FORTINET

WHITE PAPER

# Delineating the Cornerstones of a Secure Wireless Solution

## Executive Summary

**Wi-Fi is a popular way to connect to enterprise networks—for both legitimate users and hackers. The newly available WPA3 security protocol makes encrypting a wireless connection easier. However, this still leaves other wireless network vulnerabilities that hackers exploit. Thus, wireless security must be multi-layered, with the ability to segment users and devices, perform a continuous trust assessment of network traffic, identify and monitor Internet-of-Things (IoT) devices, and control network access using strong authentication. These capabilities, which need to be integrated into a security fabric, provide the cornerstones of a secure wireless solution.**

**The number of devices connecting to the WLAN is exploding, with IoT devices a critical factor in the 30% CAGR through 2023.**

**Cyber criminals are targeting Wi-Fi networks due to the amount of data attached to the wireless network, unmanaged IoT devices, and overstretched IT teams that cannot manage all of the devices connecting to the network.**

## Understanding Wireless Security Challenges

Wi-Fi was a niche technology when it was introduced in 1997 and few thought it would have much of a future.[1] Now wireless technologies are estimated to comprise 55% of specialized integrated circuit shipments (ICs) for connectivity, surpassing wired network ICs.[2] At the same time, the global wireless local area network (WLAN) market is predicted to have a compound annual growth rate of 30% through 2023, largely driven by the need to connect a rapidly expanding number of IoT devices.[3] In the case of the latter, one million IoT devices are being added to networks each month.[4]

The growing use of Wi-Fi presents attackers with an attractive target for several reasons. First, the data they seek is likely to be attached to the wireless network. Second, there are often many unmanaged IoT devices on a Wi-Fi network that are "headless" or lacking a user interface, such as temperature sensors, building controls, and security cameras. An IoT environment offers attackers a good place to hide from detection. Third, overstretched IT teams are rarely in a position to know about and manage every device on the network, and many assume that once a device has authenticated and connected to the network, it is safe.

Hackers can draw on several strategies when targeting wireless networks:

### 1. Attack Guest/Legacy Networks

Many companies offer guest networks, which frequently grant open access or have easy-to-defeat security, such as an openly posted pre-shared key (PSK). While guest networks are typically separated from the corporate network, they provide a launch point for attacks, enabling hackers to test the strength of network segmentation (if it exists). Some corporate wireless networks also serve legacy devices such as point-of-sale (POS) systems, HVAC controls, and medical systems that are critical to the host organization's mission. However, as they lack adequate embedded security, they serve as additional targets.

### 2. Compromise an Approved Device

More vulnerabilities develop when employees are on the go: 61% connect their company-owned laptops to open public networks.[5] In these circumstances, hackers can either compromise the data the device is sending or load malware onto the device itself. When the employee reconnects to the network, the attacker gains access to company resources.

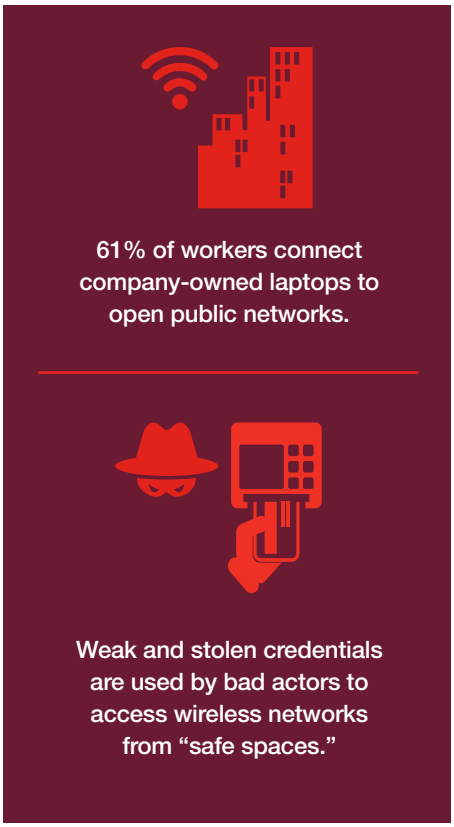
### 3. Compromise an IoT Device

IoT devices such as sensors are good targets. They are typically small, headless, low-powered, and added in high volumes, with designs that usually prioritize low-cost over security. As a result, they can be easy to exploit and hard to detect when compromised. Many IT

teams lack the time and tools to monitor rapidly expanding IoT environments. The FBI has warned that IoT networks are a highly sought-after vulnerability,[6] and 25% of all attacks are expected to target IoT by 2020.[7]

