locally or remotely to the network. The platform seamlessly integrates with popular network switches, wireless controllers, Firewalls, EMM and Security Information Event Management (SIEM) systems. Pulse Policy Secure solution includes:

- **Pulse Secure Profiler** identifies and enables automatic and custom classification of both managed and unmanaged endpoint devices and IoT devices; providing operational visibility, reporting, and policy-based controlled access to networks and resources, based on the user, device, applications, communications and other attributes.
- **Pulse Policy Secure** is a high-performance, context-aware policy engine, offering user, endpoint, and application contextual information. With a unified framework and policy engine, administrators can apply granular rules for dynamic monitoring, reporting, and access control; including establishing whitelist or blacklist applications, to minimize access risks.
- **Pulse Client** offers agent and agentless options for pre- and post-admission control. The solution incorporates the Host Checker functionality, which applies multiple factors to verify endpoint configuration, communication and behavior for such devices as printers, wireless access points, video cameras and medicine dispensers. This approach can leverage an existing 802.1x supplicant/agent or use other posture assessment means that negate reliance on a supplicant/agent.

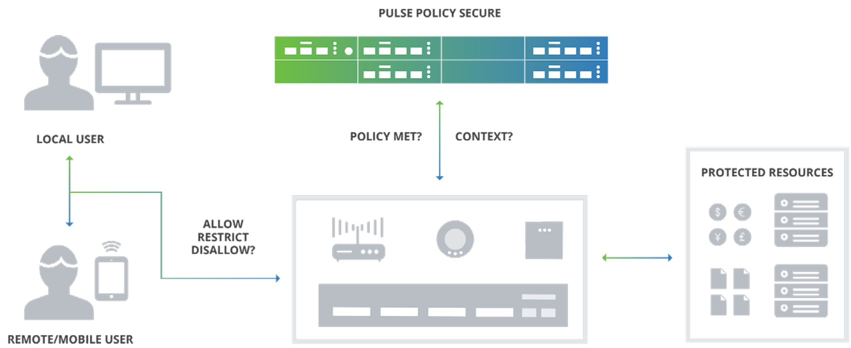

Figure 1: Real-time network visibility and enforcement to enable Zero Trust security

Challenges

Sprawl leads to device blindness and vulnerable networks

A healthy business is a great thing. Business expansion necessitates the need for trained employees, enjoyable work premises, and scalable solutions that support core business. New solutions that support the breakneck pace of business has created an influx of next-generation network-connected devices that are overwhelming IT team's capacity to control.

BYOD, guest-access networks, and IoT solutions are generating device numbers on an immense scale. As a result, IT teams are struggling to cope with endpoint discovery and policy enforcement.

The challenges of device sprawl and policy control:

- Visibility
- Enforcement
- Zero Trust security based on user and device
- Scale
- Management

Solution

Pulse Policy Secure empowers IT teams to meet the most stringent security requirements for device transparency, enforcement, and management. Organizations discover all BYOD, IoT, and endpoints using Pulse Policy Profiler. Policy compliance enforcement is accomplished with Pulse Policy Secure. The solution includes a central management console from which IT can manage appliances, monitor health and alert status, and generate powerful reports.

Key features of Pulse Policy Secure include:

- Security policy enforcement for any BYOD, laptop, or IoT device
- Onboard RADIUS server for seamless device authentication, regardless of location
- User Entity Behavior Analytics (UEBA) engine utilizes user, device, and location device profiling to detect anomalies
- Complete device visibility whether on-premise or off-premise
- Scalable solution that supports over 50,000 concurrent devices

Use Case Overview

Pulse Policy Secure is helping to adapt network security to the rapidly changing workplace. Enterprises use its proven NAC to enforce policy compliance by employees, guests, and contractors regardless of location, device type, or device ownership. Users enjoy greater productivity and the freedom to work anywhere without sacrificing access to authorized network resources and applications. Integrated BYOD onboarding optimizes the enterprise user experience by allowing workers to use their preferred device.

With Pulse Policy Secure, complete visibility of managed and unmanaged network devices is achievable.

The Internet of Things (IoT)

Enterprises today employ IoT devices with data and applications to improve business. Pulse Policy Secure offers enterprises the ability to discover and secure these devices.

CHALLENGES	PULSE POLICY SECURE SOLUTION
Discovery and profiling of IoT devices	Pulse Policy Secure discovers managed and unmanaged devices. Moreover, it can profile them so subsequent discovered devices are managed and secured. This concept is extended to industrial factory floors or smart buildings where IoT systems now manage legacy devices such as factory floor PLCs or office building HVAC systems.
Behavioral Analytics	Pulse Policy Secure provides enhanced security for managed and unmanaged IoT devices. This is accomplished using behavioral analytics that utilizes user and device traffic patterns to detect compromised IoT devices. Behavioral Analytics builds baseline behavior profiles for IoT devices by collecting and correlating NetFlow, user, and device data. Profiled base behavior is used to detect anomalous device activity, anomalous user access, domain generation attacks and MAC spoofing.

