Pulse Secure®

Pulse Policy Secure and Great Bay Software

Real-time, Contextual Visibility for Comprehensive NAC Deployments

✓ **Automate Real-time Discovery of All Connected Endpoints**

✓ **View Real-time and Historical Endpoint Data**

✓ **Unify the Authentication of All Connected Endpoints**

Continuous Visibility and Assurance of Any Endpoint for Network Performance and Security

6.4 billion connected things are in use worldwide in 2016*. IT administrators need automated solutions to discover and document all network-attached endpoints, managed as well as unmanaged. Since every endpoint must be discovered, located, and provisioned prior to being authenticated on the network, many enterprises have stalled authentication projects yet face network blind spots. Great Bay Beacon offers a comprehensive real-time inventory of every connected endpoint and makes endpoint management effortless.

The combination of Great Bay Beacon and Pulse Policy Secure offers comprehensive, context-aware network access control delivering automatic classification, authentication, and real-time monitoring of endpoints to support BYOD and IoT for the enterprise.

Challenges

Secure Company-Owned Endpoints Including IoT

Generates an automated real-time inventory of all endpoints, including those known to be non-responsive hosts, and automatically classifies them.

Simplify and Streamline BYOD and IoT Initiatives

Ensures every endpoint connecting to the enterprise network—even personal mobile devices that have not yet been provisioned and IoT devices—is identified, authenticated, and dynamically assigned an appropriate role with Pulse Policy Secure.
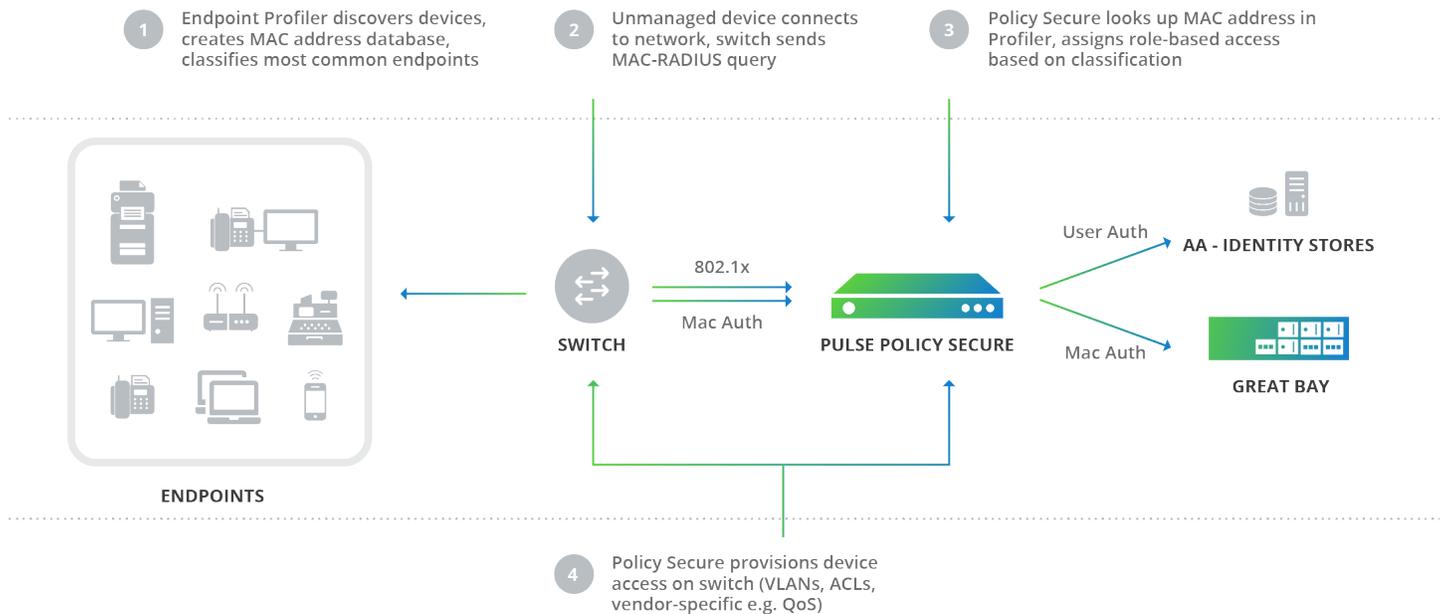
Mitigate Network-Threat Events

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

* http://www.zdnet.com/article/internet-of-things-finding-a-way-out-of-the-security-nightmare/

Real-Time, Context-Aware Network Access Control

Pulse Policy Secure and Great Bay offer a comprehensive solution to streamline context-aware access and information sharing for trusted endpoints and real-time remediation for non-compliant endpoints.

1. Endpoint Profiler discovers devices, creates MAC address database, classifies most common endpoints

2. Unmanaged device connects to network, switch sends MAC-RADIUS query

3. Policy Secure looks up MAC address in Profiler, assigns role-based access based on classification

ENDPOINTS

SWITCH

802.1x

Mac Auth

PULSE POLICY SECURE

User Auth

AA - IDENTITY STORES

Mac Auth

GREAT BAY

4. Policy Secure provisions device access on switch (VLANs, ACLs, vendor-specific e.g. QoS)

Benefits

Automated real-time discovery of endpoints

Eliminates the need for manually discovering and documenting network-attached endpoints. Automatically assigns a profile based on device type classification to all connected endpoints, providing increased visibility for the IT administrator.

Real-time and historical views of endpoints

Offers a better understanding of the state of all network-connected endpoints with on-going mining and leveraging of device location, previous addressing, and behavioral attributes and data.

Unified authentication of endpoints

Centralizes authentication, dramatically reduces NAC deployment time, and facilitates the mobility of networked devices and users that today's businesses demand.

Addresses regulatory and government requirements

Uniform, cross-platform network collaboration between Pulse Policy Secure and Great Bay Beacon enables discovery and appropriate action against rogue devices, spoofed endpoints, and other policy violations.