FORTINET

WHITE PAPER

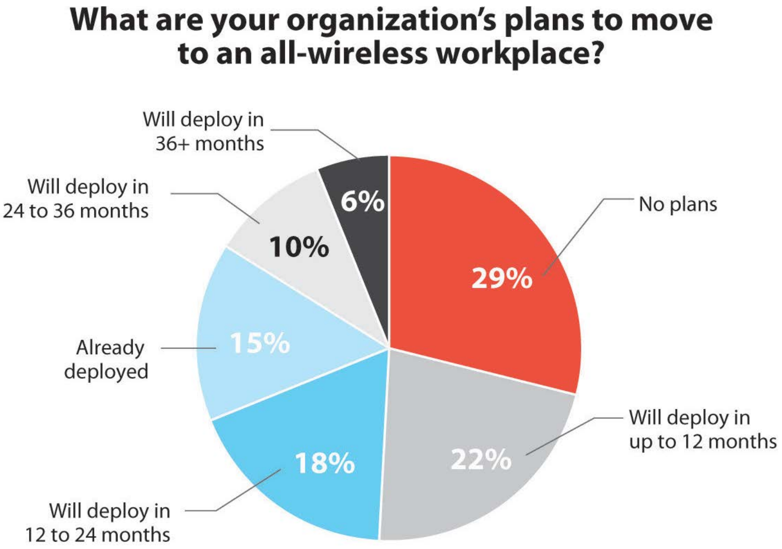
The Top 7 Criteria For Cloud Wi-Fi

Wireless Is Now Business Critical

The mandate for today's IT leader has changed more than for any other business executive in the past five years. The bimodal IT model has become the norm, meaning organizations expect the IT department to help make workers more productive by enabling the company to become increasingly agile while lowering the cost of running IT.

The shift to an all-wireless workplace (a business in which 90% of client connectivity is wireless) is a current IT trend that can achieve both goals. This is why more than two-thirds of businesses are in the process of or are planning to shift to an all-wireless workplace (Figure 1).

Historically, businesses had to choose between the conveniences of wireless and the performance of wired, but that's no longer the case. Wireless LAN (WLAN) technology has evolved rapidly over the past decade, much more so than wired technology. WLAN speeds are now on par with wired, and WLAN is in a position where it can become the primary access network.



What are your organization's plans to move to an all-wireless workplace?

Figure 1: Businesses are embracing the concept of an All-Wireless Workplace.
Source: ZK Research 2015 Network Purchase Intention Study.

Although the vision of "all wireless" has been in place for several years, it has now become a business imperative for the following reasons:

- **"Bring your own device" (BYOD) is gaining acceptance.** A decade ago, bringing personal devices into the workplace was frowned upon by most organizations. However, times have quickly changed, and now 82% of businesses support the use of consumer devices in the workplace, including many heavily regulated verticals such as healthcare and financial services, according to the ZK Research 2016 Mobile Business Mobility Survey. Most of these devices can only be connected by wireless, which increases the number of Wi-Fienabled devices from one to two per user to three to five per user, the survey revealed.
- **The mobile worker population continues to grow.** ZK Research defines a mobile worker as someone who spends at least 35% of his or her time away from the primary work location. Five years ago, 41% of all workers were considered mobile, and today this number has just jumped to 65%, according to ZK Research studies.

- **The Internet of Things (IoT) is becoming a reality.** Historically, only IT-centric devices such as laptops, PCs and printers were connected to the company data network. However, the growth of IoT will connect many operational technology (OT) devices such as factory floor equipment, health care devices, surveillance cameras, pipelines, wearable technology and a wide variety of other devices. With IoT, we will live in a world where everything is connected—many of these devices over Wi-Fi. ZK Research predicts that more than 50 billion devices will be connected by 2020 (Figure 2).

