Pulse Secure®

Pulse Profiler

Security Starts with Visibility

Highlights

- Contextual visibility into remote and local users and endpoints, both agent and agent-less
- Automatically detects and classifies known and unknown devices against a growing database of tens of thousands of unique device types
- Seamlessly integrates with security infrastructure for policy-based enforcement
- Easy to deploy using a simple wizard-based configuration

"How many IoT devices exist, with how many computing devices do they share data? How many others have access to that data and what decisions are being made with this data? No one really knows. We just don't know."

Rebecca Herold, The Privacy Professor, at SecureWorld Atlanta

"Perhaps the two most important things are that we have increased our security posture and for the most part, there has been zero impact on our end users."

Dave Cullen, Manager of Information Systems, Entegrus

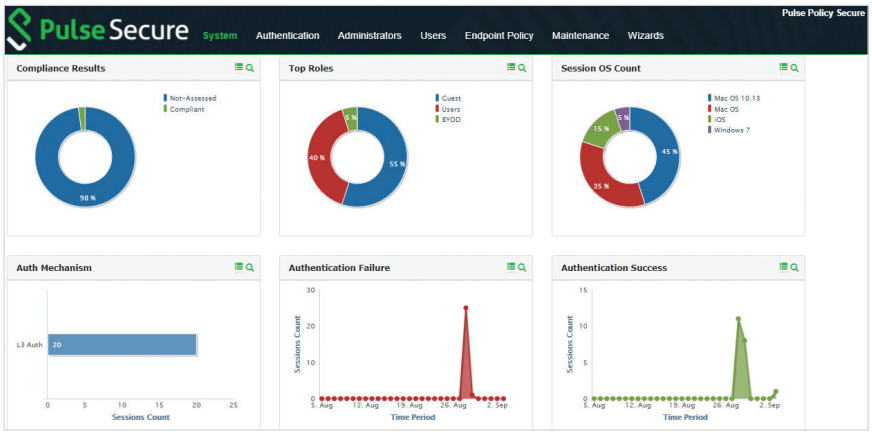
Pulse Profiler delivers real-time visibility, insight and tracking of endpoints and IoT devices, regardless of whether they connect over VPN, wired or wireless networks. It is an essential tool for any organization to track and monitor an ever growing and wide variety of devices connecting to the network.

Today's network visibility challenges

In today's increasingly complex threat landscape, organizations are more prone than ever to security breaches as hackers have become more adept at finding security gaps across the network and managing to escape un-noticed as they steal valuable assets, disrupt service and harm customers. The rise of Bring-your-own-device (BYOD) and IoT across workplaces, with a plethora of devices connected to the internet has created an enormous challenge for organizations to protect from a wide variety of threats that can originate from anywhere, anytime. Today, as many as 90% of companies are unaware of the endpoint and IoT devices connected to their network, magnifying the risk of breaches associated with lack of visibility: you cannot secure what you cannot see.

The solution: Pulse Profiler

Pulse Profiler has a growing database of over 2.3M unique fingerprints along with the ability to categorize devices based not only on their hardware/software versions and device types but also on their real-time behavior and applications accessed. Unlike traditional network visibility solutions Pulse Profiler can profile devices that are accessing resources remotely, making it a comprehensive, end-to-end visibility solution for both remote and local users and devices.



