White Paper

A Roadmap for BYOD Adoption

By Jon Oltsik, Sr. Principal Analyst, and Bob Laliberte, Sr. Analyst

April 2012

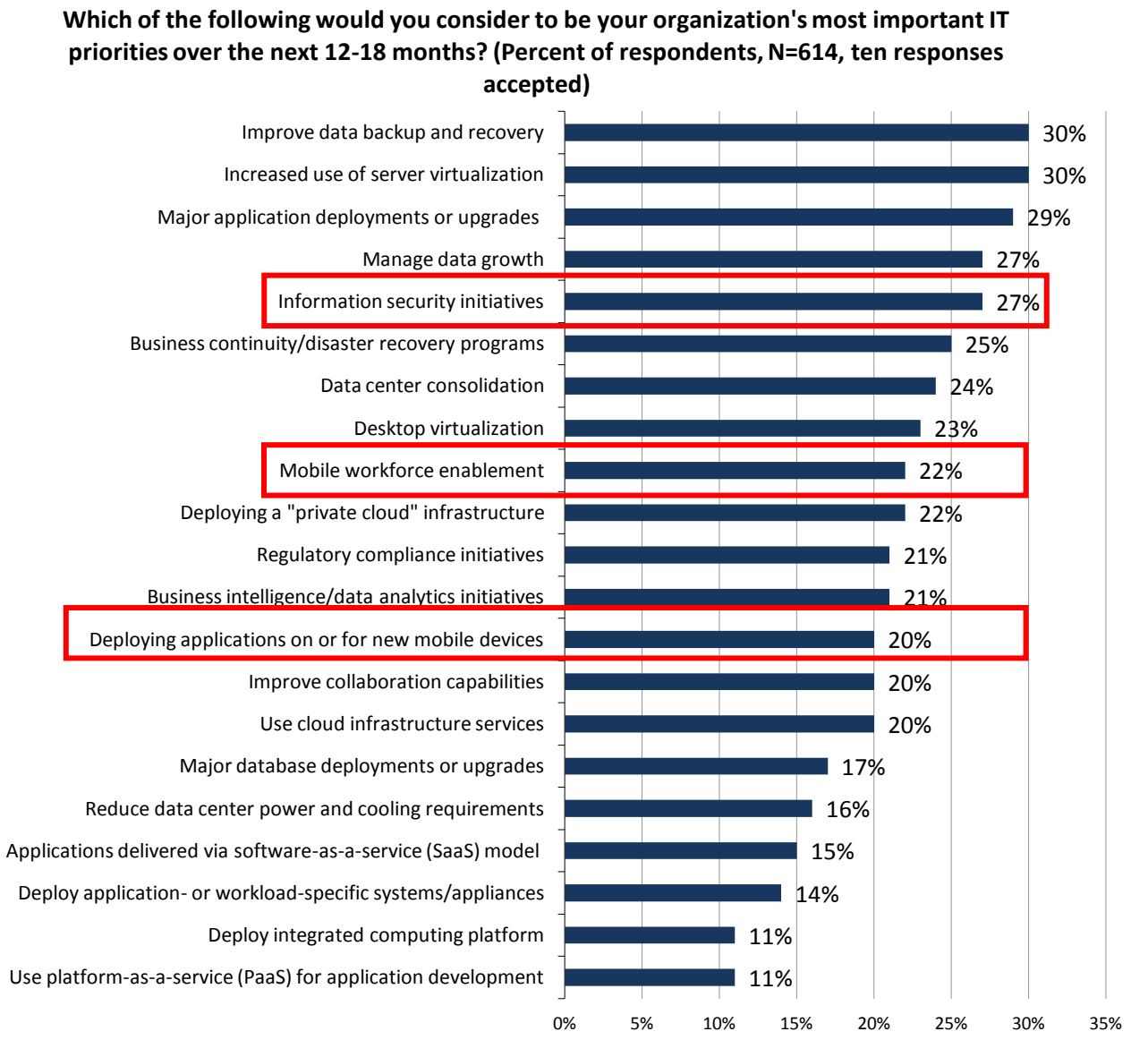
This ESG White Paper was commissioned by Enterasys and is distributed under license from ESG.

