FORTINET

SURVEY REPORT

Wireless Security Survey 2015

Wireless Security Deployed: State of the Market

Wireless Security Survey 2015

Wireless Security Deployed: State of the Market

Technology and market trends are forcing rapid changes to enterprise IT—especially in regard to how networks are secured.

Growth in Unsecure Connected Devices

As the number and types of network-connected wireless devices continue to grow exponentially, these connected devices present new vulnerabilities and a growing attack surface for hackers to exploit.

Application Proliferation Enlarges Attack Surface

Growth of mobile applications goes hand-in-hand with the increasing number of devices. Enterprises not only face additional support challenges, but also new threat exposures from additional applications being introduced to the network.

Operational Complexity for IT

On top of this unprecedented growth, users expect a unified access experience that ensures consistent, secure policies across wired and wireless environments. This creates major challenges for IT organizations that are stressed to fill gaps in security if policies are inconsistently applied and not easy to manage.

This global survey studies the state of the market for wireless LAN security deployed among 1,490 medium-to-large enterprises across a broad range of industries, and shows that the majority of enterprises have holes in their WLAN security strategy.

WELL-FOUNDED FEARS

92% of CIOs are worried that their wireless security is inadequate. This wireless security survey shows that their concerns are well-founded. Basic measures such as firewall and authentication were lacking in hundreds of businesses surveyed.

Yet, paradoxically enterprises are embracing BYOD in record numbers and showing great interest in Cloud Wi-Fi. These are two factors that add complexity to any security framework.

Respondent Profiles

The findings of this report come from an independent survey of 1,490 IT decision makers (ITDMs) representing organizations with 250 or more employees. Over 46% of organizations surveyed exceeded 1,000 employees.

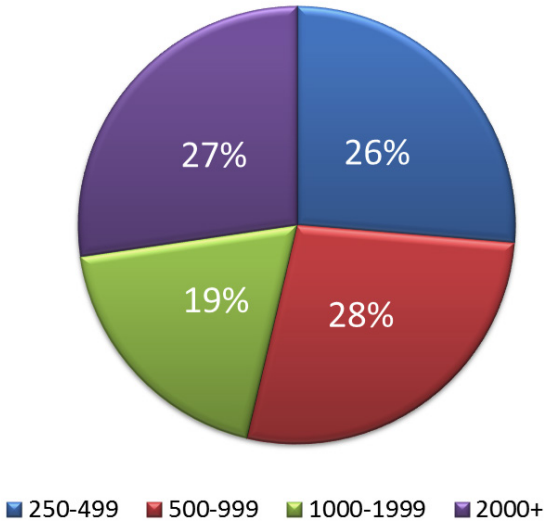

FIG 1: SIZE OF ORGANIZATION BY # OF EMPLOYEES

Respondent organizations came from a broad spectrum of industries, including the public sector. Within each sector, there was a fairly even distribution of organization size among the four size categories.

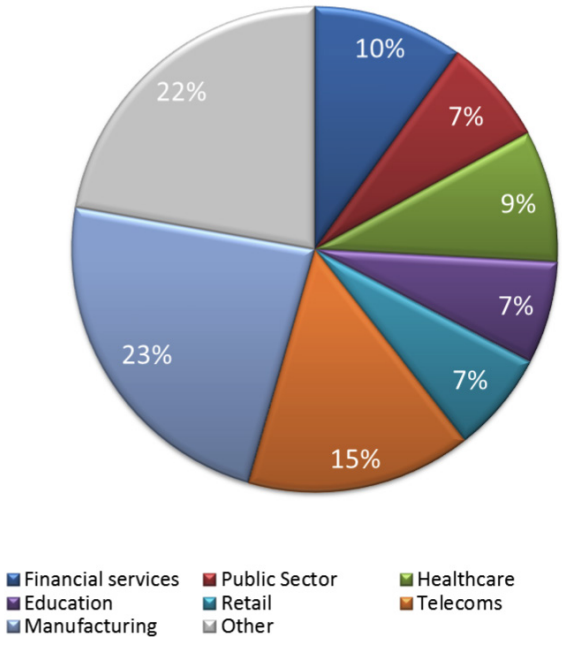

FIG 2: DEMOGRAPHICS OF ORGANIZATION INDUSTRIES

All respondents were sourced from independent market research company Lightspeed GMI's online panel[1] and were customers of all the major WLAN equipment vendors.