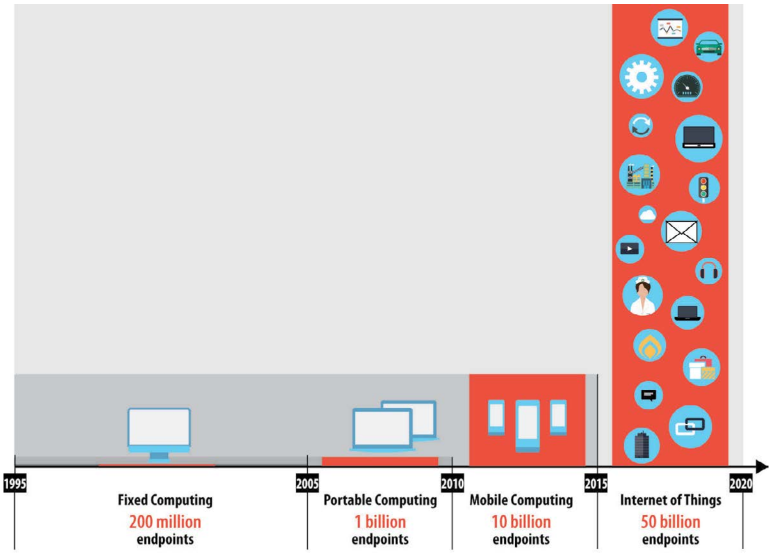


Figure 2: IoT device explosion.

Source: ZK Research, 2016.

- **Wireless LAN is now the basis of competitive advantage.** In many verticals—such as retail, healthcare, entertainment and education—the WLAN connects not only employees but also many external constituents such as students, customers and other patrons. The wireless network provides both the connectivity and critical contextual information such as location and identity. This data can be analyzed and used to create new ways of engaging customers.

  As the use of Wi-Fi and the strategic nature of the technology continue to grow, organizations will need to determine the best way to deploy and manage it. Many options are available today, and it's critical that IT leaders choose the best solution for their company. For many organizations, a cloud Wi-Fi solution is the best option.

The Era of Managed Wi-Fi Has Arrived

The traditional controller-based model of managing the WLAN has been in place for well over a decade. Controllers are physical or virtual appliances that are premises based and control the operations of local access points. Controllers are ideally suited for highly dense environments that contain hundreds or even thousands of access points (APs). However, for highly distributed organizations with just a few access points per location, controller-managed Wi-Fi may not be ideal, as running multiple controllers in different locations can be complex and expensive.

As a result of the challenges associated with controller-based solutions in distributed organizations, cloud Wi-Fi solutions emerged. With cloud Wi-Fi management, customers are only required to purchase APs and not management servers or controllers. Another benefit of cloud-managed solutions is that the organization has flexibility in deployment size. Businesses that choose a cloud solution can start with a single AP and then grow to hundreds or even thousands. Cloud Wi-Fi is ideally suited for distributed companies, as the controller dependencies have been removed. Lastly, because cloud Wi-Fi was developed later than controller solutions, the management interfaces have been built around the concept of simplified GUIs. Cloud Wi-Fi was designed to be simple to use, while other management systems were designed to deal with legacy systems and processes.

However, while cloud-managed Wi-Fi does offer many benefits with respect to cost and management complexity, the solutions aren't fundamentally different from traditional controller solutions. But cloud controllers move the controller from the physical site into the cloud, which can introduce several new challenges that did not exist with controller-based solutions. First, if the connection to the cloud disappears, the Wi-Fi may stop working, meaning workers cannot access even local resources, which would be a huge problem for an all-wireless company. Also, with cloud solutions, security is provisioned in the cloud but the devices are in the local branch, creating some new vulnerabilities. These legacy cloud solutions offer cloud-controlled wireless but aren't full cloud-managed solutions. An all-wireless business requires a true managed solution.

Top 7 Criteria

What's required today is a solution that was built from the ground up to meet the demands of a distributed, all-wireless enterprise. While many solutions require businesses to make trade-offs between performance, security and ease of management, cloud-managed wireless meets the demands of all three. It is a solution with the scalability and security of controller-managed wireless combined with the ease of management of cloud controllers. Below are the top seven criteria that an all-wireless business should use when choosing a cloud Wi-Fi solution:

1. **A full management system**
   On-site and cloud controllers do a great job of providing a platform to push configuration updates to access points. What's needed today is a network-management system that goes beyond basic control and provides a single dashboard for managing the infrastructure and security for the entire network. The management system should also enable unlimited network scalability so organizations can start with a small deployment and increase the number of APs as quickly as required.

2. **Easy and rapid provisioning with zero-touch capabilities**
   The platform should enable organizations to deploy new APs remotely, anywhere in the world, without requiring local technical support. It should operate in a "zero-touch" mode, so as each AP powers up for the first time, it will automatically register with the cloud and automatically download default configurations for that specific organization as well as the latest firmware. The automated capabilities can bring up remote APs and have them fully operational in minutes.