Contents

Introduction

Organizations of all sizes are being impacted by the consumerization of IT: empowered by smartphones and tablet computers, more employees bring their own devices to the workplace and expect to use them for communication, productivity applications, and even personal use. As a result, IT organizations are forced to deal with a rapidly growing population of wireless devices in the workplace, many of which are unauthorized. While struggling to understand the ramifications of this influx of new devices, businesses are also working to embrace these new technologies. According to ESG research, respondents list enabling a mobile workforce as a top ten IT priority for 2012. Furthermore, information security initiatives and deploying applications on or for new mobile devices also ranked highly, as shown in Figure 1.[1]

Figure 1. Top IT Priorities for 2012



Source: Enterprise Strategy Group, 2012.

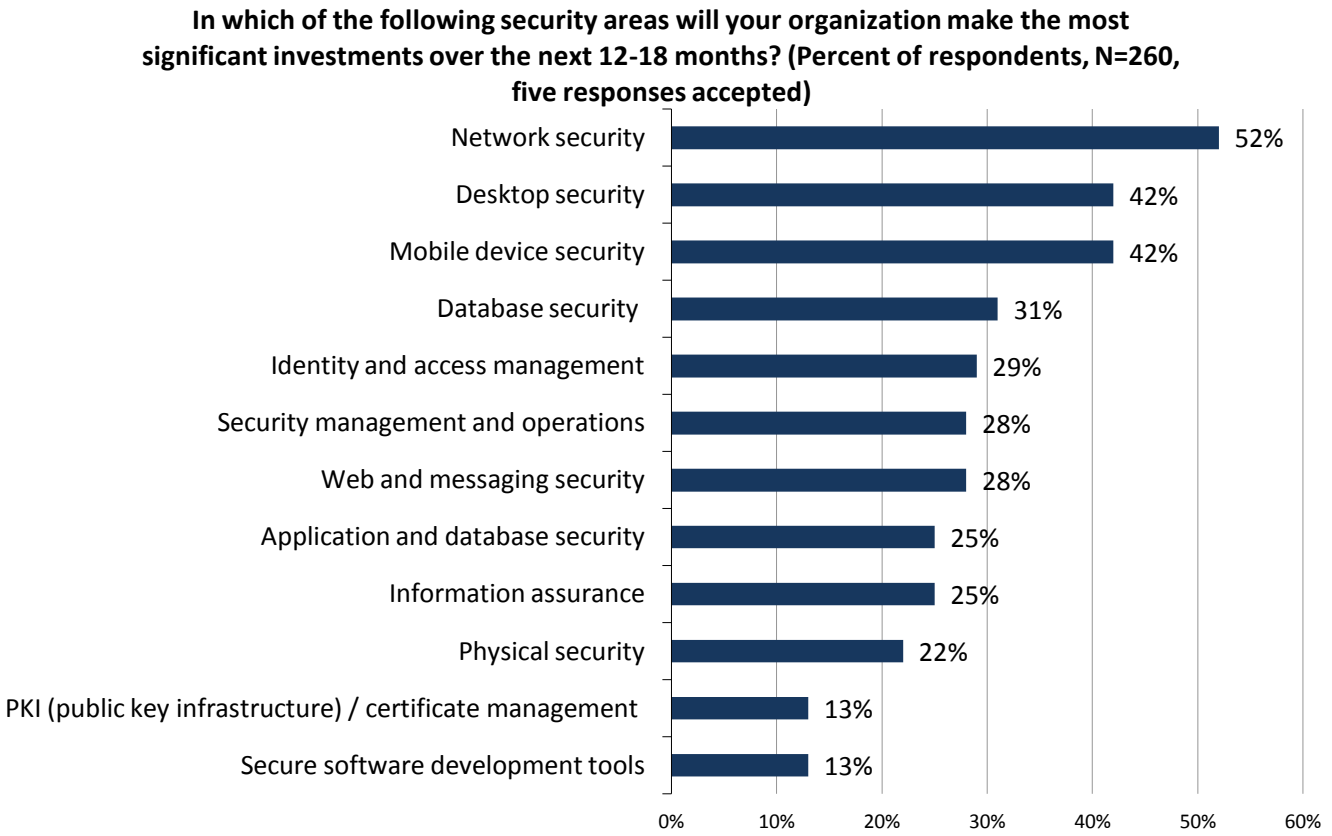
Indeed, what started as a bring your own device initiative, or BYOD, has morphed into BYO3 or more as employees (and students) now have an assortment of mobile devices that typically include a smartphone, tablet, and PC. For colleges and universities, this list expands to include gaming devices that require wireless access, while hospitals

