Brochure

A holistic approach to your BYOD challenge

HP BYOD solution

Introduction

As more and more enterprises like yours begin to see significant benefits from allowing employees to choose the device they use to get their jobs done, more companies are adopting bring your own device (BYOD) initiatives. In fact, a CIO survey conducted at Gartner Summits held in the United States and Europe indicated that, by 2014, 80 percent of the global workforce will be eligible to participate in a BYOD program.[1] While the BYOD trend increases flexibility and productivity, it introduces a host of new challenges for your IT administrators.

A key concern for IT is how it can effectively secure and manage the network and application access for personally-owned devices. User-owned devices cannot easily be identified, and therefore managed by your IT department. When employees, customers, or visitors bring in their own devices, IT loses control because it does not know where the device has been, what applications the user has downloaded, or what device has been introduced into the network. Beyond that, the health of the device is unknown, which creates a big risk when the mobile device connects to your enterprise business network and accesses vital applications and information.

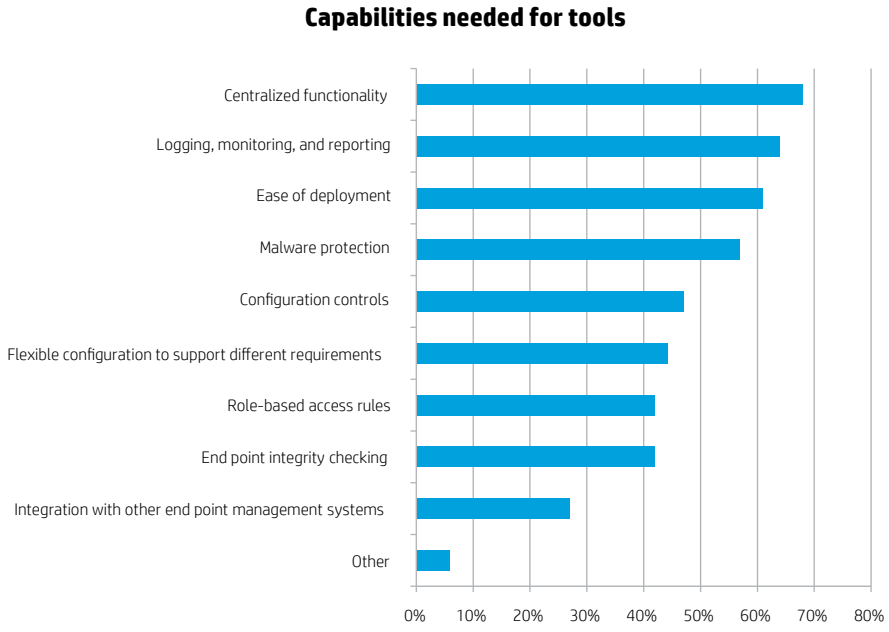
Mobile devices, even if company issued, routinely travel outside the company perimeter and are inevitably used for personal reasons. Rising Internet threats, security attacks, and lost or stolen devices introduce new vulnerabilities and potentially expose confidential business information. Security breaches can tarnish your organization's reputation and cost immeasurable goodwill. It can also put your organization at risk of violating industry as well as private and public regulations.

Security is not the only challenge to successfully implementing a BYOD initiative. Your enterprise might still rely on traditional infrastructure management tools that are not designed to provide the flexible access policies that personally-owned devices require. The influx of 802.11n Wi-Fi devices also places increased demands on your enterprise network, necessitating design changes. For instance, Gartner predicts that organizations deploying Apple iPad devices without proper planning will need 300 percent more Wi-Fi.[2] This can significantly impact your network performance, unless it has been taken into consideration when designing your WLAN.

Last but not least, there is the challenge of introducing another management platform into your already crowded IT manager's tool belt. User-owned devices span wired and wireless networks, including laptops, smartphones, and tablets. Your enterprise needs to think beyond BYOD access and consider the critical need to have unified visibility, concurrent control of wired and wireless networks, WLAN scalability to support new BYOD devices, as well as user access and network monitoring to eliminate possible errors and to simply streamline your overall network management.

1 "Creating a Bring Your Own Device (BYOD) Policy," Michael Disabato, Gartner, April 2012.
2 "Without proper planning, enterprises deploying iPads will need 300% more Wi-Fi," Tim Zimmerman Gartner, October 2011.

