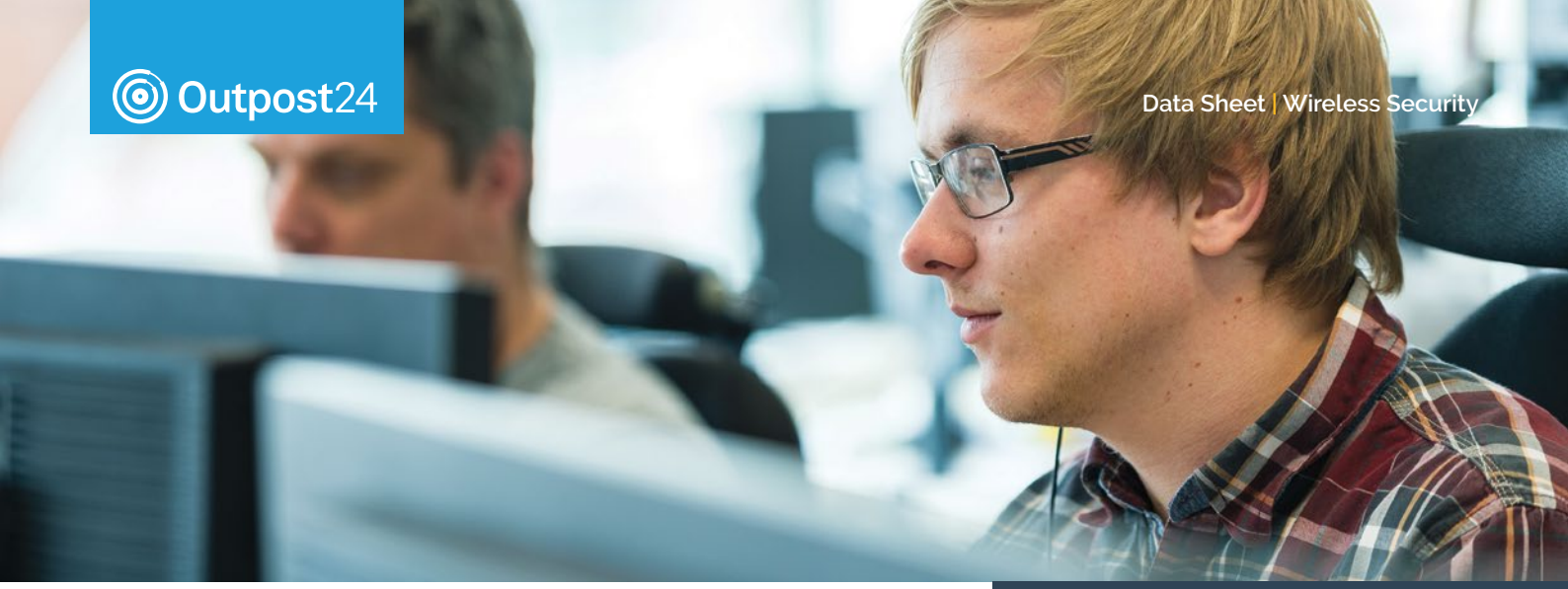


Wireless Network Security Assessment

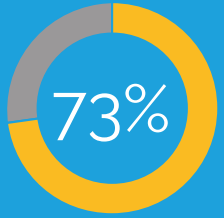
Stay ahead of wireless threats and prevent rogue devices from disrupting your business operations

In the race to speed up business efficiency, reduce costs and improve IT services, rogue devices including phones, tablets, watches, laptops and drones are being deployed and used at a pace that challenges even the most secure networks. Increasing the threat of unauthorized Wi-Fi access, as hackers look to exploit weak access points to break in and disrupt your business.

These devices could come in many forms, the majority aren't malicious and are in the hands of trusted colleagues. However, illicit activities could originate from an unknown contractor walking through a branch office with an unauthorized tablet, and the malicious actor who placed a previously undetectable rogue hacking device in the lobby of your headquarters. This poses a huge threat to your business, however it's becoming much easier to secure what you don't know about with a wireless security solution.