Visibility

Every networked device is a potential entry point from which cyberattacks may originate. Establishing of complete endpoint device visibility gains the insights required to dynamically identify and classify all managed and unmanaged endpoints. Through visibility, organizations gain valuable insights on users, required to reduce security exposure.

CHALLENGES	PULSE POLICY SECURE SOLUTION
Profiling	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.
Numerous Device Types	Pulse Secure Profiler can automatically classify devices against a growing database of over 11,000 unique device types. The solution profiles endpoints assigned with static IP addresses and actively scans open ports to detect MAC spoofing.
Ease of Deployment	Pulse Policy Secure is easy to deploy, use, and maintain. Pulse Policy Secure can be flexibly deployed and scaled using multi-purpose physical (PSA series) or virtual (VMware, Hyper-V & KVM) appliances. It comes with an embedded standards-based RADIUS Server.

Policy Enforcement and Compliance

Pulse Policy Secure prevents unauthorized network, application, or data access by dynamically assessing and remediating device security before the device connects to the enterprise for both VPN and Wi-Fi access. This protects the corporate network from infected devices and enforces consistent, cross-network access policies. It also ensures only authorized workers have access to enterprise resources based on their role, location, and time of day.

CHALLENGES	PULSE POLICY SECURE SOLUTION
Guest User Support	Pulse Policy Secure provides a self-service portal with a customized and branded interface. It is a highly scalable enterprise guest access platform that supports thousands of guest users, ensuring every guest gets automated and authorized access to the network while remaining compliant with corporate security policies.
BYOD Onboarding	Pulse Policy Secure empowers employees to use their personal devices for work with self-service onboarding of personal laptops and mobile devices.
Unified Compliance Enforcement and Seamless Access Control	Pulse Policy Secure prevents unauthorized network, application, or data access by dynamically assessing and remediating device security before the device connects to the enterprise for both VPN and Wi-Fi access. It also ensures only authorized workers have access to enterprise resources based on their role, location, and time of day.

Pulse Policy Secure can be flexibly deployed and scaled using multi-purpose physical (PSA series) or virtual (VMware, Hyper-V & KVM) appliances.

How it Works

Pulse Secure Policy Secure is a comprehensive, easy-to-deploy, Zero Trust ready network access control (NAC) solution that granularly enforces security policies. It is centrally managed with a context-aware policy engine that provides user, role, device, location, time, network, and application granularity. A unified client provides an easy-to-use agent for both VPN and NAC.

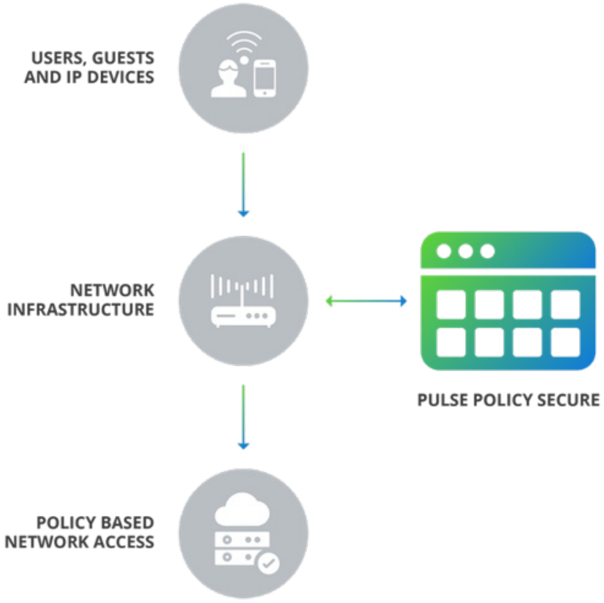

Figure 2: Pulse Policy Secure delivers an integrated 'comply to connect' solution that protects your network

Pulse Secure delivers a full featured, Zero Trust Access Control Solution:

An easy, flexible path to next generation NAC, starting with visibility by leveraging the Pulse Profiler and subsequently migrate to full enterprise-class NAC functionality while phasing in access enforcement, network coverage and core integrations.

"Comply to connect" policy enforcement and security orchestration with popular next-gen firewalls (NGFW), security information and event management solutions (SIEMs), switches, wireless controllers, enterprise mobility management (EMM) and endpoint security solutions.

Expedited NAC deployment for current Pulse VPN users by leveraging the same device Client (agent and agentless), centralized management console, and policy framework, while gaining full intelligence on remote, on-premise and cloud user and endpoint activity.

Pulse Secure®

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 20,000 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.

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