PULSE TECHNICAL SPECIFICATIONS

Wireless Spectrum:

- 802.11 a/b/g/n/ac
- Bluetooth 4

Information Captured

- IP/MAC Address
- Operating System
- Open Ports
- Running Services
- Wireless AP/BSSID & ESSID
- Wireless encryption
- Profiling of Wireless Clients
- Device Manufacturer
- Discoverable Bluetooth
- Wireless Client Probe Requests

Tools Available

- Kali Linux stack
- Custom scripts determined by the user

Pwnie Express provides threat detection of the billions of wireless and wired devices in and around your workplace. By automating wireless and wired device detection, Pwnie solutions continuously detect the devices on or around your network that are open pathways for attackers. Pwnie arms your security team to win the BYOD battle with the ability to detect and fingerprint any device, from phone to thermostat, in order to prioritize your security response, reduce alert fatigue, and provide situational intelligence.

See all the things you're missing at pwnieexpress.com or @PwnieExpress.

PROFESSIONAL SENSOR

Hardware

- Processor: 1.8GHz Intel i3
- Memory: 4GB DDR3
- Disk Storage: 32GB SSD
- Onboard I/O: 1x Gigabit Ethernet, 2x USB ports, 1x HDMI
- Dimensions: 7.7" x 1.5" x 5.2"
- Weight: 6 lbs

Wireless

- Onboard high-gain dual-band 802.11 a/b/g/n wireless supporting packet injection & monitor mode (with detachable antennas)
- Onboard high-gain Bluetooth supporting packet injection & monitor mode (with detachable antennas)

STANDARD SENSOR

Hardware

- Processor: 1.1GHz dual-core Intel Celeron
- (2 threads, 64-bit)
- Memory: 2GB 1600MHz DDR3
- Disk Storage: 32GB mSATA SSD
- Onboard I/O: 1x Gigabit Ethernet, 3x USB ports, HDMI
- USB-Ethernet adapter for second Ethernet interface
- Dimensions: 4.6" x 4.4" x 1.5"
- Weight: 5 lbs

Wireless

- Onboard high-gain dual-band 802.11a/b/g/n wireless supporting packet injection & monitor mode (internal antenna)
- Onboard Bluetooth supporting device scanning & monitor

rev20181008

Find the devices putting your company at risk

DETECT, ANALYZE AND RESPOND TO ROGUE, MISCONFIGURED, AND UNAUTHORIZED WIRELESS AND WIRED DEVICES

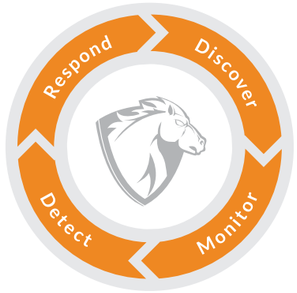
Devices — phones, laptops, tablets, printers, watches, thermostats, fitness trackers, and now even drones — represent the fastest growing threat surfaces in the enterprise. It used to be that IT owned the network and the devices connecting to the network, but with the growing openness of IT, security teams are now responsible for securing their business from devices they don't own.

Every device, whether actually connected to your network or simply near it, expands the threat surface well beyond the control of your current security tools. These devices are in the hands of the employee connecting to your network with an unsecured Android phone, the unknown contractor walking through a branch office with an unauthorized tablet, and the malicious actor who placed a rogue hacking device in the lobby of headquarters.

How do you control these devices that are putting your business at risk? It starts with the visibility to see and assess all the devices in your distributed enterprise, and the ability to respond to these devices, all without having to place any agents or controls on the device itself.

PULSE FROM PWNIE EXPRESS: Real-time wireless and wired device threat detection

The Pulse security platform lets your security teams easily detect and respond to rogue, misconfigured, and unauthorized wireless and wired devices in your enterprise. The SaaS solution provides centralized management to automatically detect, monitor, fingerprint, analyze, and alert on the behaviors of all these devices, whether found at headquarters, a field location, or a branch office. Pulse works seamlessly with the security tools you already have in place, while amplifying and accelerating your people and security controls. Pulse is the only real-time wireless and wired device detection solution, providing broad-spectrum device visibility and awareness covering BYOx/mobile, Wireless, Blue.tooth, wired, and other network-enabled devices



73% of IT professionals consider it likely that a company will be hacked through a connected device.