#### 4. Use Stolen Credentials

A Verizon study reveals that 81% of data breaches are tied to stolen or weak credentials.[8] Attackers steal credentials from employees using tactics such as social engineering, packet sniffing on public Wi-Fi, or brute force attacks that crack weak passwords. Stolen credentials give an attacker the same level of network access as the employee. And if the corporate Wi-Fi signal is strong enough, an attacker can use stolen credentials from a safe space, such as sitting a car in the corporate parking lot.




## Addressing Wireless Security Challenges

Encryption is an important first step in securing wireless connections, and the Wi-Fi Alliance has made it easier with the newly available WPA3 security protocol.[9] Among other benefits, WPA3 enhances authentication by making brute-force dictionary attacks much more difficult and time-consuming for the attacker, requiring interaction with the network for every guess at a password.

However, despite the protections it provides, users can have a false sense of security when using encryption for wireless traffic. It is only a first step. Hackers need not decrypt if they can access the network and pull information directly. Indeed, all four Wi-Fi network vulnerabilities in the previous section can be successfully exploited without cracking encryption. To protect a wireless environment, additional security objectives need to be achieved. See table 1 for details.

## Wireless Security Elements

| Wireless Threat | Security Objective |
|---|---|
| Attack guest/legacy networks | Segment traffic based on who and what device is accessing the network. |
| Compromise an approved device | Continuously evaluate and police devices to watch for indicators of compromise (IoC), and then automatically quarantine potentially infected devices. |
| Compromise an IoT device | Gain visibility and control over IoT devices. |
| Use stolen credentials | Use strong authentication to ensure only approved users are on network. |

Figure 1: Wireless Attack Vectors.

To achieve the objectives described in table 1, several security elements should be present at different layers of the network—not just at the access points. Further, all security elements should be integrated with each other and work together to automate threat response within a security fabric framework. This ensures a faster response to threats and saves IT investigation time. Security elements should include:

#### 1. Next-Generation Firewalls (NGFWs)

Segmentation is a critical security tool. Most organizations have several networks and employ segmentation to give users different levels of access depending on their identities and roles. An NGFW enables them to enforce segmentation directly at the point of entry, rather than enabling attackers to VLAN-hop or launch other attacks at the access layer before traffic hits a control point. Here, an NGFW controls the variety of traffic coming from a wide selection of possible clients, and ensures that users are blocked from resources they are not authorized to use.

When evaluating NGFWs, keep in mind that some include threat management technologies such as integrated endpoint protection, sandboxing, threat intelligence, and additional safeguards against ransomware and phishing. The ability to centralize, coordinate, and integrate security capabilities such as these is an important advantage. These deliver efficiencies that point security solutions, when working separately, cannot match. Also, some NGFWs have a wireless controller onboard, eliminating the need to buy extra controller hardware and licenses.

### 2. Strong Authentication

It is also important to verify who and what is connecting to the network. Strong authentication is necessary to achieve this goal. Multifactor authentication stipulates that users employ at least two forms of verification, selected from secrets the user knows, devices or tokens a user owns, and/or biometric information connected to the user.

Instead of using the "personal" grades of WPA authentication, which feature a passphrase, organizations need to use a remote authentication dial-in user service (RADIUS)-based system. It checks user credentials against a central list, such as Access Directory, and can verify network access rights for each user before allowing access.

Multifactor authentication offers additional protection for a RADIUS-based system. It helps to guard against stolen credentials by also requiring access to a token and/or personal biometric information. In this case, multifactor authentication makes it far more difficult for a hacker to spoof the personal login information of an employee, as the hacker must possess all of the user's credentials (user name, password, and authentication token).

