Solution Brief

Pulse Secure

Pulse Policy Secure for Government

Federated visibility and control for Smart Government

- Control access to confidential resources based on device and user roles
- Mitigate cyber security risks from infected or noncompliant endpoints
- Deploy with ease across multi-vendor networking environment

Visibility and Assurance for e-Public Services (Civic public services)

Seeking to improve citizen services for the digital individual, leaders of "smart cities" are re-inventing and streamlining today's public services. Local experiments include "smart parking" that helps commuters find spots (and streamlines city enforcement) via their in-dash navigation or smartphone. To ensure an appropriate and consistent level of security, government IT organizations must demonstrate and maintain compliance with a large and growing number of regulations, directives, and standards.

Challenges

Civic-ready Secure Access

Multi-tier 'Acceptable Use' security policies across federal, state and local branches for public sector employees, contractors, and citizens.

Cyber Readiness Inspection

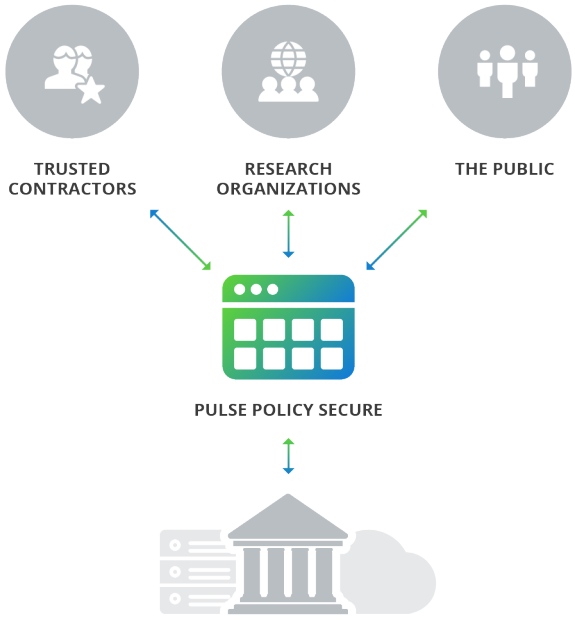
Comprehensive policy-based access control that offers real-time monitoring and automated remediation.

Interoperability to Existing Networking Infrastructure

e-Government mandates interoperability for improved efficiency, transparency, accountability, and access. Policy Secure interoperates with any vendor's standards-compliant switching and wireless infrastructure. We have enhanced vendor-specific customization for integration with Cisco, Aruba, Ruckus.

Institutional-grade Secure Access for Federal, State, and Local Entities

Pulse Policy Secure offers comprehensive network access control to streamline context-aware access and information sharing for trusted contractors, research organizations, and the public.



Solution Components

Secure Access Appliance

Use your PSA, MAG or virtual appliance.

Pulse Policy Secure

Requires Pulse Policy Secure software running on your appliance.

Benefits

Citizen-grade Guest Access

Remove cumbersome and resource-intensive guest access interface and offer simple café-like access to resources for your constituents.

Community-based BYOD

Meet multi-level security policies of federal, state, and local with a dynamic context-aware (who, what, when, where) platform that supports pervasive access.

Civic Compliance

Comply with North American, European and international regulatory mandates and directives designed to protect sensitive information, from FISMA to ENISA.

Comprehensive Network IQ

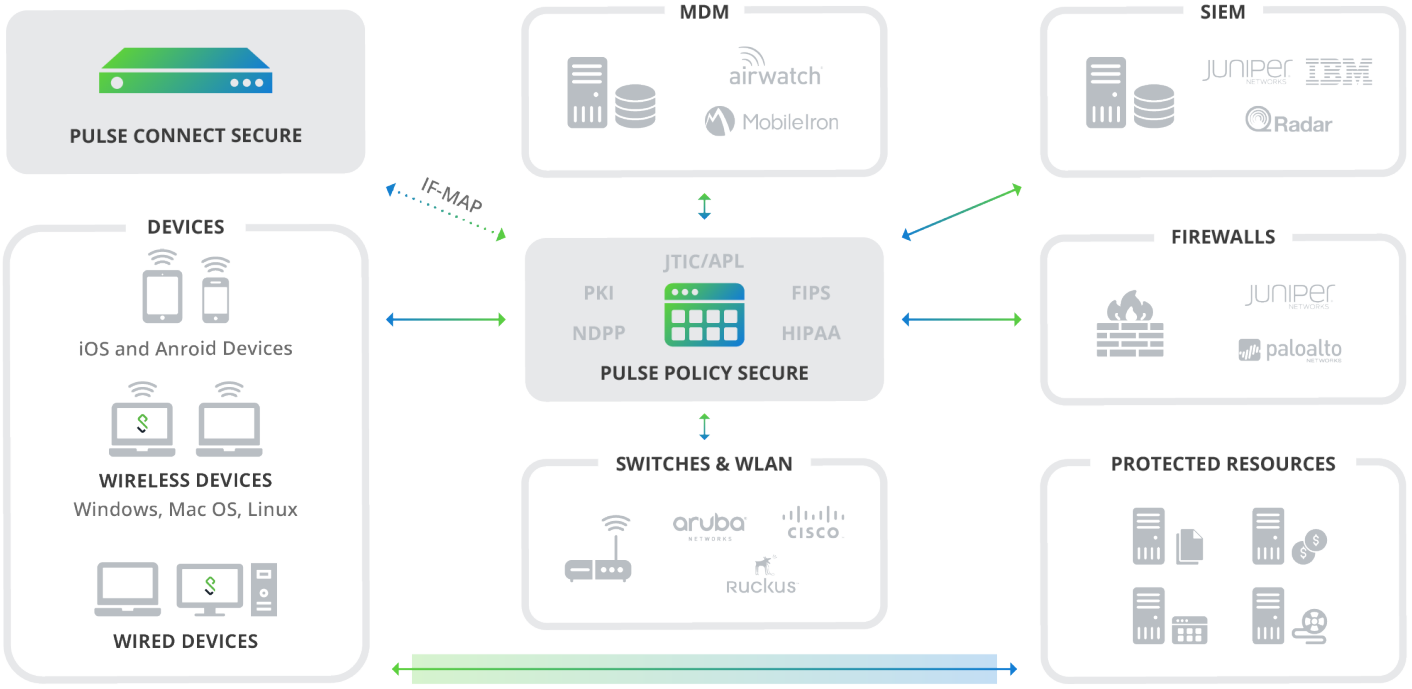
Offers a coordinated cross-platform network collaboration among parts of the IT infrastructure from asset and configuration management to SIEM.

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.



How does it work

Pulse Policy Secure delivers simple, secure network, and application access control with a standards-based, granular solution that provides secure access based on context (user identity, device type, integrity, and location). Policy Secure supports phased deployments and can scale to support global distributed organizations. Policy Secure uses three core components; Appliance (Pulse PSA Series, MAG Series or Virtual Appliance), Pulse Client (or Clientless), and Policy Enforcement Points (wireless access points, switches, and/or firewalls). In conjunction 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, offering self-registration or sponsor registration, with 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 reduce operator risk via centralized policy platform to define and apply context-aware secure access.

Wizards and templates

Reduce complexity and cost of deploying and maintaining a NAC solution to address DISA guidelines and recommended cybersecurity frameworks by DoD, NIST, and JTIC.

Unified client for remote and onsite access

Single client, with host-checking capabilities, to deliver a seamless secure access experience while addressing compliance enforcement.