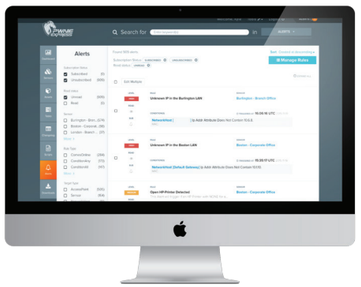
~ ISACA

www.pwnieexpress.com 1-855-793-1337

PULSE TECHNICAL SPECIFICATIONS

Threat Response

In an era of security alert fatigue Pulse helps by monitoring, alerting, and prioritizing only your security policies, security infrastructure, and critical controls. Our rules library is fully customizable and can be set up to continuously monitor devices, alert to changes in known devices, and then alert directly to your team or via integration with your SIEM/WIPs tool.

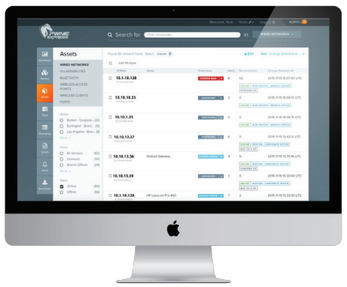


Discover & Fingerprint

Pulse continuously discovers, in real-time, all wired, WiFi, and Bluetooth devices in the vicinity of each of your organization's locations. Our intuitive user dashboard serves this informaton up for your security team to not only gain device visibility, but to then make immediate decisions on next steps.

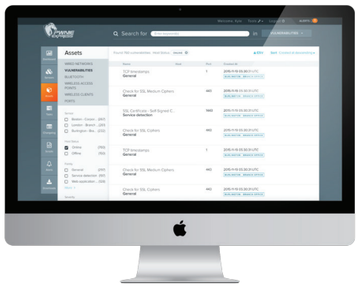
Threat Detection

The Pulse integration is futher exemplified with our rapid response capabilities allowing your team to track and disable devices from your network either directly or via your SIEM/WIPs tool. Additonally, the system is built with interactive reporting to tell the full story of your device security environment.



Monitor & Audit

Pulse then identifies and audits the device to provide immediately actionable data that includes a comprehensive list of devices, behaviors, and even historical information to help recognize noncompliant, misconfigured, or unauthorized devices that may pose an immediate threat to your organization.



51% of IT professionals say they are not aware of its organization's connected devices.

~ ISACA

Minutes After Deployment: What You'll Find

The Pulse distributed architecture detects all wired, wireless, and Bluetooth devices across your entire organization and alerts for unauthorized, vulnerable, rogue, and suspicious devices and access points. Plug-and-play sensors are deployed across your organization and connect back to our SaaS console that provides the dashboards, reporting, alerting and centralized management. Sensors come pre-configured and our plug-and-play technology means deployment is done in a matter of minutes, providing you immediate visibility and detection capabilities.

Shadow IT and High-Risk Bring Your Own Everything (BYOX)

- Unauthorized Personal Devices in Violation of Policy
- Corporate-Sponsored BYOD Hardware
- Devices in Default, Misconfigured, or Vulnerable State

Vulnerable IOT Devices

- Wireless/Mobile Devices Roaming from Corporate Approved to "guest"/unauthorized Wireless Access Points (APs)
- Wireless/Mobile Devices Connecting to Open, Unencrypted Third Party Wireless Networks
- Vulnerable, Default-state, or Misconfigured Printers
- Default-state Wireless APs
- Default-state Network Equipment

Purpose-Built Malicious Hardware

- Purpose-built, Application Specific Devices Designed to Capture Passwords, Credit and Debit Card Numbers, PINs, Keystrokes and Confidential or Proprietary Data
- Devices Designed to Breach WiFi Networks, Wireless APs, Wireless/Mobile Client Devices, and Bluetooth Devices
- Devices Built to Compromise Cellular Networks
- Devices designed to attack or imitate other commonly used RF Technologies

67% of workers already use their personal devices in the workplace.

~ Microsoft

GETTING STARTED

Deploying the Pulse platform is a simple, plug-and-play process of adding peconfigured sensors to desired offices and locations and logging into the console.

1. Determine Pulse and Sensor Specifications

- HQ, Remote, Branch
- Pulse subscription priced per sensor

2. Device Sensors Shipped

- Pre-configured sensors
- Plug-and-play into existing infrastructure

3. Pulse Activation

- Immediate asset detection and assessment
- Reduces or eliminates cost of on-site assessments
- Offset costs of vulnerability scanning and penetration testing
- Visibility to quickly enforce device policies

Ten Minutes to Immediate Value

Real-Time Discovery & Alerting

- Immediately and continuously assess

Remote Security Assessment

- Dramatically reduce vulnerability assessment costs across distributed enterprise from centralized location

Cyber & Physical Incident Response

- Accelerate IR between both cyber and physical security intrusions