### 3. Network Access Control (NAC) for IoT devices

No network is secure until the IT team can control who and what is attached, including enforcement of how they can use the network. This is getting more difficult because today's networks typically include a rapidly growing volume of IoT devices such as sensors, HVAC controls, and printers. A network access control (NAC) solution is needed to identify different types of IoT devices, including those that are:

- Controlled by the IT team
- Deployed as operational technology (OT), managing equipment such as production machinery, valves, electrical transformers, or other industrial controls
- Deployed by shadow IT (systems or devices attached to the network that are beyond the awareness, approval, and control of IT)

A NAC solution must be able to:

- Monitor device behavior and recognize a particular device by its characteristics (such as a temperature sensor for an HVAC system)
- Set behavior parameters (e.g., observing what a temperature sensor should and should not access, and detecting unusual behavior, such as when a sensor that makes an address resolution protocol [ARP] call, etc.)
- Automate remediation, sending alerts when behavior strays from parameters and quarantining a potentially hacked IoT device

**Segmentation at the point of entry significantly enhances the security of a WLAN.**

**Multifactor authentication is a requisite for any organization seeking to verify who and what is connecting to the network.**

**With upwards of 25% of all attacks targeting IoT by 2020, network access control is critical for controlling which devices have network access and to what they can access.**

### 4. Ability to Scan for Indicators of Compromise (IoC)

Another important security element is to assume the network is always infected. Users do not intend for their devices to become compromised, but many take them offline for remote work and then reconnect to the network when they have access to do so. This creates an opportunity for what is often deemed infection "in the wild." Here, a compromised device that reattaches to the network will not be identified as infected by a firewall or even the most robust authentication. Thus, it is important to automatically analyze all traffic from devices, identify any suspicious behavior, and quarantine those that are suspicious.

This is best done with a security fabric approach that integrates point security solutions, shares threat intelligence across and between the different security elements, and scans traffic to conduct a continuous trust assessment of elements on the network (see Figure 1). When the security fabric detects IoC from a device, it should coordinate an automated response such as a quarantine, send appropriate alerts, and shrink the remediation window by automatically capturing complete, contextual logging and reporting.

## Security Fabric

Integrates and Coordinates Security and Network Elements as the Cornerstone of Secure Wireless.