[1] Source: ESG Research Report, *2012 IT Spending Intentions Survey*, January 2012.

enable a number of medical devices over WLANs. As a result, campus networks across these and other verticals are being inundated by devices requesting network access.

With so many new devices requiring access to networks, organizations need to be able to handle the influx safely and securely. This is driving network and security teams to assess new risks and implement new controls. Indeed, ESG research indicates that significant investments will be made in network security, desktop security, and mobile device security to cope with the consumerization of IT (see Figure 2).[2] Also of note is the need to invest in identity and access management solutions, and in better security management and operations.

Figure 2. Top Security Investments



Source: Enterprise Strategy Group, 2012.

BYOD, coupled with increased focus on the network and mobile devices, will force organizations to require greater levels of visibility and control. These edge networks will need to go beyond simple connectivity to be capable of handling device registration, device profiling, on boarding, policy-based management, and enforcement. Automation will also play an important role as the network scales.

Health Care and Higher Education

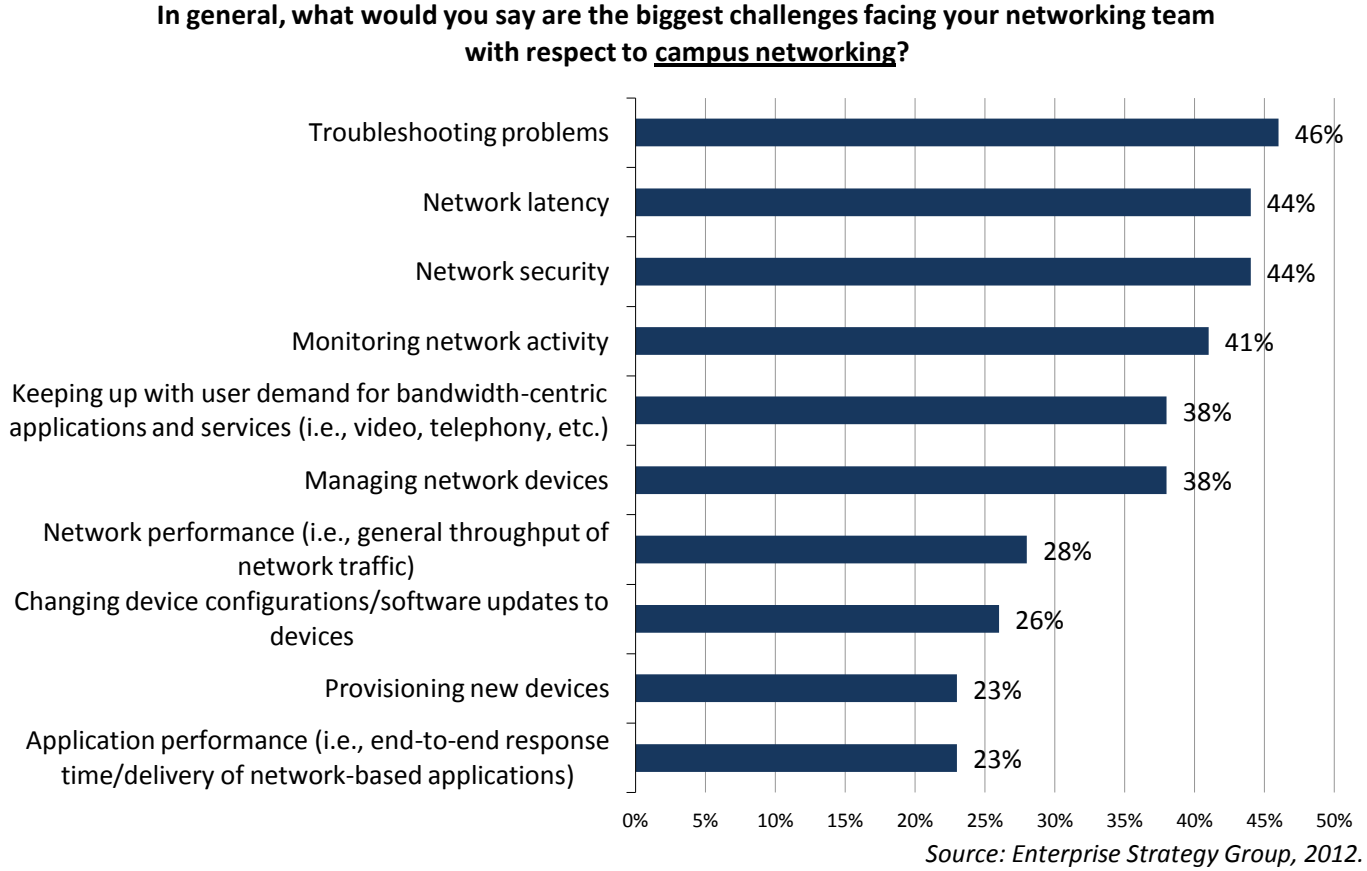
BYOD environments are highly prevalent in health care (highly mobile users with multiple devices) and higher education (multiple devices including smartphones, tablets, game consoles, and PCs). However, there is a tremendous difference in how these environments need to be deployed. Compliance in health care is very important and as a result organizations may leverage different strategies for addressing the BYOD issue. For example, in order to better control and secure the data, a hospital may deploy a virtual desktop environment, whereas a college or university may choose to support devices natively. Regardless of the approach taken, these environments will typically require different security zones and a context-based, policy-driven approach, based on the individual requesting information and even potentially where they are located.

