WatchGuard

Wi-Fi is Easy, **Secure Wi-Fi** is the **Challenge.**

Table of Contents

Wi-Fi Is **Everywhere**

Organizations across all industries are facing increased pressure from customers, vendors, and employees to offer wireless access. While offering this service provides gains, there are multiple areas of consideration for the provider, including mobility, hotspots, IoT (Internet of Things), and the widening cellular spectrum capacity gap.

In this eBook, we'll explore the increasing demand for Wi-Fi, and more importantly, how to secure your wireless network.

Of all **Internet traffic** in the world,

63%

of it will travel over **Wi-Fi** by **2019**[1]

Drivers for Wi-Fi Adoption

Workplace Productivity

With the increase in wireless connection throughput to 802.11ac speed, workers are no longer tethered to an Ethernet cable. Organizations can offer the flexibility of a mobile workspace, while at the same time making no sacrifice to productivity with wireless bottlenecks.

Superior ROI

Traditional wired infrastructure is inflexible and costly to install. Businesses that choose to exclusively offer wired connectivity must cover the cost of wire, wall jacks, and switches, along with the cost of setup and maintenance. As the organization grows and users are added, additional costs are incurred. Offering wireless hotspots is far less expensive, provides greater scalability, and offers the flexibility and efficiency for users to roam around the facility.

Customer Satisfaction and Repeat Visits

Guest Wi-Fi has become a ubiquitous offering across many business sectors. Organizations that choose to provide this service also need to accommodate high speed demands of streaming HD video and music. The hospitality industry is especially dependent on offering Wi-Fi, as travelers rank free Wi-Fi access as their number one criterion in selecting a hotel.

Proximity Marketing

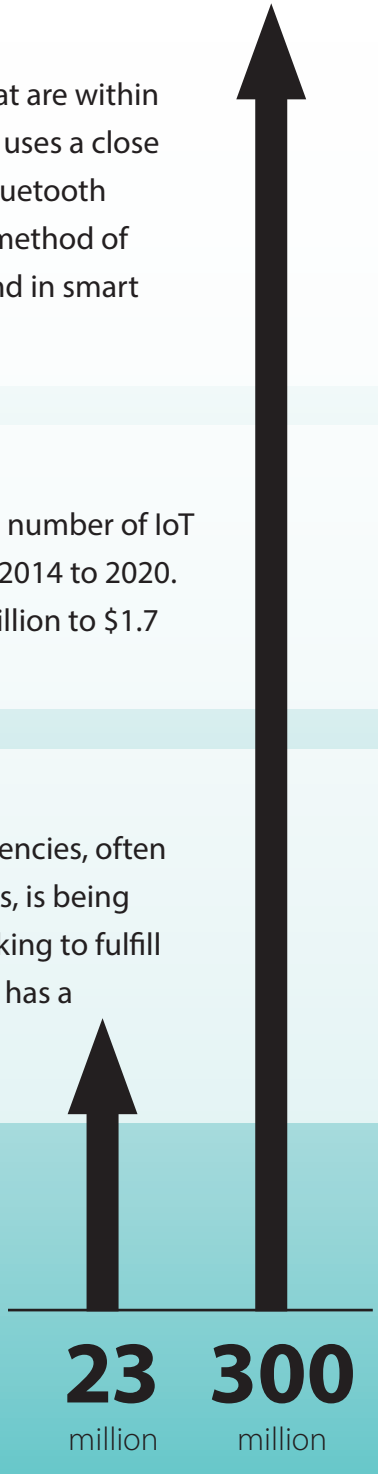
Organizations are quickly adopting new and sophisticated methods of marketing to consumers that are within the vicinity of their physical locations. Technologies include Bluetooth and NFC systems. Bluetooth uses a close range method whereby marketers can broadcast various types of media to consumers that have Bluetooth enabled on their smartphones and tablets. NFC (near-field communication) systems are used as a method of pull-marketing, which can send mobile devices advertisements or special offers, and are often found in smart posters and mobile wallets, such as Apple Pay and Google Wallet.

Internet of Things (IoT)

The amount of "things" connected to the Internet is growing at a rapid pace. IDC estimates that the number of IoT endpoint-connected devices such as cars, refrigerators, and everything in between will triple from 2014 to 2020. The firm predicts that the global IoT market will grow 150% during the same period, from $655.8 billion to $1.7 trillion.

Widening Cellular Capacity Gap

Cellular data providers are investing heavily in the rights to send signals over the air via radio frequencies, often referred to as spectrum. The capacity of each spectrum, which is licensed by government regulators, is being outpaced by consumer demand. In order to fill this growing gap in capacity, data providers are looking to fulfill the demand through Wi-Fi, specifically on the 5GHz ISM band. But, compared to cellular data, Wi-Fi has a very short range. This presents a challenge that can only be met by a mass deployment of wireless access points, creating carrier-grade Wi-Fi networks.