Vulnerable

According to the survey, wireless networks are ranked as the most vulnerable IT infrastructure, with the highest proportion of ITDMs (49%) placing it in their top two. Respondents positioned wireless as significantly more vulnerable than core networking infrastructure, with just 29% of ITDMs ranking this in the top two.

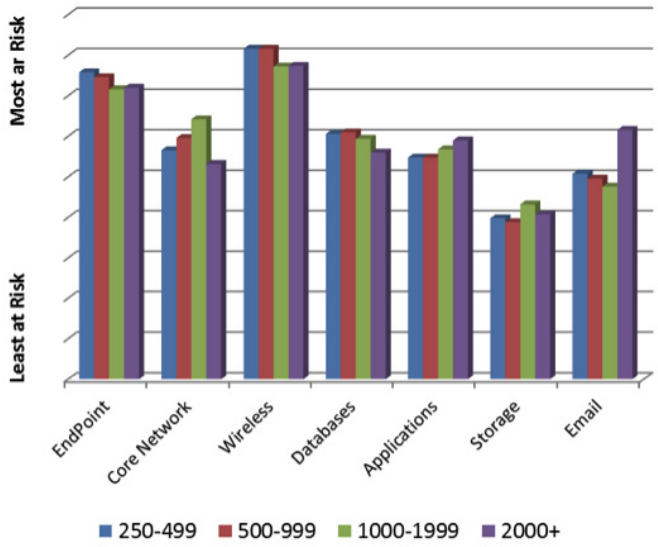

FIG 3: VULNERABILITY OF WIRELESS VERSUS OTHER IT INFRASTRUCTURE

While endpoint security was also noted as the second top concern (45%), application (17%) and storage (11%) infrastructure components were considered least at risk.

Inadequate Wi-Fi Security

82% of ITDMs and 92% of CIOs polled reported fears that their WLAN security was inadequate, with nearly half of ITDMs (48%) citing the potential loss of sensitive corporate and/or customer data as their biggest concern, and 22% citing industrial espionage as their biggest fear of operating a wireless network with incomplete security.

Only 70% of organizations surveyed protected the WLAN with a firewall and only 63% had authentication to secure internal wireless LAN access. While more than 60% of organizations used antivirus scanning, fewer than 40% were protecting their wireless networks with IPS, Application Control and URL Filtering.

The relatively low deployment of IPS, application control, and URL Filtering might also suggest that wireless security is not being treated as solemnly as it deserves to be.

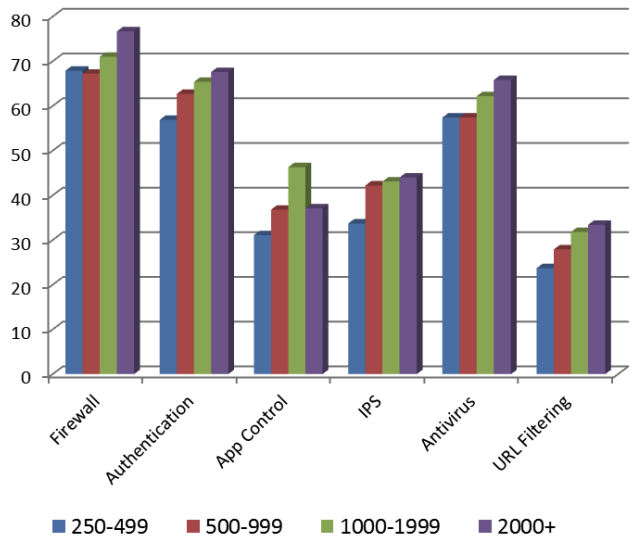

FIG 4: WLAN SECURITY IMPLEMENTED BY SIZE OF ORGANIZATION

In the face of advanced persistent attacks increasingly targeted at multiple entry points, overlooking the most basic measure of firewall (29%) and authentication (37%) is playing with fire.

Unsecured Guest Access

Basic security for guest Wi-Fi was shown to be lacking as well. 13% of organizations that deployed guest access on the same WLAN infrastructure used by employees reported that guest Wi-Fi is totally open, and a further 24% allow guests to use a shared username and password.