3. **Granular application visibility**
   Businesses need the ability to understand what traffic is running across the network. This requires a solution that is able to distinguish and identify high-bandwidth or latency-sensitive applications such as Netflix, YouTube, Skype, SIP and video. Also, while the configurations need to be made in the cloud, the policies should be downloaded to the AP for real-time enforcement.

4. **User authentication to specific SSIDs**
   This enables the IT staff to create separate access profiles for different administrative groups within the business. For example, a hospital could create different access policies for medical staff and patients, and a school could create different policies for faculty and students. The policies can assign different groups to specific segments or SSIDs. This can be particularly useful to organizations in heavily regulated verticals.

5. **Guest captive portal**
   In the ZK Research 2015 Network Purchase Intention Study, guest access ranked No. 2 among applications businesses were intending to deliver over the WLAN (Figure 3). Businesses that set up guest access should also invest in a captive portal that contains the company logo and even offer something to market and connect with customers. For example, retailers can use the portal to offer customers mobile coupons, while a hotel can leverage it to inform guests of special events. The Wi-Fi network should allow for any number of SSIDs to be configured with fully customized captive portals to enable the operation of multiple branded portals simultaneously.

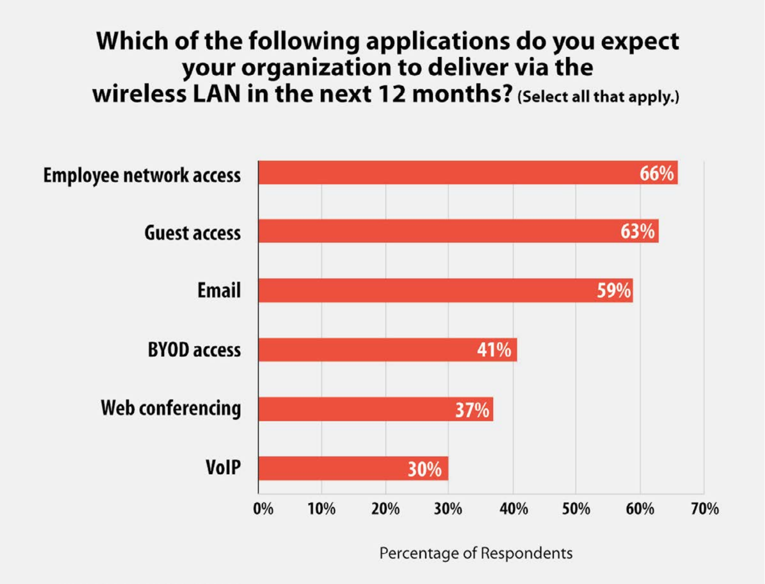


Figure 3: Guest access is a must-have Wi-Fi feature.

Source: ZK Research 2015 Network Purchase Intention Study.

6. **Health, utilization and application analytics**
   It's not enough for the Wi-Fi network to just provide access. To move to a predictive management model, it also needs to offer visibility into the health of the network. The dashboard view should show the status of each AP and then offer drill-down capabilities to enable users to understand the status and performance of each AP. Also, Layer 7 application visibility is necessary to understand which applications are being used, by whom and the bandwidth being consumed. The IT department can use the information gathered and analytics to set baselines and look for anomalies that indicate security or future application performance problems. Lastly, the solution should provide preconfigured and custom reports for compliance issues or for business reporting.

7. **Security designed for an all-wireless business**
   One highlight of the ZK Research 2015 Network Purchase Intention Study is that security is now the top concern for both business and technology executives, with 75% of IT leaders stating that mobility presents their biggest security challenge. Also, security remains the top inhibitor to IoT deployments (Figure 4). Many of these concerns can be addressed by securing the Wi-Fi network, as this is the first point of access for many mobile devices and IoT endpoints.