Figure 1. Tools needed for mobile security solutions



Three essentials for BYOD

Based on a recent **SANS mobility/BYOD security** survey of 500 IT professionals[3] the top three priorities that organizations are looking for in a BYOD security solution (see figure 1) are:

1. Centralized functionality
2. Logging, monitoring, and reporting
3. Ease of deployment

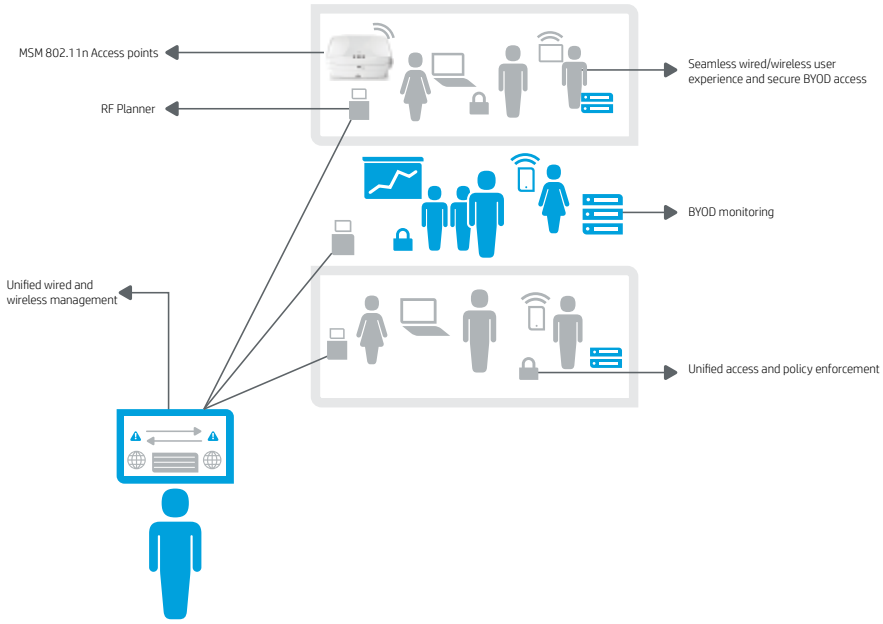
From an IT perspective it is clear that an effective BYOD solution should simplify deployment by converging network management with the administration and enforcement of access policies based on device, user, or access method. An effective BYOD solution should also automate your user/device on-boarding process to minimize user disruption and offer real-time reporting of your BYOD traffic and security to optimize resource allocation and quickly measure, enforce, and meet compliance mandates.

Unified network with flexible policy-based access delivered by single pane of glass management

The HP BYOD solution pivots around HP Intelligent Management Center (IMC), which offers you a single-pane-of-glass network management solution that delivers complete visibility across your entire enterprise network, from the data center to the network edge. IMC goes beyond BYOD by delivering converged management across various networks—physical and virtual, wired and wireless, and applies the appropriate security policies to the users and devices (personal or company-owned) accessing your network. HP IMC's modular design integrates traditionally separate management tools, network services, policy management, and user and traffic monitoring that delivers to your enterprise a single-pane-of-glass tool to centrally manage and secure the wired and wireless infrastructure.

3 Co-sponsored by HP security products

Figure 2. HP end-to-end BYOD solution



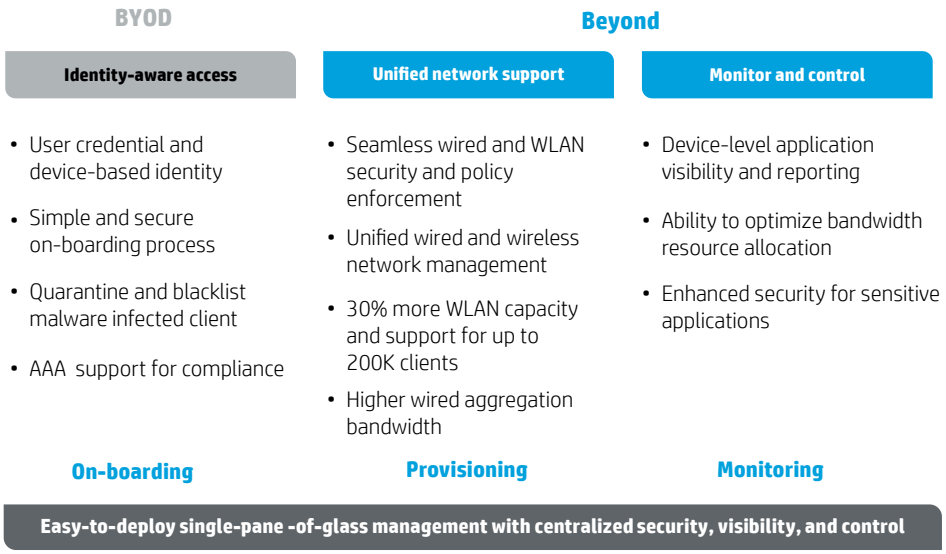
For granular network and application access, HP IMC manages user access control and identity-based policies to help your IT managers overcome the complex security challenges associated with the widespread adoption of user-owned devices. Your IT administrators can establish and enforce granular and consistent network access policies for wired and wireless users to protect your IT assets, mitigate risks, optimize network availability, and ensure regulatory compliance.