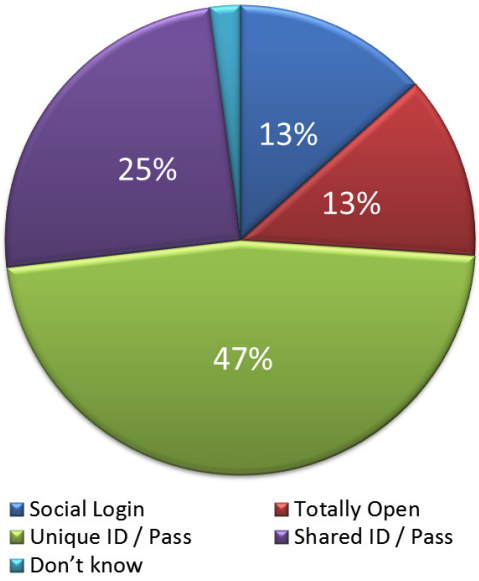

FIG 5: GUEST ACCESS SECURITY LEVEL IMPLEMENTED

The recognized best practice for guest access is to authenticate guests through a captive portal with a unique ID and password, and to subject traffic to real-time antivirus scanning, usage controls (time of day, length of session, rate limits), and content filtering through guest policies associated with a guest SSID.

All vendors offer captive portals and most also support social login. Basic bandwidth management can be enforced by on-site or cloud controllers, but sophisticated application controls require deep packet inspection on a specialized appliance. Antivirus and URL filtering also require additional security appliances on the corporate LAN or in the data center.

Future Security Priorities

When considering the future direction of their wireless security strategies, the majority of respondents said they would maintain focus on the most common security features, namely, firewall and authentication.

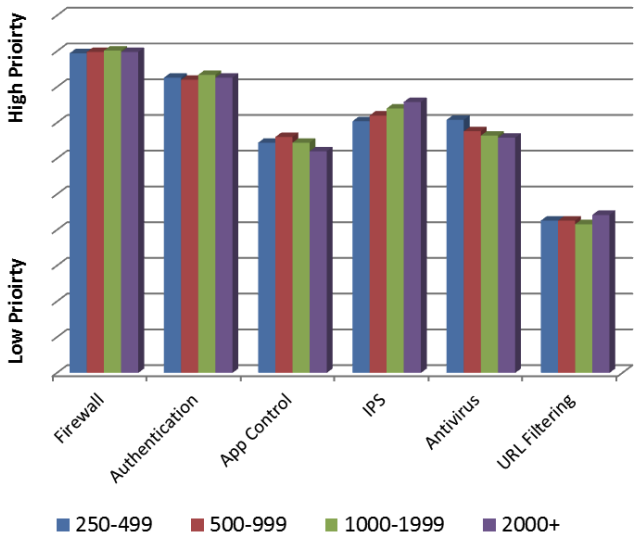

FIG 6: RELATIVE PRIORITY OF FUTURE SECURITY ENHANCEMENTS

Albeit at a lower priority, demand persists for complementary security technologies such as IPS, antivirus, and application control for complete threat protection. For example, nearly 16% of respondents placed IPS as their top priority, in comparison to under 3% flagging URL filtering as their top priority. Intrusion prevention was identified as a higher priority by respondents in healthcare, retail, and manufacturing which have a wide variety

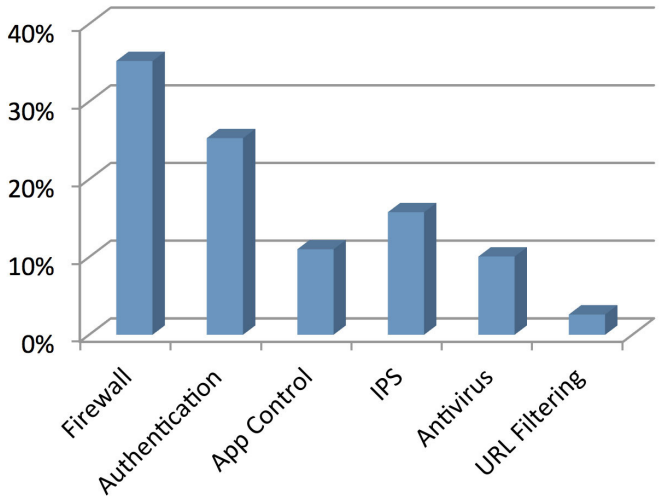

FIG 7: % RESPONDENTS RANKING MEASURE AS THEIR TOP PRIORITY

of mission-critical embedded systems such as medical devices, mobile Point of Sale (mPOS) terminals, and RFID readers. Such embedded devices are often vulnerable to attacks that target weaknesses in unpatched firmware.