[2] Source: ESG Research Report, *2012 IT Spending Intentions Survey*, January 2012.

Campus Network Challenges

Simply adding more wireless mobile users to a network sounds like a simple task, but given the existing challenges in a campus network, the BYOD trend could break an already strained environment. According to ESG research, campus networks are already creating a number of significant challenges for network operations teams (see Figure 3).[3] On top of the list, organizations are challenged by troubleshooting problems, network latency, and security. It is not surprising that troubleshooting is a top concern: networking professionals in higher education tell ESG that bursty traffic from student gaming systems and online video consumed by mobile devices saturate campus networks from various access switches in unpredictable patterns. Adding even more mobile devices will only exacerbate these issues. The larger and more complex the environment becomes, the harder it will be to rapidly isolate problems and guarantee security. Plus, new bandwidth-hungry applications and services like video are difficult to support on mobile devices. In other cases, simply monitoring network activity can be problematic, yet very important: if organizations don't know what is consuming bandwidth, it will be difficult to establish QoS for applications or by user group.

Figure 3. Biggest Campus Network Challenges



Source: Enterprise Strategy Group, 2012.

In addition to the challenges listed above, organizations also need to be concerned with the following:

- Re-architecting workflows. Depending on the path taken to enable BYOD, significant redesign of existing workflows or the creation of new ones may be required. For example, will business unit managers or HR be required to approve mobile devices? Are there any compliance issues that need to be considered prior to granting access, etc.?
- Registration, access and onboarding. Organizations need to determine how they will handle the lifecycle of registration of mobile devices on the network. A number of factors need to be considered, including

[3] Source: ESG Research Brief, *Will Intelligent Management Aggregation Networks (iMAN) Become Mainstream?* February 2012.

employment status, partner status, or even guest status. While guest access should be fairly straightforward, employee and partner access may differ based on their roles. The onboarding process should be easy to use and intuitive, helping to facilitate access. Organizations need to have a common policy-based approach to overcome potentially complex manual processes. This could be even more challenging for hospitals that have to protect patient privacy while allowing medical professionals access or higher education that needs to separate faculty from students.