HP IMC provides a comprehensive BYOD solution that supports wired and wireless device on-boarding, provisioning, and monitoring. Deployment of the BYOD solution delivered through IMC comes with ease because of IMC's modular design. The modular design gives you the flexibility to add functionality as needed without the need to deploy separate management tools.

"It is no longer acceptable to have two different network management applications or differing guest access applications. Unifying network service applications reduces complexity by providing a single display and reduces costs associated with redundant solutions."

Source: "A unified access layer forces changes to infrastructure thinking at the edge of the network," Gartner (analysts: Tim Zimmerman and Mark Fabbi), March 2012.

Figure 3. BYOD and beyond—a holistic approach



Mobile device on-boarding

IMC supports user authentication based on identity, device location, time, and endpoint security health. Users can be assigned automatically into the appropriate VLAN based on their identity, device type, device posture, time of day, application type, or other factors. Access to the network can be granted based on a device's IP or media access control (MAC) address, which is particularly useful for printers, IP phones, and barcode scanners.

Because IMC centralizes network access and policy enforcement with network management capabilities, your IT administrators can integrate, correlate, and collaborate user and network device management from a single platform. By providing authentication and authorization for devices accessing your network, IMC helps you reduce vulnerabilities and security breaches.

IMC fully supports the IEEE 802.1X network access control standard and leverages HP advanced fingerprinting technologies for Apple iOS and Android devices and comes with a self-registration portal for guests and personally-owned device to automate the on-boarding process and reduce the administrative burden so that you can support your organizations' BYOD initiatives quickly and easily.

Provisioning

You can further minimize security risks through HP IMC-integrated security policy management and endpoint posture assessment. This allows your administrators to control end point admission based on the device's identity and posture. If an endpoint is not compliant with the established policies, access to the network can be isolated for remediation or blocked to protect your network assets. IMC security policy component further provides non-intrusive actions to secure your network edge proactively, including end point monitoring and notification. This component also supports security evaluation, security threat location, and security event awareness. To ensure continued security HP IMC policy component continually monitors each end point's traffic, installed software running processes, and registry changes. These functions enable all end points connected to your network to be secure.

Monitoring

With HP IMC, administrators will have full visibility into what users are accessing from personal and company issued devices. Since IMC can provide information regarding what users have accessed from their device, you will be able to differentiate between business oriented access versus recreational access. Integration with network resource usage data such as network address translation (NAT), flow records provide you with full visibility of BYOD traffic and compliance reporting. Based on this data, you can set the appropriate network access policies, manage network resources and capacity more effectively across wired and wireless networks.