BYOD Ahead of Security

BYOD is pervasive and unstoppable. November 2014 research by Tech Pro Research[2] indicates that 60% of organizations (up from 44% in February 2013) now support BYOD, and a further 14% plan to allow it in the next 12 months. The findings of this survey suggest, however, that deployment of the security measures needed to minimize the risk of BYOD has not kept pace with the rapid rate of BYOD adoption.

With laptop sales giving way to tablets, enterprises can only expect more employee-owned devices entering the workplace and being used for corporate business. Enterprises need to adjust their security posture for BYOD in order to fully protect company data.

This survey similarly found more than 76% of organizations allow employee BYOD—and just over two-thirds of those employees are permitted to access sensitive corporate data on those user-owned devices.

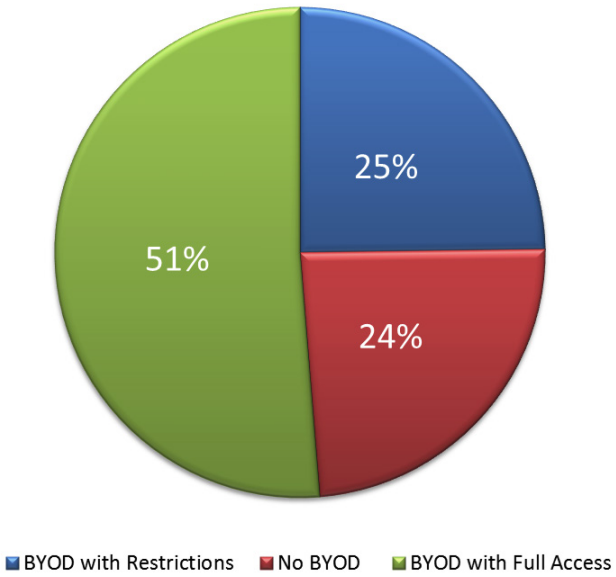

FIG 8: ADOPTION OF BYOD AND ACCESS LEVEL PERMITTED

Unless there are good measures in place for securing access to sensitive data from untrusted devices, this should be a grave concern for CIOs. There are two main security issues concerning BYOD: securing the device itself and securing the data streams.

The market for Mobile Device Management (MDM) tools that check integrity and wipe data from lost devices is languishing at 30% penetration according to Gartner estimates.[3] Part of the reason for this is that they are limited to only securing the device.

The other half of the equation—securing the data streams—requires corporate security policies that govern user privileges and enforce antivirus scanning, application priorities, and content inspection. This is not a job for MDM. These measures are network-based.

Rogue AP detection is an increasingly relevant consideration. Almost any mobile device these days can share its radio as a virtual AP and become an attack vector. Continuous rogue screening is advisable.

Cloud-managed Wi-Fi

Respondents were bullish about migration to cloud-managed WLANs. IDC predicts the cloud Wi-Fi market will see 46% CAGR thru 2018 and will total $2.5B in value by 2018.[4]

72% of respondents said they managed at least part of their network through the cloud. Distributed enterprises such as retail and financial services led the pack with 80% penetration of cloud-managed Wi-Fi, while large enterprises with 2,000+ employees have been slower to embrace WLAN management from the cloud. Only 65% of large enterprises reported using the cloud for some or all of their WLAN management.

Many enterprises use cloud management only partially—to initialize remote APs when installed in branch offices by non-IT personnel. After initial setup, ongoing management is then done over the WAN from the corporate network or datacenter.

Only 12% of respondents did not trust the cloud for WLAN management; however, of the 88% that do, nearly two-thirds indicated they would prefer cloud management hosted in their own data center rather than third-party hosted management.