Outpost24 has a solution, Pwn Pulse, which gives you maximum visibility of 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 devices themselves.

Pwn Pulse works seamlessly with the security tools you already have in place, while amplifying and accelerating your people and security controls. Pwn Pulse is the only real-time wireless and wired device detection solution, providing broad-spectrum device visibility and awareness covering BYOx/ mobile, wireless, bluetooth, wired, and other network-enabled devices.



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

When to improve your wireless detection security:

Detect and protect your business against rogue, misconfigured, and unauthorized wireless devices on or around your network airspace

Get full control and visibility of Wi-Fi and bluetooth access points through a centralized interface and automatically monitor all devices and be alerted to malicious activity in real time

Protect your business against wireless attack at multiple locations across your headquarters, field locations, or branches

Reduce your wireless attack surface with seamless integration with your network security tools to amplify and optimize your security processes

Access real-time wireless and wired device detection alerts, enabling you to stay ahead of the latest possible threats

How Pwn Pulse Works

Fully automated threat detection from identification to response in one single view.

PWNIE EXPRESS
an Outpost24 company

Threat Response

In an era of security alert fatigue Pwn Pulse helps by monitoring, alerting, and prioritizing your security policies, security infrastructure, and critical controls.

Discover & Fingerprint

Pwn Pulse continuously discovers, in real-time, all wired, Wi-Fi, and bluetooth devices in the vicinity of each of your organization's locations.

Threat Detection

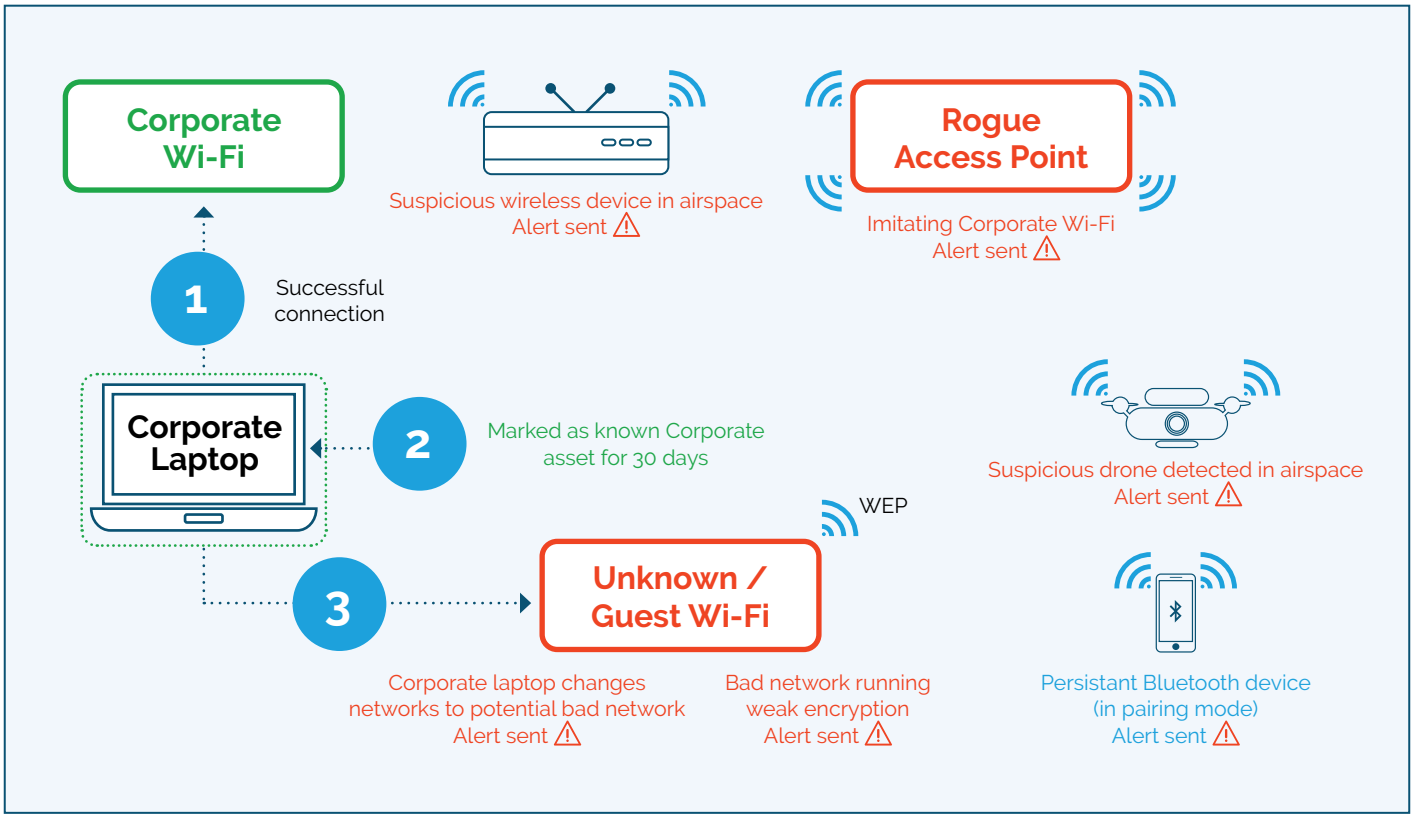
The Pwn Pulse integration is futher exemplified with our rapid response capabilities allowing your team to track and disable devices from your network either directly or via your SIEM/WIPs tool.