High-performance wireless to support today's mobile devices

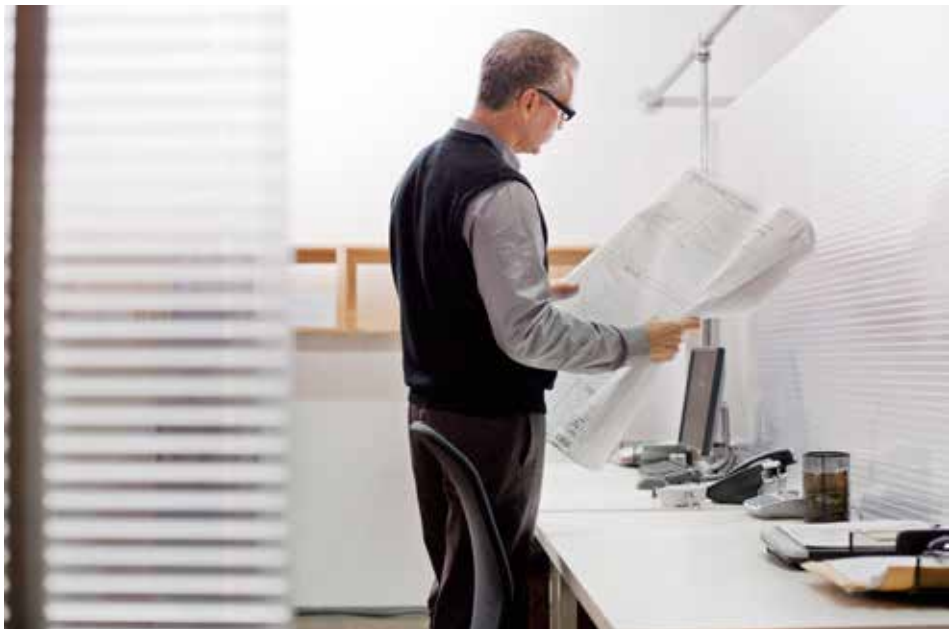
HP MultiService Mobility (MSM) access points and wireless controllers deliver the wired-like performance and scalability needed to support your mobile workers, who rely heavily on smartphones, tablets, and laptops. We offer a portfolio of high-performance mobility solutions, including dual-radio three spatial stream 802.11n access points that provide you near gigabit client access and support nearly twice the number of users compared to two spatial stream access points. You can leverage HP radio frequency (RF) optimization features such as beam forming and band steering to optimize client performance and move 5GHz-capable clients to the less congested 5GHz spectrum. This leaves the 2.4 GHz for clients that are not 802.11n capable, increasing your overall network capacity. Your IT administrators can also use channel bonding in the 5GHz spectrum to double effective throughput for high-bandwidth applications and BYOD traffic.

HP non-blocking WLAN architecture combines centralized management and control with flexible forwarding options, and intelligent access points at the edge of the network to deliver unparalleled scalability and application performance to your mobile users.

HP Wi-Fi Clear Connect software further improves the coverage and performance of your wireless network by automatically adjusting to changing RF conditions and mitigating RF interference. You get a better performing, more reliable Wi-Fi network at a lower cost.

Wi-Fi Clear Connect also helps you improve your users' Wi-Fi experience by dynamically balancing the client load across access points.

HP RF Planner allows you to model WLAN coverage accurately by factoring in variables, such as physical features, building materials, and WLAN equipment characteristics. With RF Planner, your network architects can ensure that your 802.11n network is optimized for the dense mobile environments that support today's mobile workers and tablets.



Conclusion

With HP IMC, you can move beyond BYOD access to efficiently manage your entire converged network infrastructure, secure personally-owned devices, and monitor BYOD traffic. You can enjoy ease of deployment, low operational costs, and strong and consistent security. Simplified NAC allows you to easily and securely support employees', partners', and guests' tablets, notebooks, smartphones, and other mobile devices on your campus network while holding the line on operational expenses. With HP, mobility is based on open standards, simple to deploy and easy to manage.

HP Networking warranties, support, and services

Warranties
HP has a broad, customer-focused portfolio backed by equally robust warranties, from lifetime warranties through competitive one-year warranties. Details of the HP Hardware Limited Warranty Statement and product coverage are available at hp.com/networking/warranty.

Support
To ease implementation, use and maintenance, HP products are also supported by self-help tools, including electronic case submission and software updates. These are available 24x7 on the Web, via telephone and by email. Details can be found at hp.com/networking/support.

Services
Product and solution services from HP and HP Authorized Channel Partners help you manage your office environment as it evolves, decrease operational costs, and protect data while reducing risk. Services include HP Care Pack Services, a portfolio of packaged, affordable, proven services that scale to meet your needs and offer complete technology lifecycle support—and expert advice—all at an affordable price. More information is available online at hp.com/go/carepack.

Financial Services
HP Financial Services provide innovative financing and financial asset management programs to help you cost-effectively acquire, manage, and ultimately retire your HP solutions. Further information on these services can be obtained from an HP representative or online at hp.com/go/hpfinancialservices.

Global citizenship at HP

Developing solutions to major social and environmental challenges
hp.com/hpinfo/globalcitizenship

Learn more

Think BYOD and beyond. Enable unified access and management of your wired and wireless network. Visit hp.com/networking/byod

Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document

4AA4-0638ENW, February 2013