| WHITE PAPER |

BRINGING BYODs INTO THE FOLD

with NETSCOUT

ENTERPRISE

Employees want to bring their own Wi-Fi enabled smart devices into the workplace, and businesses have much to gain by embracing this bring-your-own device (BYOD) trend.

While surveys show that most organizations are already moving in this direction, many have yet to fully understand much less address the multitude of impacts that BYODs are having on enterprise WLAN performance, security and compliance. In this paper, we show how factoring smart devices – including BYODs – into the full WLAN lifecycle can fill this gap, avoiding costly problems and simplifying trouble resolution. NETSCOUT's AirMagnet solutions can play an instrumental role by enabling detection, planning, compliance monitoring and troubleshooting of all smart devices, helping IT bring BYODs into the fold.

Introduction

Today, many workers are pushing consumer electronic products into the workplace by demanding that IT support the same technologies for business. This "consumerization of IT" has driven many organizations to embrace bring-your-own smartphones and tablets. Specifically, market research conducted by NETSCOUT showed that 82% of organizations now permit corporate network access by smartphones, tablets, and other smart devices designed for and purchased by consumers for personal and business use. Many organizations permit these bring-your-own devices (BYODs) to foster employee mobility, connectivity, and productivity. However, BYODs are a double-edged sword.

BYODs that use corporate networks, with or without IT approval, are already having tangible impact on enterprise WLAN performance and security. Unlike corporate-purchased or approved smart devices designed for enterprise use, BYODs are hard to predict, relatively diverse, and less robust. As a result, roughly half of the organizations surveyed by NETSCOUT already experience daily employee complaints about BYOD connectivity and are concerned about BYOD bandwidth consumption. Worse, explosive consumer electronic sales are likely to exacerbate these problems, as fewer than 50% of those organizations planned any WLAN redesign to accommodate growth.

The decision many organizations now face is not whether to allow BYODs; that ship has sailed. Rather, today's challenge is to find effective methods and tools to discover smart devices used in the workplace (no matter who owns them), assess their impact on the corporate network, reduce unwanted side-effects and facilitate trouble-free business-appropriate use.

Understanding BYOD impacts

IT initiatives to tackle BYOD challenges often focus on mobile device and data management. Those measures can be critical for successful BYOD adoption – for example, using a mobile device manager to provision secure WLAN settings and later remove them after device loss, theft, or retirement. However, they do not fully address the many ways in which BYODs impact corporate networks.

Unplanned BYODs compete for scarce airtime and drain WLAN capacity. Network planners have long designed for the capacity required by corporate assets (e.g., number of IT-procured laptops in a given office). However, the number of smart devices carried by each individual continues to grow, surging in unpredictable ways. For example, when employees return to work after a holiday with new BYO smartphones and tablets, capacity planning assumptions can be quickly blown away. Not only does client competition for shared channels grow, but Wi-Fi chipsets in consumer electronics differ. For example, Gartner reports that Apple iPads consume three times the capacity used by a typical laptop due to lower transmit power (10 mW vs. 30-50 mW).

BYODs behave in unexpected ways, degrading overall performance. When IT selects a smart device, network planners can first verify interoperability and isolate constraints like unsupported Wi-Fi data rates or modes that cause some clients to use more airtime at their neighbors' expense. However, IT has little control over BYOD selection; most BYODs are less robust consumer-grade devices.

BYODs may operate insecurely, jeopardizing corporate assets. Today, virtually all Wi-Fi certified smart devices – including BYODs – are capable of supporting WPA2-Enterprise security. However, corporate WLANs secured with WPA2-Enterprise are sometimes off-limits to unapproved BYODs that aren't enrolled in directories or issued certificates for 802.1X authentication. These unapproved BYODs may therefore resort to using open guest WLANs where they expose traffic (both personal and business) to eavesdropping and various man-in-the-middle attacks. Worse, when IT is not monitoring BYOD activity, such exposures go undetected.