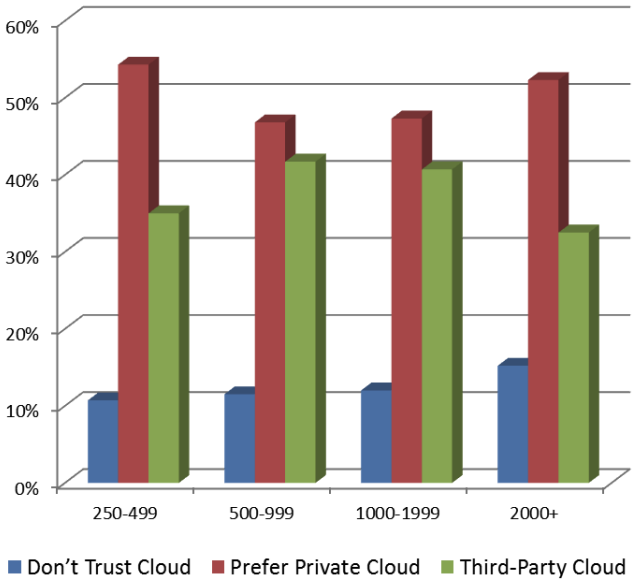

FIG 9: INTEREST IN CLOUD-MANAGED WI-FI

The Cloud Wi-Fi Paradox

WLAN vendors are promoting their cloud Wi-Fi offerings with much gusto these days. That's because they want to convert customers to subscribers. For some businesses, the CAPEX/OPEX tradeoff makes sense; for others not.

What makes sense to everyone is the simplification of WLAN management that comes with the cloud. Initial setup, configuration, and maintenance are all easier—as is the implementation of basic authentication policies.

But when it comes to adapting more sophisticated security measures (such as IPS, antivirus, DLP and application control), the cloud may not be best place to incorporate some of these capabilities. And implementing them to work alongside a cloud Wi-Fi architecture adds considerable networking complexity.

Fortinet Secure Access Architecture

With these trends and challenges, the deployment and management of enterprise networks, applications and devices must be simplified. A network access layer that is not only secure, but also easy to manage.

Fortinet's network access solutions offer the best of next-generation firewall capabilities together with enterprise access. As opposed to traditional wireless solutions (which only address connectivity) Fortinet's secure access solutions feature robust network security at their core—in addition to connectivity. Fortinet secure access solutions are designed to provide the same award winning and third-party validated security in every type of deployment—from a stand-alone AP in an isolated office, to a handful of APs in a retail store, to thousands of APs deployed across a large enterprise campus. Our product offerings enable any business to choose the topology and network management that best suits their needs, without having to compromise on security protection.

Securing business communications, personal information, financial transactions, and mobile devices involves much more than network access control. It requires scanning for malware, preventing access to malicious websites, end-point integrity checking, and controlling application usage. But typical Wi-Fi solutions do not cater to these requirements. Fortinet's unique approach addresses the shortcomings of other Wi-Fi offerings.

With Infrastructure, Integrated, and Cloud solutions—Fortinet offers a comprehensive set of deployment options. These three solution options are designed to extend or upgrade existing network systems. Our secure access portfolio provides the most flexible cyber security platform with end-to-end enforcement for enterprises of all sizes and verticals of any type.

[1] The Fortinet Wireless Security Survey was a research exercise undertaken throughout May 2015, by market research company Lightspeed GMI. The survey was conducted online amongst 1,490 qualified IT decision makers–predominantly CIOs, CTOs, IT Directors and Heads of IT–at organizations with more than 250 employees around the globe. Twelve countries participated in the survey: Australia, Canada, China, France, Germany, India, Italy, Japan, Hong Kong, Spain, UK, and USA.

[2] http://www.techproresearch.com/downloads/wearables-byod-and-iot-current-and-future-plans-in-the-enterprise/

[3] http://www.crn.com/news/security/240156399/mobile-device-management-market-wont-last-gartner.htm

[4] Cloud-Managed WiFi Set to Grow to $2.5 Billion by 2018 (IDC #247738)

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE
Paseo de la Reforma 412 piso 16
Col. Juarez
C.P. 06600
México D.F.
Tel: 011-52-(55) 5524-8428

Oct 15, 2015