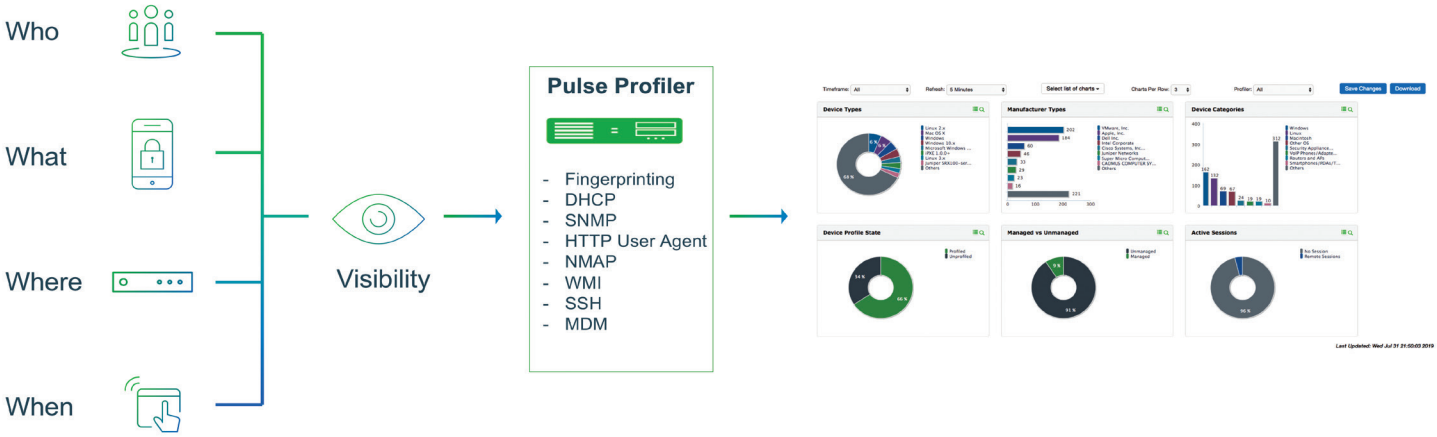
Dashboard for centralized visibility of discovered devices

Devices that are discovered are profiled and updated in the Device Discovery Table. An overall summary is shown in the Device Profiles Dashboard. The dashboard displays a clear overview of the status of all devices such as:

- Devices waiting to be profiled
- Devices for which the profile has changed
- Unmanaged devices
- Devices waiting for administrator approval
- Recently added devices...and more

Pulse Secure Profiler

Visibility with Context

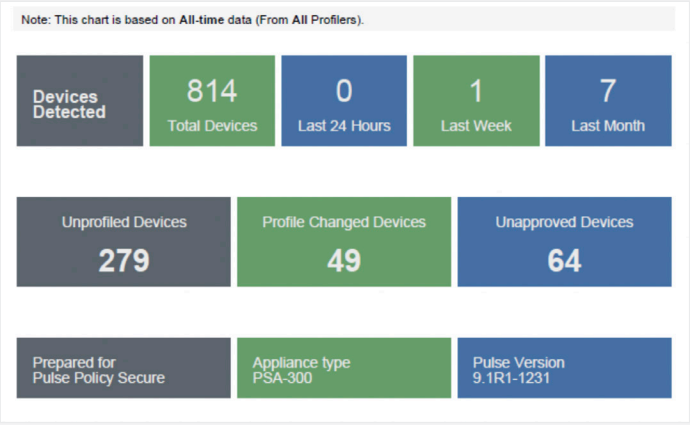


Detect and Classify devices

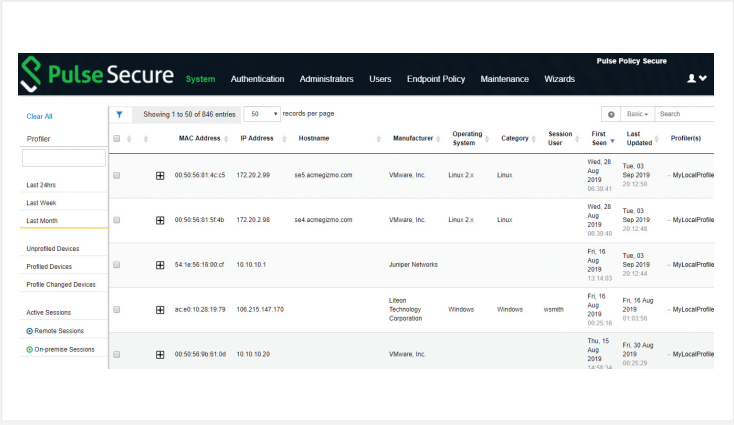
Pulse Profiler uses active and passive collectors for a wide spectrum of identification capabilities (DHCP, SNMP, Nmap, WMI, SSH, HTTP etc.) to accurately scan and discover devices. It continuously analyzes the behavior of all endpoints on the network. If an endpoint's behavior changes, Profiler can send an alert to the security management system or deny network access in conjunction with Pulse Policy Secure. Profiler monitors threat attempts from any endpoint connected via any means: wired, wireless, or remote, making it an essential **end-to-end visibility tool**.