Even approved BYODs can be difficult or costly to trouble-shoot. Consumer-grade smart devices often lack remote diagnostic interfaces and tools for help desks to investigate and resolve problems. For example, remote control agents supported on laptops and Windows phones are unavailable for iPhones and iPads due to Apple iOS restrictions. And while some Android OEMs (e.g., Samsung SAFE) offer proprietary extensions for logging and diagnostics, the vast majority of Android BYODs support very limited administrative APIs that cannot help IT trouble-shoot from afar. As a result, malfunctioning BYODs often remain a mystery, sapping WLAN performance indefinitely. Moreover, BYODs have grown so numerous that IT may not have sufficient staff to trouble-shoot them, nor much motivation to expend time on non-corporate devices.

As these examples show, ignoring BYOD impact on corporate networks can degrade business efficiency and increase operating costs. Furthermore, until employers acknowledge and address these challenges, they cannot harness the business benefits of these increasingly ubiquitous devices, such as tapping BYODs to reduce monthly telecom spend and liability for personal use of corporate phones (e.g., overage fees).

Melding BYOD into the WLAN Lifecycle

To more fully address their business impacts and facilitate productive business use, BYODs should be proactively factored into every step of the WLAN lifecycle.

Wi-Fi Planning & Design: Today's enterprise WLANs should be designed not just for laptops, but also to meet anticipated BYOD coverage and capacity needs. Build in extra bandwidth and higher client density to accommodate inevitable BYOD growth. Optimize the network for expected BYOD device usage based on known devices. When positioning APs, plan ahead for the shorter reach and lower data rates associated with battery-powered consumer electronics that have 1x1 MIMO antennas. Allocate available RF spectrum while bearing in mind that most contemporary BYODs don't support 5 GHz or 40 MHz bonded channels.

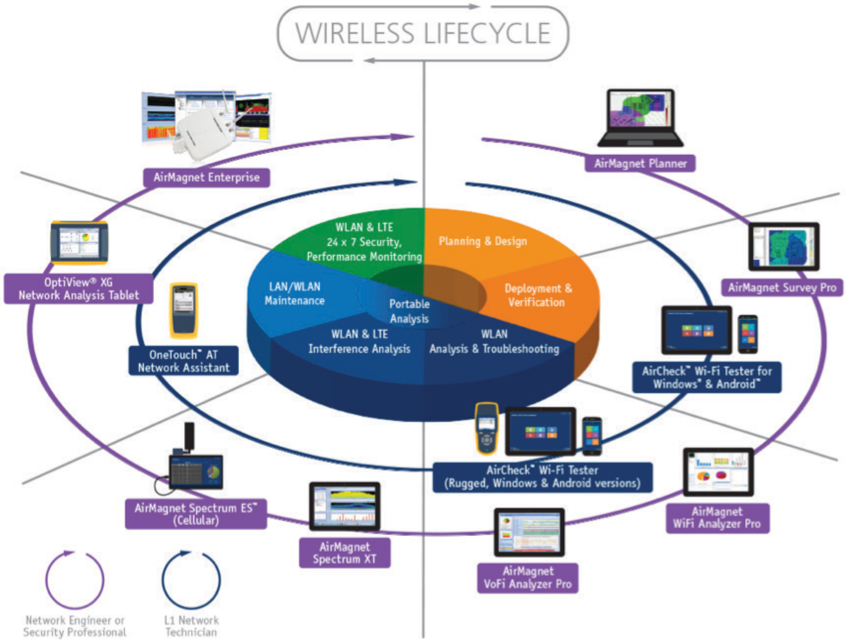
Site Survey, Deployment and Verification: Follow initial planning and deployment with site surveys, conducted with IT-issued laptops and handsets and a representative set of BYODs (e.g., Androids). To verify true user experience, measure business application performance in both upstream and downstream directions; results are likely to differ and often do not correlate directly to signal strength (i.e., bars displayed by a smartphone). Measure performance at every location where smart devices can connect to the corporate network throughout your facility to get a complete and accurate picture of real-world results. Finally, use all of these survey results to offer guidance on recommended or banned BYODs and help employees make personal product choices that improve both overall network and individual user productivity.

