Solution Brief

Pulse Secure

Pulse Policy Secure and Ruckus Wireless

Identity Enforced Secure Access

- Granular reinforcement via device and user roles to confidential resources
- Expanded monitoring and reporting with real-time mitigation
- Extended endpoint compliance

Dynamic network resource for your mobile workforce

Today's digital workforce continues to challenge IT administrators with their increasing needs to be productive anytime. Balancing new workforce productivity trends, like BYOD, and the security essentials for industry compliance, enterprises need a robust user authentication, device compliance and secure access policy enforcement for their smarter Ruckus Wireless systems. Pulse Policy Secure offers an enterprise grade network access control solution that is flexible, scalable, and context-aware to meet the growing demands of a dynamic workforce.

Challenges

Flexible workstyle secure access

Visibility into BYOD environments and offering self-registered guest access.

Network surveillance for security orchestration

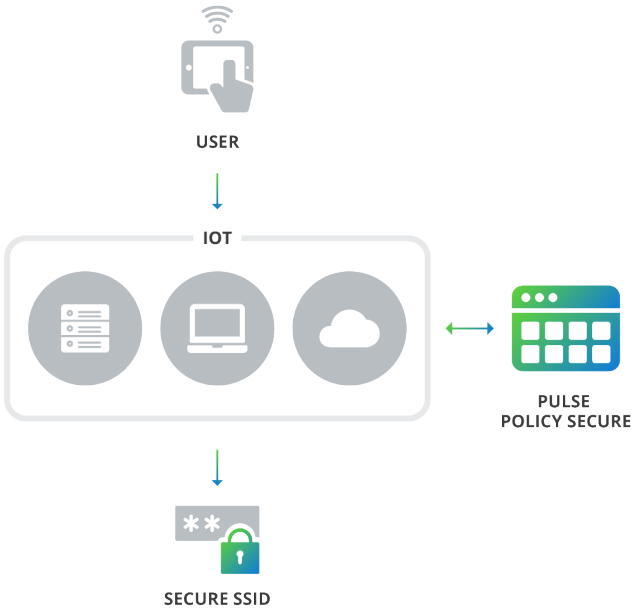
Comprehensive policy-based access control that offers real-time monitoring and automated remediation.

Easy comprehensive compliance check

Manage BYOD and other IP-enabled endpoints access to existing networks for policy management, while delivering a café like onboarding experience.

Simplified Secure Access for the Digital Workforce

Pulse Policy Secure and Ruckus Wireless offer a comprehensive network access control to streamline context-aware access and information sharing for a mobile workforce that demands productivity on their time.



Solution Requirements

Secure Access Appliance

Use your PSA, MAG or virtual appliance.

Pulse Policy Secure

Requires Pulse Policy Secure software running on your appliance.

Ruckus Wireless

Integration with Ruckus Wireless SmartZone and ZoneDirector WLCs products.

Benefits

Self-registered guest access

Remove cumbersome and resource-intensive guest access experience and offer simple café-like access to your distributed workforce.

1.2.3. BYOD

Offer support for BYOx with a dynamic context-aware (who, what, when, where) platform that supports pervasive access.

End-to-end compliance

Adhere to many compliance standards and guidelines: Sarbanes-Oxley (SOX), the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS) and Federal Financial Institutions Examination Council (FFIEC) principles and standards.

Comprehensive network IQ

Offers a uniformed cross-platform network collaboration among parts of the IT infrastructure from asset and configuration management to SEIM.