- Setting usage policies. In many instances organizations may want to restrict access to resources during a certain period of time or location. For example in higher education, IT may want to restrict access to certain resources during certain period of time for students, while allowing access to faculty or staff.
- Budget constraints. IT organizations will always be under pressure to reduce or contain costs; that will be difficult when trying to support rapidly-growing BYOD markets. Organizations should at least try to deliver predictable costs associated with mobile users so anticipated growth will be easier to budget for and understand.
- Technical resources. Finding the appropriate skill sets to properly design and implement a scalable network infrastructure to handle BYOD can be difficult. In many instances, employees are learning on the job, which can result in missteps and setbacks. Organizations need to consider leveraging the talents of outside services organizations to help accelerate the time to value for their BYOD environment.

When trying to accommodate BYOD initiatives, organizations can take a number of different approaches to handle this problem. For example, many choose to control access by having mobile users register via a Web page in order to gain access to the network. The network will then provide access and services based on policy and role. Other organizations may decide to centralize desktop applications and deploy a virtual desktop to users at corporate locations like call centers, or even for remote users at home. Increasingly, organizations are also turning to mobile device management (MDM) solutions to gain control of content on a device (e.g., remotely wipe the device if lost or stolen). These approaches can also lead to additional management, security, and even infrastructure challenges. Organizations need to take a unified approach that can leverage existing skills, infrastructure, and management solutions.

The BYOD Journey Should Start with a Fabric Approach

Highly virtualized and dynamic environments require any-to-any non-blocking network connectivity in order to handle shifting demand and meet end-to-end performance requirements. This equates to a network fabric architecture. While most often aligned with data centers, network fabrics need to extend beyond the data center and cover the campus environment as well. The any-to-any fabric goes beyond host to host or host to storage, and extends to the end-users as well.

By creating an underlying architecture that offers any user the ability to access any application, organizations can rapidly adjust to changing business needs. Given the pace of business, many can't afford to wait for the network team to reconfigure network infrastructure or, worse, deploy new circuits in order to handle a service request. Organizations should also consider:

- Integrated wired and wireless. For BYOD environments, a big part of creating that network fabric is the inclusion of the wireless network. Creating a unified or common fabric that spans wired and wireless networks can guarantee any-to-any connectivity regardless of device or location, and ensure quality of experience into the cloud. It will also ensure common policy enforcement across wired and wireless networks, so no matter where or how a user assesses the network, the same policies will apply.
- Automated policy-based decision making. Given the sheer volume of mobile devices requesting network access, attempting any type of manual approval process is folly. Organizations need to apply automation and policy-based decision making in order to keep up with the influx of devices. Most importantly, these policies need to be context-based and the automation should be focused on the registration process,

determining the appropriate level of access and security based on the the role of the individual requesting access.

- Open architectures. Organizations have the flexibility to adopt multiple technologies to approach the BYOD problem. Management software should be flexible enough to integrate with those technologies. This could include APIs to connect to virtual desktop infrastructures (VDI), or mobile device management (MDM) technologies for better management and the ability to integrate additional services like threat management, voice, video, location-aware services and application visibility, which are becoming much more popular.
- Applications and services to mobile users. As mentioned, organizations need to think about this in terms of connecting users on their mobile devices to the appropriate applications and services they need to be productive. Just providing a connection to the Internet may be fine for guests, but employees and partners may need access to a number of applications, so the end-to-end path needs to be considered. It will also be important to have the appropriate security measures in place (VLANs, ACLs, firewalls, etc.) so that only approved users can access certain applications. Even then, usage should be closely monitored.
- Ease of use. As the BYOD environment continues to scale, solutions that are easy to use and have simple intuitive interfaces will be necessary as IT budgets and headcounts will most likely not scale at the same pace. That means that the same or fewer IT staff members will need to manage a rapidly scaling BYOD environment. A good user interface will go a long way in this regard.