Troubleshooting and Managing Interference: When it comes to BYODs, ignorance is a surefire path to RF inefficiency. Deploy tools that can routinely monitor and deliver actionable visibility into the physical and link layer interference caused by smart devices carried by both employees and guests. Develop diagnostic practices to proactively isolate BYOD-induced anomalies and Wi-Fi connectivity problems, helping administrators cost-effectively spot and remediate new interferers before help desk calls begin and productivity suffers.

Wireless Security Monitoring: Without adequate tools and automation, BYODs are difficult if not impossible to monitor for possible security breach. Take steps to backfill this all-too-common blind spot by using a Wireless Intrusion Prevention System (WIPS) to continuously monitor your entire corporate airspace for all smart devices, no matter who owns them. Take advantage of WIPS to auto-classify and respond to BYOD-induced threats and security policy deviations, logging all activity 24/7 to better understand BYOD use and satisfy regulatory compliance and reporting needs. Additionally, make sure a solution that will allow for devices classification is in place. It is important to have visibility into the smart devices on your network and be able to differentiate between a smart device and a regular 802.11 station. This will save hours of troubleshooting by being able to immediately identify those BYODs that are rogue.

Proactive Performance Assessment: Augment reactive troubleshooting with continuous active wireless testing to proactively detect network congestion, growing error rates, degraded data rates and other problems caused by unexpected increases in the number, density and diversity of Wi-Fi devices. With BYODs, frequent unplanned change is a virtual certainty; trend analysis can be an effective way to assess emerging impact and adapt plans and policies to satisfy demand and avoid BYOD troubles.

Integrating BYODs into practices and tools used throughout the wireless LAN lifecycle is an investment in business success and efficiency. For example, iPad and Android tablet sales are growing, but many enterprises have not yet embraced these popular BYODs. Nonetheless, it makes sense to consider the presence of all personal smartphones and tablets carried by employees. Proactively watch for RF interference caused by iOS and Android mobile hotspots and continuously test your WLAN to detect and evaluate their business impact. When rolling out new APs, include consumer devices in site surveys, planning layout and spectral allocation to ensure coverage. When the time comes to embrace these consumer tablets for business, your WLAN will be well-positioned to do so without costly redesign.

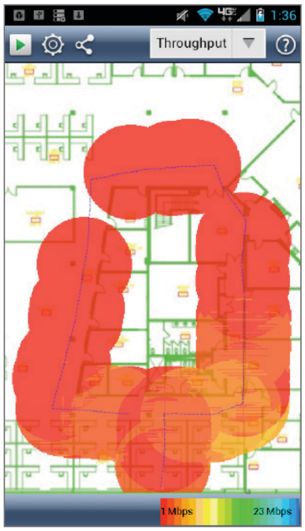

WIRELESS LIFECYCLE
AirMagnet Enterprise
AirMagnet Planner
OptiView® XG Network Analysis Tablet
WLAN & LTE 24 x 7 Security, Performance Monitoring
Planning & Design
LAN/WLAN Maintenance
Portable Analysis
Deployment & Verification
WLAN & LTE Interference Analysis
WLAN Analysis & Troubleshooting
AirMagnet Survey Pro
OneTouch™ AT Network Assistant
AirCheck™ Wi-Fi Tester for Windows® & Android™
AirCheck™ Wi-Fi Tester (Rugged, Windows & Android versions)
AirMagnet Spectrum ES™ (Cellular)
AirMagnet Spectrum XT
AirMagnet WiFi Analyzer Pro
AirMagnet VoFi Analyzer Pro
Network Engineer or Security Professional
L1 Network Technician

How NETSCOUT's can help

NETSCOUT's AirMagnet product line offers a complete portfolio of solutions, spanning the entire WLAN lifecycle, to help businesses ensure wireless LAN security, performance and compliance. The AirMagnet products can help your organization bring BYODs into the fold by discovering employee-owned mobile devices used in business settings, assessing their impact on the corporate network, reducing unwanted side-effects and facilitating trouble-free business-appropriate use.