The number of hotspots is predicted by iPass to grow from

23 million in 2014 to almost

300 million in **2018**[2]

Top Seven Threats to Your Wireless Network

1 Wi-Fi Password Cracking

Wireless access points that still use older security protocols, like WEP, make for easy targets because these passwords are notoriously easy to crack.

2 Rogue Hotspots

Nothing physically prevents a cyber criminal from enabling a foreign access point near your hotspot with a matching SSID that invites unsuspecting customers to log in. Users that fall victim to the rogue AP are susceptible to a malicious code injection that often goes unnoticed.

3 Planting Malware

Customers who join a guest wireless network are susceptible to unknowingly walking out with unwanted malware, delivered from bad-intentioned neighboring users. A common tactic used by hackers is to plant a backdoor on the network, which allows them to return at a later date to steal sensitive information.

4 Eavesdropping

Guests run the risk of having their private communications detected, or packet sniffed, by nosey cyber snoops while on an unprotected wireless network.

5 Data Theft

Joining a wireless network puts users at risk of losing private documents that may contain highly sensitive information to cyber thieves who opportunistically intercept data being sent through the network.

6 Inappropriate and Illegal Usage

Businesses offering guest Wi-Fi risk playing host to a wide variety of illegal and potentially harmful communication. Adult or extremist content can be offensive to neighboring users, and illegal downloads of protected media leave the business susceptible to copyright infringement lawsuits.

7 Bad Neighbors

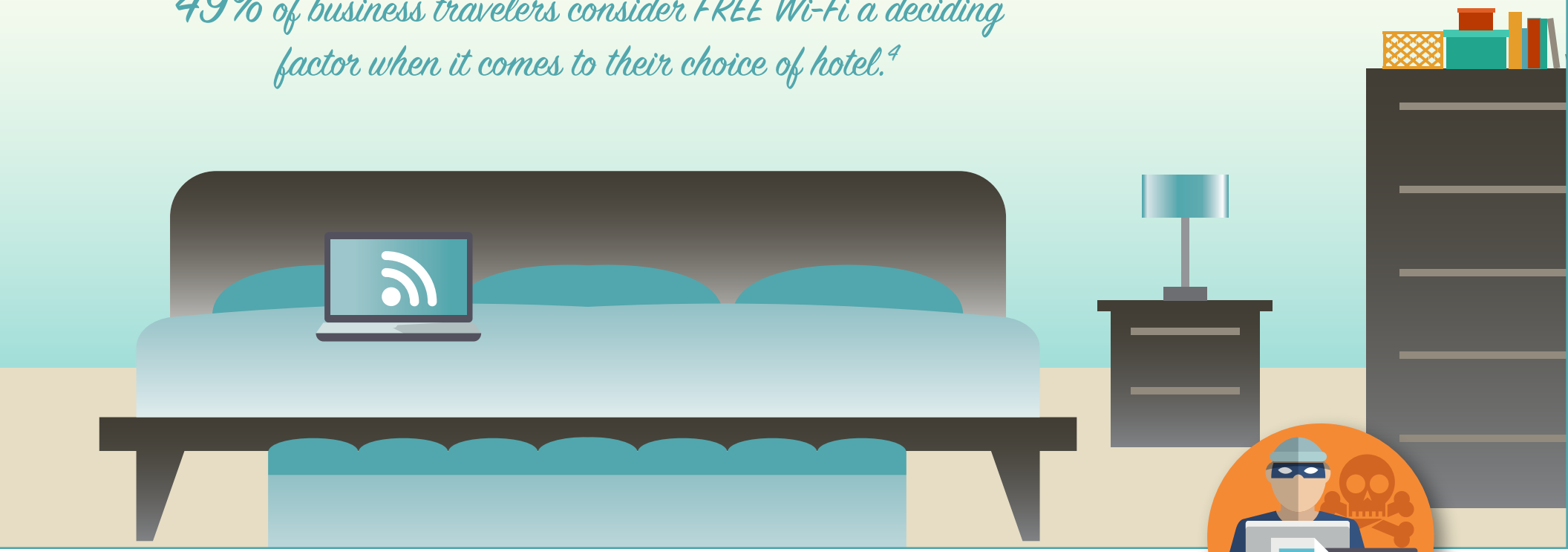
As the number of wireless users on the network grows, so does the risk of a pre-infected client entering the network. Mobile attacks, such as Android's Stagefright, can spread from guest to guest, even if victim zero is oblivious to the outbreak.