The Enterasys Roadmap for BYOD

Enterasys recognized the issues facing organizations responding to the BYOD trend and has responded with a comprehensive approach to address the challenges. Its roadmap for BYOD includes a combination of technology and services to enable organizations to quickly and effortlessly deploy a solution to accommodate any approach that will scale to meet future needs. Based on the OneFabric concept, these modular offerings can be deployed together to form a comprehensive solution, or individually as time and budget allow. The main components of the Enterasys solution include:

- A single end-to-end fabric solution. Enterasys has created OneFabric to enable organizations to deploy a comprehensive end-to-end fabric in modular components. The company first launched OneFabric Data center and then quickly followed with OneFabric Edge, which cover both wired and wireless networks in the campus environment. These solutions provide the any-to-any connectivity required by a dynamic environment.
- An integrated security solution. Enterasys OneFabric Security provides an architecture that is well suited to address the BYOD problem. It provides the requisite visibility and management, spanning the data center to the mobile devices. This includes auto discovery, flexible on-boarding, guest access, multi-level device profiling, context-based policy management, and integration with VDI, MDM, and threat management solutions. A key piece of this architecture is the Enterasys Mobile IAM, which delivers:
    - Auto discovery, multi-level device profiling, flexible on-boarding, context-based policy management, and guest access management for up to 3,000 devices. The solution is capable of scaling up to 100,000 devices in increments of either 500 or 3,000.
    - Comprehensive software for identity, access, and inventory management; a single user interface (UI) for end-to-end management; auditing and reporting capabilities; and context-based policy enforcement.
    - Flexible deployment options; Mobile IAM can be deployed as a physical or virtual appliance.
    - Context-based policy: One of the largest attributes of a BYOD environment is that different users are likely to be doing very diverse tasks on a variety of devices—usually determined by external factors such as where they are physically performing the task, the time of day, or the role they play in their surroundings.

- Guaranteed services. Mobile IAM guaranteed professional services help accelerate the time to value for deploying and making the Mobile IAM operational. For organizations struggling to deal with day to day operations and deploy new technologies, these services will greatly reduce the time and stress involved with bringing a platform online. Additionally, the professional services teams can also facilitate the integration of MDM, VDI, and firewall solutions to Mobile IAM.
- Predictable pricing. Enterasys is trying to simplify the process of supporting BYOD initiatives by making pricing predictable and simple. A per device charge starts as low as $5 per device. To further simplify the process, Enterasys offer a free initial scoping and assessment service.
- Integration with MDM and VDI. The Enterasys BYOD solution can be tightly integrated with VDI and MDM systems providing a complete solution for securing, managing, and onboarding the mobile device user. This approach significantly cuts down the time requirements placed on IT support for onboarding and troubleshooting while at the same time enhancing the end-user experience.

The Bigger Truth

The consumerization of IT shows no signs of abating, and BYOD initiatives are rapidly becoming BYO3 as individuals augment their laptops with smartphones and tablets. While having multiple tools may prove to be personally advantageous, they create significant challenges for the IT organizations trying to support them. Given the size and scope of BYOD, it is not advisable to approach this in a piecemeal fashion. Because of the potential network impact and security threats, organizations should be taking a more strategic approach.

While approaches to handling BYOD can vary, it is clear that the underlying infrastructure needs to be able to rapidly adjust to changing demands and provide any-to-any connectivity. This would include the ability to deliver applications to end-users on mobile devices, so solutions should incorporate data center and campus environments, both wired and wireless.

Enterasys developed OneFabric architecture to address the networking needs of modern business. It has developed the Mobile IAM solution and designed services specifically to address the needs of BYOD environments and to accelerate the time to value. For organizations deluged by BYOD dilemmas in need of a comprehensive, secure, and scalable solution, Enterasys should be on the short list.

Enterprise Strategy Group | **Getting to the bigger truth.**

20 Asylum Street | Milford, MA 01757 | Tel: 508.482.0188 Fax: 508.482.0218 | www.enterprisestrategygroup.com