During Wi-Fi planning and design, AirMagnet Planner enables predictive modeling of enterprise WLANs. Using information about your facility, RF environment, and Wi-Fi device population, AirMagnet Planner predicts the coverage and performance of your WLAN to help you refine physical layout and RF band/channel allocations. By speculatively adding BYODs to any AirMagnet Planner project, designers can easily perform "what if" analysis to understand the impact of BYOD growth – for example, how many APs would be needed to satisfy coverage and performance requirements if employees brought iPads to work next year.

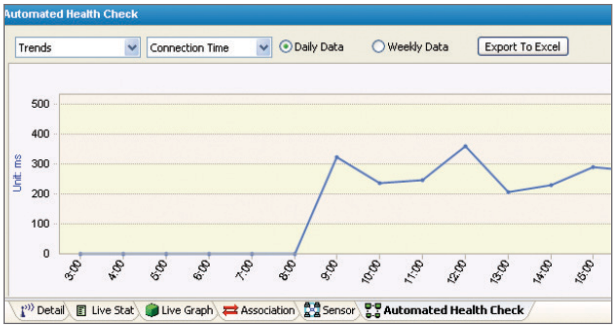
After WLAN deployment, AirMagnet Survey can measure actual on-location coverage and verify true end-to-end performance. Especially for BYODs that tend to be extremely diverse and poorly-documented, there is no substitute for capturing, mapping, and analyzing actual user experience by connecting to a production WLAN. To facilitate this, Fluke Networks introduced AirMagnet AirMapper™ (right), an easy-to-use Android application that can be installed on any Android device (version 2.2 or higher). The AirMapper App makes it easy to map and visualize coverage experienced by Android BYODs, while the PRO version can export measurements to AirMagnet Survey PRO to broader, deeper analysis and reporting.



Over time, AirMagnet Enterprise can continuously monitor RF activity throughout your WLAN, including remote sites equipped with SmartEdge Sensors that use three 802.11n

3x3 MIMO radios – two for full-time dual-band monitoring and one dedicated to spectrum analysis. This infrastructure can automatically detect new BYOD interferers and support proactive client performance verification.

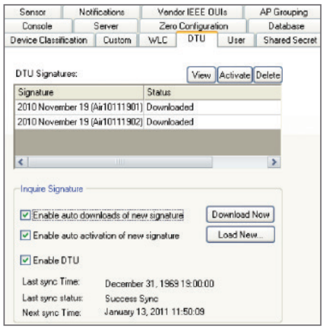
The latter is accomplished by AirMagnet Enterprise's Automated Health Check (AHC) feature (below, left) which leverages hardware or software sensors to test network health end-to-end. With scheduled health checks, IT can be quickly alerted to emerging problems triggered by misbehaving or misconfigured BYODs. When a problematic device is discovered, AirMagnet Enterprise's Dynamic Threat Update (DTU) feature (below, right) can be used to create new signatures to detect that specific device type or problem. These tools can help IT rapidly discover and automatically respond to BYODs, minimizing the adverse impact they might otherwise have on WLAN performance and business applications.



Trends

Connection Time

● Daily Data ○ Weekly Data



DTU Signatures:

Signature	Status
2010 November 19 (Air10111901)	Downloaded
2010 November 19 (Air10111902)	Downloaded

Inquire Signature

☑ Enable auto downloads of new signature

☑ Enable auto activation of new signature

☑ Enable DTU

Last sync Time: December 31, 1969 19:00:00
Last sync status: Success Sync
Next sync Time: January 13, 2011 11:50:09

With AirMagnet Enterprise's BYOD Classification, smart devices are automatically classified and grouped with detailed information including operating system and model name. Additionally, the IT administrator can also get a smart device list report detailing the above information.