Problems Across Key Industries

Retail Concerns

Mobile Point of Sale (POS) systems are becoming increasingly common. Any business that accepts credit cards via a wireless or wired network has a responsibility to secure the storage and transmission of cardholder data. A group of banks developed a standard by which payment information must be secured called PCI DSS, or Payment Card Industry Data Security Standard. This set of guidelines is designed to protect retailers and consumers from theft. Organizations face stiff fines if they fail to meet these guidelines when securing their Wi-Fi hotspots.

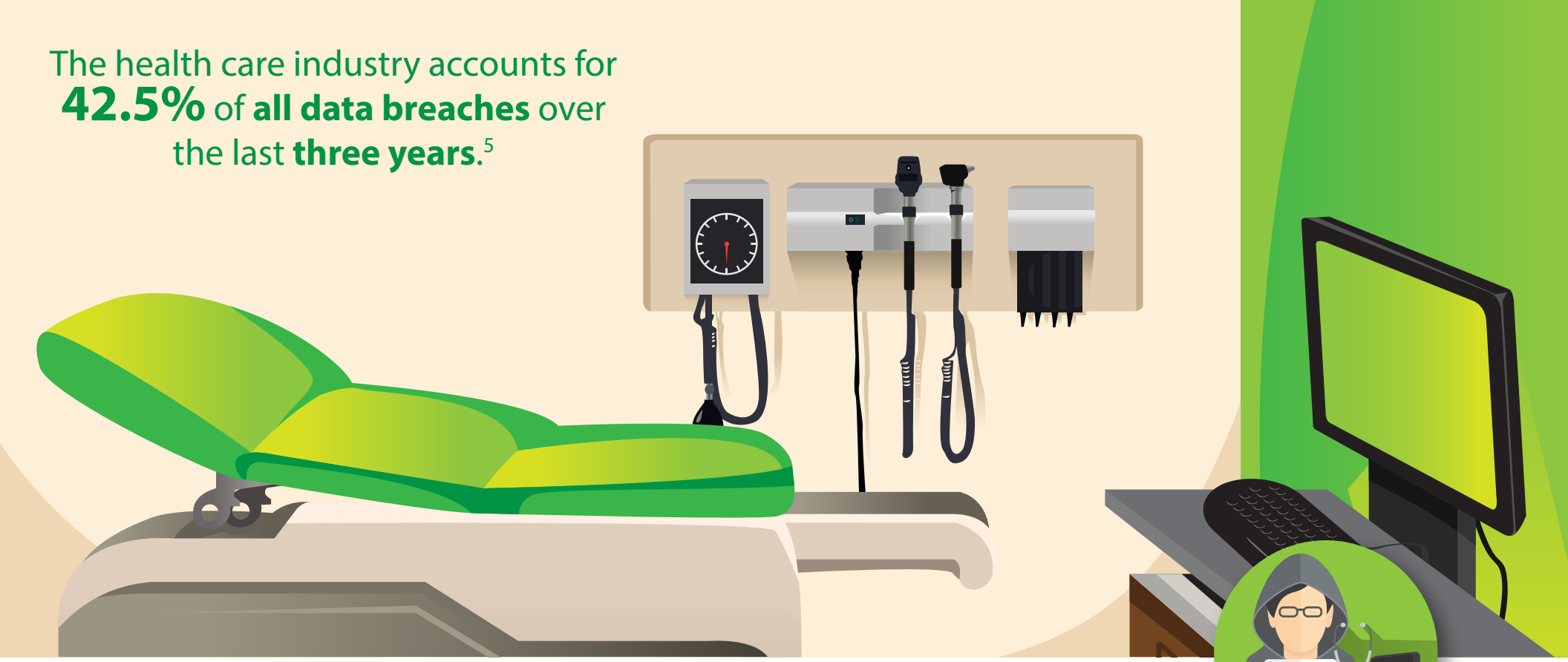
49% of business travelers consider FREE Wi-Fi a deciding factor when it comes to their choice of hotel.[4]



Hospitality Concerns

A Property Management System (PMS) is a software application used by hotels to automate and coordinate multiple business functions ranging from front office to back office operations, including management of guest credit card information. PMS systems also commonly integrate with POS and reservation systems, which results in a high-value target for cyber criminals. Many large hotel chains have recently been victimized due to a breach in the PMS or POS system, resulting in fines, lawsuits, and damage to their reputation. A major challenge for organizations in the hospitality industry is to offer high speed Wi-Fi, but at the same time protect both their guest and corporate resources.

The health care industry accounts for **42.5%** of **all data breaches** over the last **three years**.[5]



Healthcare Concerns

The Healthcare Industry has a unique set of wireless security challenges brought on by the highly sensitive and highly valuable nature of the data being exchanged on the network. HIPAA (the Health Insurance Portability and Accountability Act), along with similar global standards, requires organizations that process patient data to adhere to a strict set of security practices. Various types of medical technology have evolved to exchange data wirelessly, opening a new window of vulnerability. This trend, also known as the Internet of Things, or IoT, has revolutionized healthcare with improved efficiency; however, these devices are the most common target of malicious attacks. The medical devices are typically running older operating system versions that are known to be vulnerable. Healthcare professionals commonly store and access protected health information on mobile devices. Access to customer and patient data over mobile devices offers huge gains in efficiency, while simultaneously increasing exposure unless strong security measures are put in place.

