Business white paper

Put wireless security worry to rest

Safeguard your wireless network with HP Wi-Fi Clear Connect integrated intrusion detection

Executive summary

A quick tour of your offices will tell you all you need to know. You'll see colleagues in corridors, in meeting rooms, or at their desks typing away at their tablets, smartphones, or laptops—perhaps you'll see someone using all three types of devices at the same time. There is a near-universal need to be productive anywhere and at anytime. And with the popularity of the bring-your-own-device (BYOD) movement, your organization's mobility needs are growing fast. Just as Wi-Fi has quickly become a must-have, built-in security protection for wireless LANs (WLANs) is also a necessity.

As your wireless needs grow, so too does your exposure to wireless security threats. HP Wi-Fi Clear Connect solution provides integrated wireless threat detection with real-time reporting. With threat detection built into your high-performing Wi-Fi network, you can stop worrying about security so you can focus on enabling your colleagues to be even more productive.

The joy of mobility often overshadows some very real consequences: security threats. Wireless brings ready access to the applications and information that your workers and you need to be productive anywhere, anytime. Employees are clamoring to use their personal laptops, tablets, and smartphones for business, but along with the many positives, a BYOD initiative can mean an increase in malware and security risk.

WLANs are subject to many of the same threats as wired networks, as well as some specific attacks that take advantage of the radio frequency (RF) medium. Attackers often try to compromise the WLAN first, and then use the wireless as a jumping-off point to attack the wired network, where they can go on to steal sensitive data. Your WLAN needs built-in detection of wireless security threats so that you can focus on running your business.

The risk is real

Small and midsize businesses are often in a difficult position when it comes to IT security. Many business owners have long believed they could fly under the radar of cyber-criminals, but organizations of all sizes are being targeted today. In many ways, the servers of a small retailer, a doctor's office, or an elementary school can be more inviting than the well-protected data centers of large enterprises.

The nature of cybercrime has changed as well. Stealing sensitive data or intellectual property is a for-profit business, but attacks are also launched as a form of social protest. The person tapping away at the keyboard may not be in a distant land, but could be a disgruntled former employee or the grassroots operation of a political movement.

Security breaches can be the result of insiders, as employees can inadvertently or intentionally open the door to attack. A worker could bring a wireless access point (AP) into the office, and while the wireless connectivity is a convenience, information passing over an unsecured network could be exposed to anyone nearby.

An outside attacker can gather your organization's sensitive data by introducing an unauthorized (or rogue) AP into or near your offices. The rogue AP can be used to trick your laptops, tablets, and other Wi-Fi clients into associating with it. Rogue devices can spoof the addresses of your authorized network devices to hide from view.

An attacker outside of your building could search for holes in your Wi-Fi network security with scanning software and a laptop or tablet. Denial-of-service (DoS) attacks are serious as well, as the massive influx of traffic can overwhelm your network, rendering it useless for productive work.

Safeguarding your WLAN makes good business sense, and it is often a regulatory requirement as well. If your organization handles credit or debit transactions, you are probably subject to the Payment Card Industry Data Security Standard (PCI DSS). PCI is commonly associated with the retail industry, but it applies more broadly to anyone in the chain of payment card processing. That means retailers, hotel gift shops, and school cafeterias that process credit and debit card transactions may be subject to PCI compliance.

PCI applies even if your organization doesn't have a WLAN, but processes credit and debit transactions. According to the standard, you must still scan for rogue APs. If you use WLANs, whether to send email or cardholder data, you must meet increasingly stringent security requirements to comply with PCI.

Security is a major concern for education, and threats can come from insiders, such as students, as well as outside attackers. In addition to protecting the wireless infrastructure, schools must protect the students. Many K-12 schools take a strong approach to security to comply with laws such as the Children's Internet Protection Act to protect students from inappropriate content online.

Connect with confidence

With HP by your side, you can connect with confidence. You can count on HP Networking's MSM Series wireless LAN solutions to deliver the performance you need to support the growing legions of laptops, tablets, and smartphones in your organization. HP Wi-Fi Clear Connect software automatically optimizes WLAN performance, detects security threats, mitigates RF interference, and simplifies management. You get a better performing, more reliable Wi-Fi network at a lower cost.

HP Wi-Fi Clear Connect safeguards the WLAN against wireless threats with an integrated wireless intrusion detection system (WIDS). The WIDS detects common threats, including denial-of-service attacks as well as unauthorized APs and clients. Wireless threat detection is built-in, without additional license fees and allows administrators to deploy APs as dedicated sensors or in a hybrid mode that provides both sensor functionality and client services.

HP Wi-Fi Clear Connect integrated IDS is supported on HP MSM410, MSM430, MSM460, MSM466, and MSM466-R Access Points as well as MSM720, MSM760, and MSM765zl Controllers.

Table 1. Wi-Fi Clear Connect Firmware v6.0 platform support

	MSM720, MSM76x	MSM410	MSM430, 46x
Radio Resource Management	X	X	X
Spectrum Analysis	X		X
Integrated IDS (requires Premium Mobility option)	X	X	X

Three flexible options

You can choose the level of threat detection that's right for your organization. With HP Wi-Fi Clear Connect your MSM WLAN can provide Wi-Fi client services and IDS threat detection at the same time, or operate in a dedicated mode.