Profiler Summary

The Pulse Profiler Reports is a snapshot in time of the different devices that have been identified and profiled by your Pulse Policy Secure appliance. This report also provides device data that includes top devices by category, OS and manufacturer. It will provide real time insights into your network and show you exactly what devices are on your network and what risks they pose. You can use the device information to create fine-grain role-based access control policies via the admin interface of pulse Policy Secure.



Periodic reporting for management



Device discovery report

CAPABILITIES	BENEFITS
Track remote devices	Go beyond traditional profiling solutions by identifying and profiling remote devices that access your resources, ensuring no threats go unnoticed
Wizard-based configuration	Step-by-step configuration of the most common deployment scenarios provide quick, error-free configuration
Dynamic authentication policy	Decrease complexity by leveraging existing AAA infrastructures. Supports RADIUS CoA (Change of Authorization) to change the attributes of an AAA session during re-authentication. RADIUS CoA allows devices to change the VLAN/ ACL for the endpoint based on roles.
SNMPv1/v2c/v3 Support	Dynamic discovery of endpoints through SNMP. Works with Pulse Policy Secure to ease NAC deployment with SNMP enforcement; no need for 802.1x supplicant. Simplify deployment and lower cost by supporting legacy switches that do not support 802.1x
Scalable Solution	Accommodate and monitor up to 50,000 endpoints using a single appliance for enterprise-scale visibility and low total cost of ownership
Comprehensive fingerprinting database for IoT/IIoT devices	Recognize a very diverse set of IoT devices with our growing fingerprinting database of over 2 million unique fingerprints. and provision them automatically with Pulse Policy Secure regardless of location
Dynamic addressing of unmanageable endpoint devices	Use MAC address authentication with whitelisting and blacklisting for unmanageable devices such as networked printers, cash registers, bar code scanners, VoIP handsets, etc.
Agentless host checker	Monitor non-NAC client capable IoT devices with our agentless host checker that provides endpoint compliance validation and security posture
Seamless integration with Pulse Policy Secure, our Next-Generation Network Access Control (NAC) solution	Get policy-based network access with Pulse Policy Secure, which is our Hybrid-IT focused next-gen NAC solution that integrates seamlessly with data center infrastructure (next-gen firewalls, switches, wireless networks and MDM solutions)
Auto-classification and multi-factor intelligence gathering	Leverage a growing database of more than 11,000 unique device types and gather insights using various methods such as DHCP Fingerprinting (Helper Address or RSPAN port), MAC OUI, SNMP/ SNMP Traps, CDP/LLDP, HTTP User Agent, Nmap, WMI and WDM for full-proof latest standard security
Comprehensive scanning and reporting	Run custom scans and schedule reports with advanced filters based on IP-subnets and profiler endpoints for granular level visibility across endpoints

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 provides easy, comprehensive software-driven Secure Access solutions for people, devices, things and services that improve visibility, protection and productivity for our customers. Our suites uniquely integrate cloud, mobile, application and network access to enable hybrid IT in a Zero Trust world. Over 20,000 enterprises and service providers across every vertical entrust 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
www.facebook.com/pulsesecure1
twitter.com/PulseSecure
info@pulsesecure.net

Version: 09-04-2019