Education Concerns

Mobile devices are transforming education. Tablets are being issued by schools at all grade levels, and students need high-speed wireless access to abundant web-based educational resources. But accessing this wealth of knowledge doesn't come without risks. Schools, especially K-12, require objectionable web content to be filtered. Elementary students are particularly vulnerable to malware because they aren't as familiar with the common traps set by hackers. In addition to external threats, student networks must be segmented from the administrator's network, to minimize the risk of cheating, tampering, and other privacy concerns.

Changes to Implement **IMMEDIATELY**:

WPA2 – Enable the **most current** security protocol.

Strong Password – **NOT** the default password.
Change password regularly.

Know Your Network – Scan for **rogue APs** and **whitelist MAC addresses** when possible.

Narrow the Wi-Fi range – **Limit range** to your areas of operation.

Keep the **firmware updated**!

Step Up to **Enterprise Grade Security**

UTM

Enabling Wi-Fi is easy. Security is the challenge. Top-notch security professionals ensure all traffic on the wireless network runs through a full set of UTM services including AV, IPS, web filtering, spam blocking, application control, reputation lookup, APT blocking, and data loss prevention. Ideally, services should be enabled without sacrificing performance, and for efficiency, everything should be centrally managed in a single interface. Ultimately, the goal is to have industry-leading performance and **best in-class** defenses that make wireless access as secure as using the wired network.

Visibility

Wireless networks are one of the most overlooked security blind spots within any organization. IT security professionals require a solution that offers **visibility** into real-time and historical network traffic, provides **automated reports** that inform stakeholders of key trends and patterns, and allows IT to **analyze wireless coverage** and detects rogue APs.

Management

Misconfiguration of networking equipment is one of the most common causes of a network security breach. By consolidating the management of wired and wireless networks, the risk of misconfiguration is dramatically reduced. Modern IT pros are looking for **complete flexibility in management options**, utilizing the cloud, Windows, the web, and CLI-based systems to enable **maximum security control**.

WatchGuard **Secure Wireless Technologies**

AP100/102/200/300

Customers can enhance or add wireless to an existing firewall by deploying wireless access points. The AP100 is a great fit for smaller wireless networks, where the AP200 and AP300 are perfect for larger and more complex wireless environments. The AP102 is resistant to water and dust, and offers the flexibility of an outdoor deployment.

Wireless T Series Models

Firebox UTM appliances consolidate the most critical security technologies onto a single appliance. Integrating wireless capability in the Firebox T Series allows businesses to extend the best-in-class security technologies to their wireless networks.

WatchGuard Dimension

Many companies make the mistake of offering a Wi-Fi hotspot, and then hoping for the best. Without complete visibility into all network traffic, businesses leave themselves vulnerable to a number of threats. WatchGuard Dimension consolidates real-time and historical wireless traffic into a single source, complete with dashboards and customizable reports, allowing IT staff to establish baselines, spot trends, and put a stop to malicious wireless activity before it becomes a larger threat to the business.

WatchGuard **Secure Wireless Products**

1. *Cisco VNI Global IP Traffic and Service Adoption Forecast, 2014-2019*
2. *http://www.marketwired.com/press-release/ipass-wi-fi-growth-map-shows-1-public-hotspot-for-every-20-people-on-earth-by-2018-nasdaq-ipas-1963515.htm*
3. *https://www.staysafeonline.org/stay-safe-online/resources/small-business-online-security-infographic*
4. *Hotels.com. "Free Wi-Fi Reigns but Wanes as Top Hotel Amenity," May 6, 2015*
5. *USA TODAY. "Another Health Care Data Breach," July 25, 2015*
6. *Websense Security Labs Blog. "Today's Lesson," July 7, 2015*

Every product that WatchGuard creates is built with consideration for the Secure Wireless environment. From network firewalls to secure access points, WatchGuard knows that your business relies on fast and reliable Secure Wireless.

Leveraging WatchGuard's portfolio of secure wireless Technologies, organizations can easily configure, deploy, and manage consistent, enterprise-grade network security and secure wireless across all remote locations without the need for technical expertise at each location with innovative RapidDeploy technology. In addition to providing best-in-class, easy-to-deploy security, the company's actionable threat intelligence platform, Dimension, delivers centralized visibility across an organization's entire network. This visibility is critical for tracking and managing network health, reporting on compliance requirements, identifying and combating possible network threats, and assisting with proactive business decision-making.

www.watchguard.com/securewireless