Finally, when mysterious smart device problems do occur, mobile diagnostic tools such as AirMagnet WiFi Analyzer and AirMagnet Spectrum XT are invaluable. The AirWISE analysis engine built into WiFi Analyzer makes it easy for field technicians to identify symptoms and possible causes for rapid problem resolution. For example, WiFi Analyzer can capture unusual traffic generated by 802.11-enabled consumer electronic devices that deviate from standards, enabling deeper analysis. Spectrum XT can be used to pinpoint the location of any smart device emitting spurious RF energy. Without tools such as these, technicians can spend many hours or days chasing troubles caused by oddball consumer devices that are not instrumented for enterprise-class Wi-Fi logging, reporting, or troubleshooting. To help optimize the network for BYODs and to easily locate rogue devices, AirMagnet WifiAnalyzer PRO uses BYOD Classification. This functionality allows IT staff to categorize smart devices that are detected in the air space enabling IT to quickly and efficiently know the details about smart devices on the network including the OS and model name.

ABOUT NETSCOUT

NETSCOUT SYSTEMS, INC. (NASDAQ: NTCT) is a market leader in real-time service assurance and cybersecurity solutions for today's most demanding service provider, enterprise and government networks. NETSCOUT's Adaptive Service Intelligence (ASI) technology continuously monitors the service delivery environment to identify performance issues and provides insight into network-based security threats, helping teams to quickly resolve issues that can cause business disruptions or impact user experience. NETSCOUT delivers unmatched service visibility and protects the digital infrastructure that supports our connected world.

Conclusion

Employees want to bring their own mobile wireless devices to the office, and businesses have much to gain by embracing this trend. A growing number of organizations are moving in this direction by recommending applications for safe productive use of BYODs or using mobile device managers to enroll them. While such measures can help, they do not by themselves address the multitude of impacts that BYODs have on enterprise WLAN performance, security and compliance. As we have shown, factoring all smart devices - including BYODs – into the WLAN lifecycle at every step fills this gap by proactively avoiding costly problems and simplifying trouble resolution.

NETSCOUT's AirMagnet solutions can play an instrumental role throughout the WLAN lifecycle, helping employers to bring BYODs into the fold. To learn more about AirMagnet wireless solutions and features that facilitate detection, planning, compliance monitoring and troubleshooting of all smart devices (no matter who owns them), visit enterprise.netscout.com/wlan

About the Author

Lisa Phifer is President of Core Competence, a leading-edge technology consulting firm. She has been involved in the design, implementation, and evaluation of network and security products for 30 years. At Core Competence, Lisa advises companies large and small regarding security needs, product assessment, business use of emerging technologies, and best practices. She often teaches about wireless LANs, mobile security, and vulnerability assessment, and has written for numerous publications, including TomsITPro, SearchConsumerization, Wi-Fi Planet, Information Security Magazine, SearchNetworking, and Information Week. An AirMagnet user since 2002, Lisa contributes frequently.

NETSCOUT

Americas East
310 Littleton Road
Westford, MA 01886-4105
Phone: 978-614-4000
Toll Free: 800-357-7666

Americas West
178 E. Tasman Drive
San Jose, CA 95134
Phone: 408-571-5000

Asia Pacific
17F/B
No. 167 Tun Hwa N. Road
Taipei 105, Taiwan
Phone: +886 2 2717 1999

Europe
One Canada Square
29th floor, Canary Wharf
London E14 5DY, United Kingdom
Phone: +44 207 712 1672

NETSCOUT offers sales, support, and services in over 32 countries.

For more information, please visit enterprise.netscout.com or contact NETSCOUT at 800-309-4804 or +1 978-614-4000