Three flexible configuration options are available for IDS:

- **AP mode:** The AP radio provides both Wi-Fi client services and threat detection on the operating channel only. The advantage is that threat detection is faster than in the dedicated IDS mode, although other non-operating channels are not scanned, so a rogue may hide.
- **Dedicated IDS mode:** The AP radio provides dedicated scanning on both 2.4 GHz and 5 GHz bands, and it does not provide Wi-Fi client services. You can limit scanning to one band or the other.
- **Hybrid mode:** The AP radios provide client services and IDS simultaneously by using a time-slicing method to scan non-operating channels. In hybrid mode, threat detection in the operating channel is fast, but off-channel threat detection takes longer than in a dedicated IDS mode. You can configure how much time to devote to off-channel scanning. Wi-Fi Clear Connect Integrated IDS is set up in hybrid mode by default.

When in hybrid mode, MSM APs minimize the impact of providing Wi-Fi service to clients. When voice traffic is active on the AP, the AP postpones the off-channel scanning so it can minimize the potential for disruptions. The AP automatically resumes scanning if there has not been voice traffic for several seconds.

Wi-Fi security that's right for you

The right option for monitoring depends on your threat environment and compliance requirements as well as your Wi-Fi performance needs. You may choose one approach or mix and match the modes to fit different security profiles.

An overlay approach using dedicated IDS mode might make sense in the higher-risk areas of your organization, such as classrooms or lobbies, or if you want to monitor areas outside your network's Wi-Fi range. In dedicated mode, the APs will spend all of their time scanning for wireless threats. If IPS is needed, then a full overlay solution with dedicated RF sensors is available from HP.

In lower-risk locations, you may choose the time-slicing approach–using hybrid mode–and the APs will perform double-duty for Wi-Fi services and threat detection. You can maximize the investment in your current APs, and still benefit from wireless threat detection. In addition, threat monitoring will take place over the same areas that your Wi-Fi service reaches and not beyond.

The criticality of threat detection should be factored into your choice. The effectiveness of threat detection depends on the ability to hear the wireless traffic that contains the threat. MSM easily detects denial-of-service and other in-channel threats, but other threats, such as the detection of rogue APs, can only be detected by off-channel scanning.

Keeping you up to date with your network

Wi-Fi Clear Connect integrated IDS firmware makes it easy for you to keep a pulse on the health of your WLAN security. Administrators gain visibility into wireless threats, with IDS events reported in real time. If a rogue device is detected, location tracking helps the administrator find the threat in the office.

The firmware includes a new framework for events and alarms that makes it easy to pinpoint all critical, major, and minor conditions on your WLAN. You can quickly drill down to gain detailed information on active alarms. Alarms also generate SNMP traps and can be logged as messages for an external syslog server.

Wi-Fi without worry

Midsize organizations can enjoy the fruits of mobility with the freedom to work anywhere, anytime. With HP's MSM Series WLAN solutions, you can be confident that you can meet your workers' needs for a high-performance WLAN service while mitigating risk and meeting compliance requirements in an affordable way.

To learn more about HP Wi-Fi Clear Connect, please contact your HP account manager or reseller, or consult the following resources:

- Wi-Fi Clear Connect
- HP Mobility Solutions
- HP Networking Wireless Home Page

Mobile by the numbers

- According to a U.K. study, people with email on their smartphones and tablets work two more hours per day—that's 460 hours per year.[1]
- Eighty percent of enterprises plan to increase the capacity of their WLANs in 2013, says Nemertes Research.[2]
- The number of employee-owned smartphones and tablets used in the enterprise will more than double by 2014, reaching 350 million, predicts Juniper Research.[3]
- Gartner predicts that employee-owned mobile devices will be compromised by malware at more than double the rate of corporate-owned devices, through 2014.[4]
- A Ponemon study of cybercrime indicates that cyber attacks have become more common occurrences, with companies in the study experiencing 1.8 successful attacks per company per week.[5]

[1] "Smartphones and Tablets Add Two Hours to the Working Day," The Telegraph, October 2012. telegraph.co.uk/technology/mobile-phones/9646349/Smartphones-and-tablets-add-two-hours-to-the-working-day.html

[2] "Mobile Application Trends," Nemertes Benchmark Report, October 2012. nemertes.com/reports/mobile-application-trends

[3] "Security Issues to Escalate as 350m Employees to Use Personal Mobile Devices at work by 2014," Juniper Research Press Release, August 2012. juniperresearch.com/viewpressrelease.php?pr=330

[4] "Gartner Reveals Top Predictions for IT Organizations and Users for 2013 and Beyond," Gartner, Inc., October 2012. gartner.com/it/page.jsp?id=2211115

[5] "2012 Cost of Cyber Crime Study: United States," Ponemon Institute, October 2012. ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf

Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document

4AA4-5084ENW, February 2013