With traditional cloud solutions, security addresses basic authentication but does not have any advanced capabilities. For these solutions, one option would be to put security devices such as intrusion prevention systems (IPSs) and application controls at every AP, but the cost and complexity of this model would overwhelm every organization. A better option would be to embed advanced security functions directly into the AP hardware. The APs would need to have additional memory and processing capabilities compared to traditional thin APs. This would enable the APs to perform real-time security processing at the network edge instead of in the cloud or even on the company LAN. Processing Layer 2-7 security in the AP in a single pass is much more efficient, and it enables granular user and device policies and provides complete visibility at the session level. Below are the security features that should be embedded into the AP:

- Intrusion prevention system
- Anti-malware
- Web URL filtering
- Application control
- Botnet protection

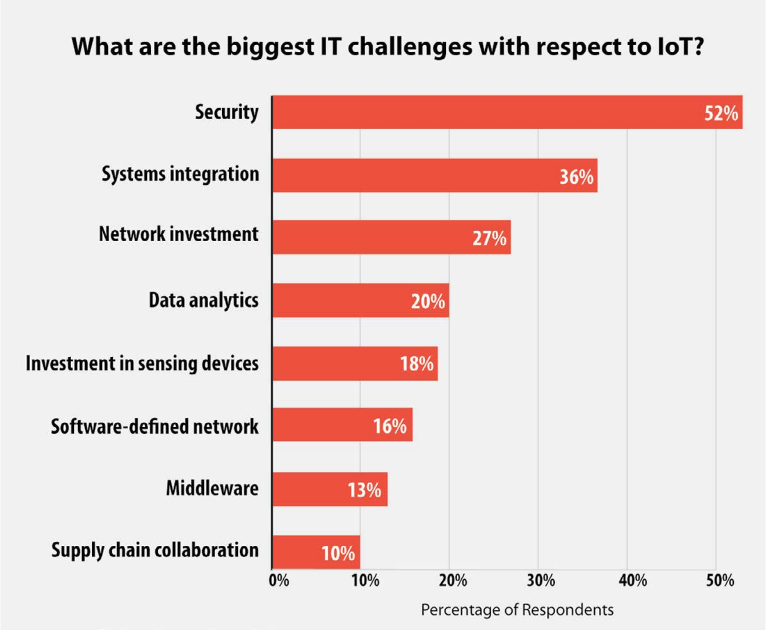


Figure 4: Security is the top inhibitor for deploying the Internet of Things
Source: ZK Research 2015 Network Purchase Intention Study.

Conclusion and Recommendations

The evolution of wireless, increased acceptance of BYOD, a growing mobile population and the Internet of Things are transforming enterprises faster than ever before. Although the vision of the all-wireless enterprise has been on the horizon for several years, the technology to support it has not been available until now. The first wave of cloud-based controllers made Wi-Fi easier to deploy in distributed organizations and simplified its management, but they did not address scalability issues, provide analytics or offer the necessary levels of security. Businesses must embrace the concept of cloud-managed wireless—a Wi-Fi solution that offers complete management capabilities and is built from the ground up for this era of wireless. To help businesses get started, ZK Research makes the following recommendations:

- **Embrace the vision of the all-wireless office.** Untethering employees from the shackles of the wired desktop can improve their ability to collaborate and streamline business processes, increasing employee satisfaction. The all-wireless enterprise also helps cut the cost of networking by removing expensive wired ports and replacing them with a lower-cos wireless network. Being an all-wireless enterprise is critical to achieving a competitive advantage today and realizing the vision of bimodal IT.
- **Look beyond your incumbent vendor.** When making IT purchases, it's easy to choose a vendor based on its market share or incumbency. This may be the right decision for mature technologies, but large incumbent vendors rarely push the industry through a transitional period. Instead, make a decision based on criteria specific to the needs of an allwireless enterprise. Test the solution against metrics such as speed of deployment, support for multimedia applications, security capabilities and how close it comes to offering a wired-like experience. It is important to do the necessary homework to evaluate all possible solutions.
- **Rethink wireless security.** Historically, wired and wireless were deployed independent of one another. This approach was ineffective because it's not possible to equip every AP with the necessary technologies to secure the organization. Instead of using additional security applications for things like antivirus, web filtering and IPS, look for solutions that have these capabilities integrated into them. Although this wasn't the way wireless networks were secured in the past, it needs to be the way security is implemented in the future.

7 Top Requirement for Cloud Wi-Fi

- Full management system
- Easy and rapid provisioning with zero-touch capabilities
- Granular application visibility
- User authentication to specific SSIDs
- Guest captive portal
- Health utilization and application analytics
- Security designed for an all-wireless business

September 18, 2019 3:08 AM
D:\Fortinet\White Paper\Top 7 Criteria for Cloud Wi-Fi\wp-the-top-7-criteria-for-cloud-wifi
485443-A-0-EN