Monitor & Audit

Pwn Pulse then identifies and audits the devices to provide real time actionable data that includes a comprehensive list of devices, behaviors, and even historical information.

Pwn Pulse monitored airspace

Pwn Pulse has picked up a known corporate laptop on the corporate Wi-Fi which is marked as safe. Pwn Pulse has detected threats and alerted the user to the unknown/ rogue devices including a rogue access point, drone and a suspicious wireless device.



Key:
Safe and known Wi-Fi and device
Rogue access point and unknown devices detected

Alerts sent via email or via platform

10 Minutes to Immediate Value

Real-Time Discovery & Alerting

Discover all IT and IoT devices on your network and in the surrounding air space to reduce risk exposure.

Cyber & Physical Incident Response

Accelerate IR between both cyber and physical security intrusions

Enterprise Sensor Management & Reporting

Manage all your sensors from one location from one easy to use interface

Identify threats in real time:

Pwn Pulse is available through an on-premise wireless sensor (hardware) and a SaaS interface on a subscription basis. Once set up, the wireless sensor detects unknown Wi-Fi access points and bluetooth devices open for pairing. You will be alerted in real time so you can keep users on approved access points while keeping unauthorized devices off your network.

The sensor can also be used as a remote penetration testing device. Using it in this way will enable Outpost24 to deliver internal application security tests such as SWAT and Snapshot.

The solution comes pre-configured and our plug-and-play technology means deployment is done in a matter of hours, and minutes after that your centralized console will be detecting:

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 Wi-Fi 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

Getting Started

Deploying Pwn Pulse is simple, plug-and-play and add your configured sensors to your desired offices and locations via one trusted source.

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 and time of on-site assessments
- Strengthen vulnerability scanning and penetration testing
- Visibility to quickly enforce device policies

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

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)

We provide threat detection of the billions of wireless and wired devices in and around your workplace. By automating wireless and wired device detection, our solutions continuously detect the devices on or around your network that are open pathways for attackers. We arm 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 outpost24.com/wireless-security

> Pwn Pulse is the only solution that meets our needs. I looked at the leading Network Access Control (NAC) and WIPS/WIDS solutions, and they couldn't touch Pwnie Express when it comes to monitoring and securing our PCI wireless network and the devices that connect to it.

Mark Abbott
Group IT Director of One Hospitality

Discover our full stack security assessment solutions at **outpost24.com/wireless-security**

Outpost24 Headquarters
Skeppsbrokajen 8
SE-371 33 Karlskrona, Sweden
Phone: +46 455 612 300
info@outpost24.com

Outpost24 US
50 South Main Street, Suite 200
Naperville IL 60540
Phone: +1 (630) 352 2283
info@outpost24.com