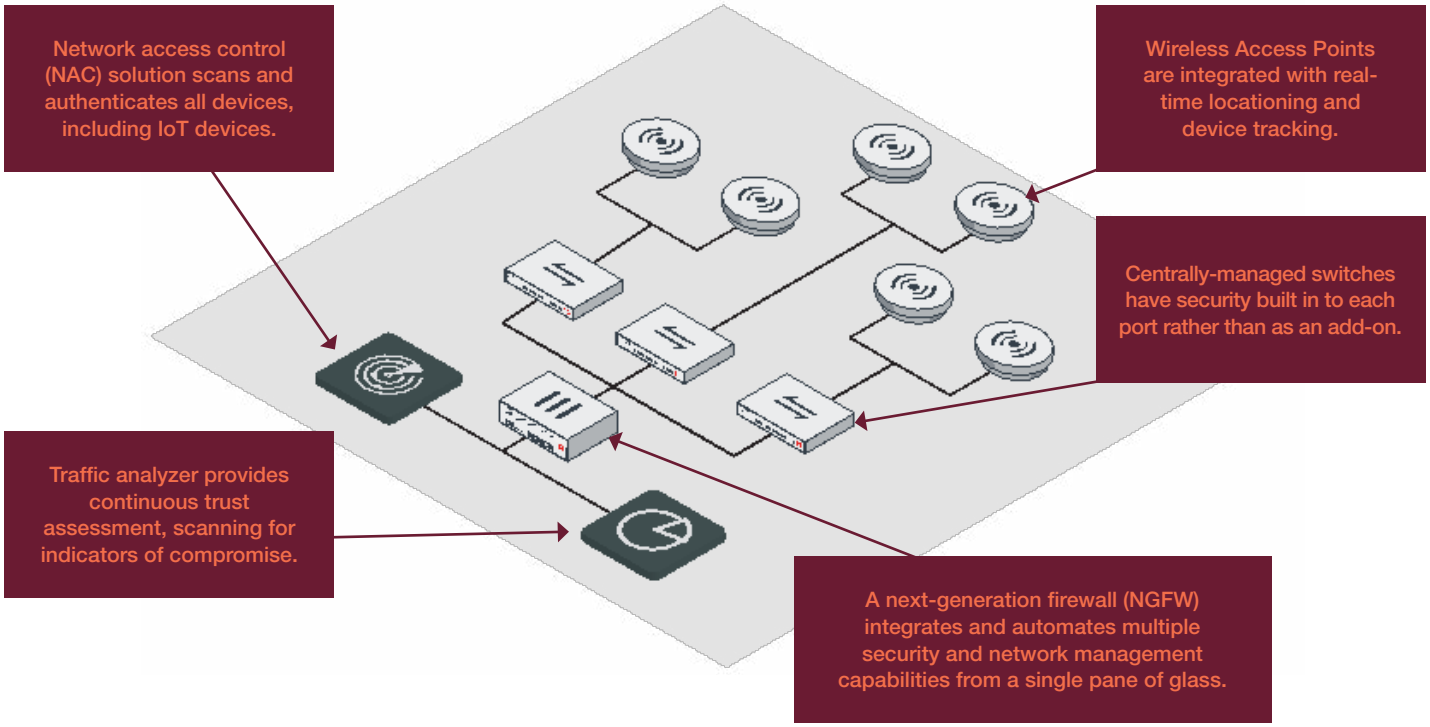



Figure 1. Security Fabric - Integrates and Coordinates Security and Network Elements as the Cornerstone of Secure Wireless.

## A Truly Secure Wireless Network

While on-air encryption will always be an important part of securing a wireless network, there are other attack vectors that need protection. As wireless encryption improves, attackers will focus their efforts on these other vectors.

Here, wireless security must be multi-layered. The following checklist is important to follow:

A NGFW must enforce segmentation and limit lateral movement.

- A continuous trust assessment capability should scan traffic for indicators of compromise and automatically quarantine suspicious devices.
- A network access solution should enforce multi-factor authentication of users and devices and identify IoT devices and monitor their behavior.
- A security fabric should unify security solutions, providing broad visibility, integrated threat detection, and automated threat responses and remediation.

[1] "A brief history of Wi-Fi," The Economist, June 10, 2004.

[2] Julian Watson, "Wireless Technologies to Comprise 55 Percent of Connectivity IC Shipments in 2018, IHS Market Says," IHS Markit, June 12, 2018.

[3] "Wireless Local Area Network (WLAN) Market 2018 Global Industry Analysis By Share, Key Company, Trends, Size, Emerging Technologies, Growth Factors, And Regional Forecast To 2023," Marketwatch, November 14, 2018.

[4] "25% of Cyberattacks Will Target IoT in 2020," Retail TouchPoints, accessed November 30, 2018.

[5] Peter Tsai. "Public Wifi Risks Worry IT Pros," Network Computing, April 12, 2018.

[6] "Cyber Actors Use Internet of Things Devices as Proxies for Anonymity and Pursuit of Malicious Activities," FBI, August 2, 2018.

[7] "25% of Cyberattacks Will Target IoT in 2020," Retail TouchPoints, accessed September 6, 2018.

[8] "2017 Data Breach Investigations Report," Verizon, accessed November 30, 2018.

[9] Curtis Franklin, Jr. "WPA3 Brings New Authentication and Encryption to Wi-Fi," DARKReading, June 26, 2018.


FORTINET

www.fortinet.com



January 29, 2020 3:11 AM

D:\Fortinet\Minor Changes\Re-color existing assets\wp-red-delineating-the-cornerstones-of-a-secure-wireless-solution-1292020

~~WP-28958~~-0-0-EN