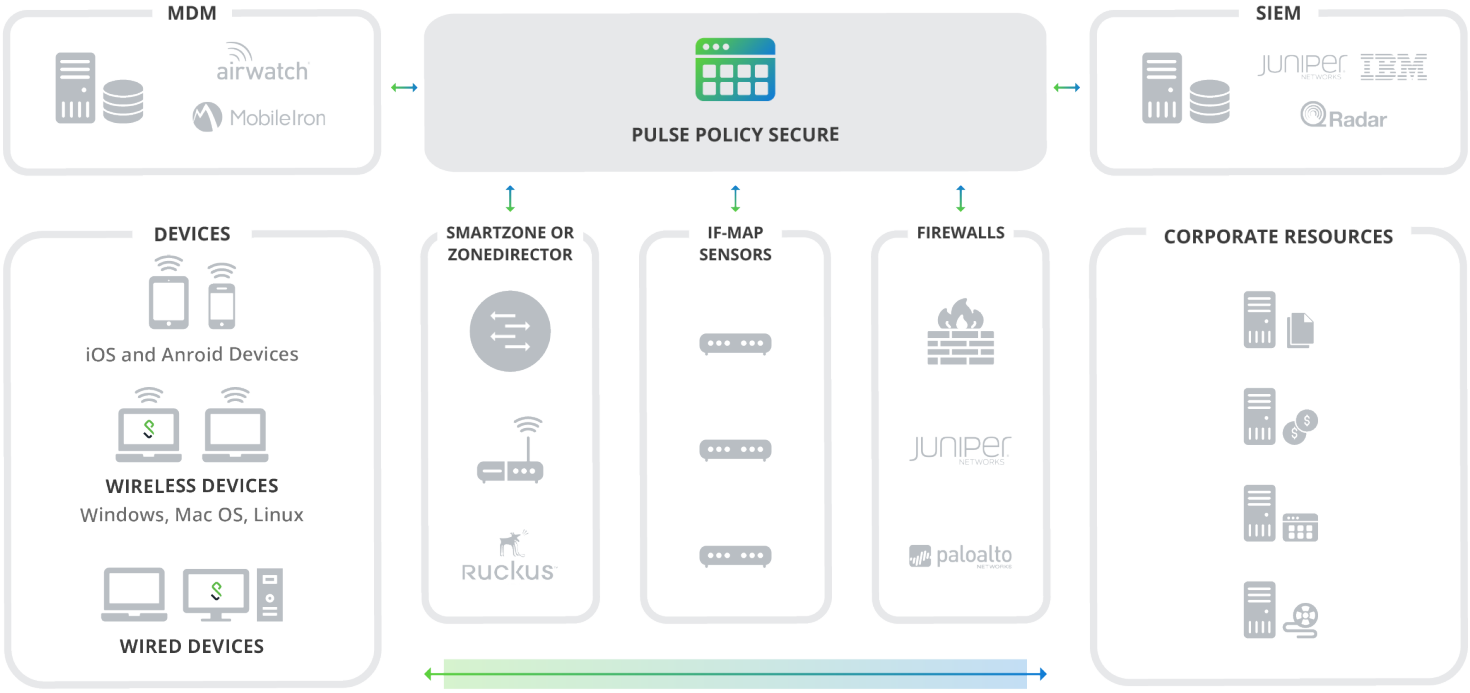
Control inside and APT attacks

Monitor network activity and health with the ability to link into an Advanced Threat Protection and Mitigation System.

Unified remote/onsite access*

Provide an optimal and cost-effective secure access experience for those workers who frequently commute remote to onsite.

*Joint solution with Pulse Connect Secure



How does it work?

Pulse Policy Secure's integration into Ruckus Wireless delivers a simple, secure network, and application access control with a standards-based, granular solution that provides access control based on context (user identity, device type, integrity, and location). Policy Secure supports phased deployments and can scale to support global distributed organizations. Pulse Policy Secure uses three core components; Appliance (Pulse PSA Series, MAG Series or Virtual Appliance), Pulse Client (or Clientless), and the following Ruckus Wireless product lines, SmartZone and ZoneDirector. Most importantly, working with Pulse Connect Secure, Policy Secure offers an optimal secure access experience for your workforce from remote to onsite via a unified client, Pulse Client.

Self-Registration + automatic credential delivery

Customizable guest portal offers easy-to-use, cross-platform registration process. Guest has the option to choose access credentials via email, SMS text, or print.

Simplified BYOD onboarding

Automated configuration of devices with settings and software for Wi-Fi, VPN and more.

Comprehensive network visibility & control

Simplified auditing and monitoring of network devices enterprise wide with a seamless interoperable ecosystem of security and compliance solutions.

Automated patch assessment and remediation

Minimize downtime through automatic remediation of patches for endpoint devices and risk via centralized policy platform to define and apply context-aware secure access.

Wizards and templates

Remove complexity and cost out of setting up a NAC solution.

Host checking

Perform endpoint checks to address compliance enforcement.