Classification – The Critical Missing Aspect of WIPS

Table of Contents

Contents

Introduction

The proliferation of Wi-Fi across the globe has created an attractive opportunity for cyber attackers to snoop, steal, and infect unsuspecting users' data and systems. As of the publication of this document, there are over 300,000 videos on YouTube explaining how to hack Wi-Fi users with simple-to-use but highly powerful tools easily found online, making it no surprise that wireless intrusion prevention is a top consideration for business owners deciding when and how to implement a Wi-Fi solution. Wi-Fi vendors around the globe have responded with the introduction of Wireless Intrusion Detection Systems (WIDS) and Wireless Intrusion Prevention Systems (WIPS). In fact, there are so many solutions out there that it has become difficult for even the most security-savvy buyers to know which solutions are the most effective. This paper will simply outline the key components of an effective WIPS solution, arming business owners with the information they need to make informed purchasing decisions.

Wireless Intrusion Prevention Systems – What and Why

Cyber criminals commonly deploy rogue and unauthorized devices in corporate environments in an attempt to intercept and steal corporate data. A Wireless Intrusion Prevention System, or WIPS, is an essential layer of protection for wireless networks that store or transmit sensitive data. WIPS are intended to enable network admins to defend their airspace from unauthorized devices, denial-of-service attacks, rogue APs, and much more.

Simply put, a complete WIPS solution must provide effective and reliable device and access point (AP) detection, classification, and prevention.

- Detection – The ability to discover all devices (including smartphones, tablets, laptops, etc., and any connected devices such as multi-function printers) and access points in your airspace.
- Classification – The ability to quickly and accurately classify each access point and device as authorized, external, or potentially harmful (rogue).
- Prevention – The ability to immediately quarantine any rogue device or access point from your airspace to prevent malicious activity before it occurs.

The advancement of wireless security techniques has made device and AP discovery and prevention pretty standard; however, the classification aspect of the process is where the problem currently lies. The ability to accurately determine if a device or access point on your network is truly malicious or just external is critical to effective mitigation. Wrongful classification of an external access point or device as rogue and taking action to isolate that device or access point can have a number of negative consequences ranging from reputation damage to legal implications.

TIP

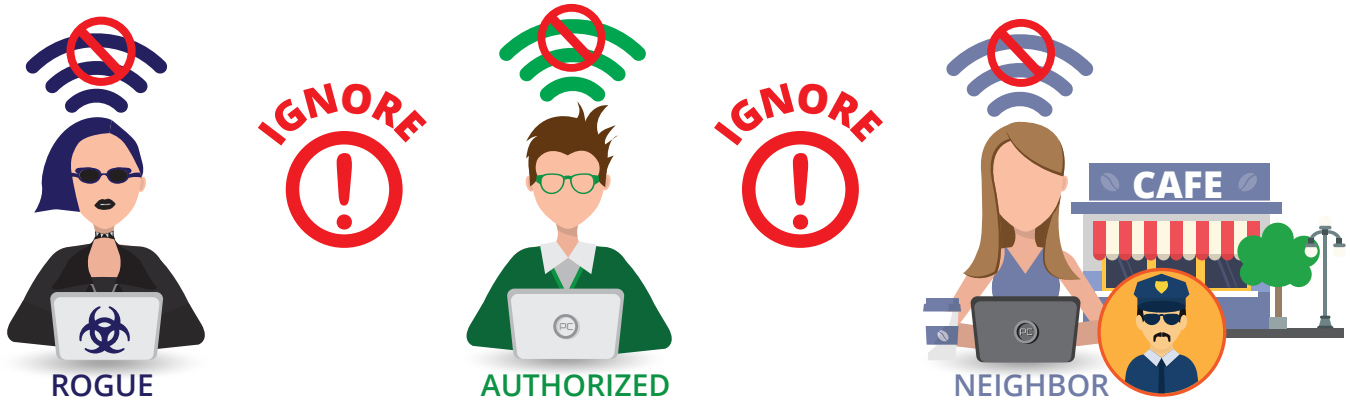
The difference between generic detection and the granular detection that enables prevention is accurate classification – make sure your WIPS provides accurate classification!

The Impact of Wrongful Classification

A good WIPS solution will detect and provide visibility into all access points and devices on or around your airspace. By the nature of how Wi-Fi works, even if a device or access point is not directly connected to your network it will show up as being in your airspace. It is very important that a business is able to not only see that device but understand if it is truly connected or just within range before they take action against that device or access point.

For example, in a crowded city environment, there can be dozens of businesses all broadcasting Wi-Fi within a single city block. It is important that each business is able to manage the security of their Wi-Fi network without interfering with users and service of their neighbors. Interfering with a neighboring Wi-Fi network is not only inconvenient for that business owner, it is illegal.

This is why it is critical for a WIPS solution to be able to not only find all devices and access points in their



airspace, but to also know the difference between truly rogue devices or access points and neighboring (or external) devices or access points. Without the confidence in the classification aspect of WIPS it is impossible to activate the prevention aspect of the tool. This is evidenced by the alarmingly high number of businesses who have downgraded their WIPS solutions to WIDS solutions, only leveraging the detection aspect of the system and then relying on manual classification of each device or access point before action is taken. While manual intervention techniques do ultimately result in removal of harmful access point and devices from the network, it is not immediate remediation of the threat and hours, days, even weeks can go by before the threat is removed.

Unlocking the Power of WIPS – Accurate Device and AP Classification

Understanding the under-publicized weakness of most WIPS offerings enables decision makers of all businesses to quickly hone in on the right questions to ask when making a Wi-Fi purchasing decision. First, make sure that the solution includes WIPS, then dig into how that system handles classification. Almost all WIPS solutions are created equal when it comes to device and access point detection and the ability to respond, but very few can accurately classify. Without accurate classification the prevention aspect of WIPS will no longer be immediate and become a manual process for an IT department that, for some businesses, may or may not exist.

TIP

When evaluating a Wi-Fi solution, ask to speak to a current customer and ask if they use automated prevention and how accurate the device and AP classification is!

WatchGuard Wi-Fi Cloud – Putting the Classification in WIPS

WatchGuard offers a full suite of Secure Wi-Fi solutions including the WatchGuard Wi-Fi Cloud, a secure, scalable, and feature-rich Wi-Fi management platform and a family of high-performance, cloud-ready access points.

Powered by an extensive portfolio of patented wireless intrusion detection and prevention techniques, WatchGuard WIPS provides 24/7 visibility into and complete control over wireless activity. Using patented Marker Packet techniques, WatchGuard WIPS automatically and quickly classifies wireless devices detected in the airspace as Authorized, Rogue, and External.

As a result, it eliminates false alarms and saves security administrators the effort of defining complex rules to identify rogue wireless devices or manually inspecting devices.

This is unlike the error-prone device classification integrated into most WLAN solutions, which rely on slow and inconclusive CAM table lookups and MAC correlation, signatures, or passive wired network sniffing. WatchGuard's advanced threat detection is the only WIPS solution that can safely and automatically shut down unauthorized access points and clients, without running the risk of interfering with neighboring wireless networks. Visit **www.watchguard.com/wifi** to learn more about WatchGuard's family of Secure Wi-Fi solutions.

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, secure Wi-Fi, and network intelligence products and services to more than 75,000 customers worldwide. The company's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for distributed enterprises and SMBs. WatchGuard is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com.

For additional information, promotions and updates, follow WatchGuard on Twitter @WatchGuard, on Facebook, or on the LinkedIn Company page. Also, visit our InfoSec blog, Secplicity, for real-time information about the latest threats and how to cope with them at www.secplicity.org.

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 www.watchguard.com