White Paper

A Roadmap for BYOD Adoption

By Jon Oltsik, Sr. Principal Analyst
with Kyle Prigmore and John McKnight

December 2014

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

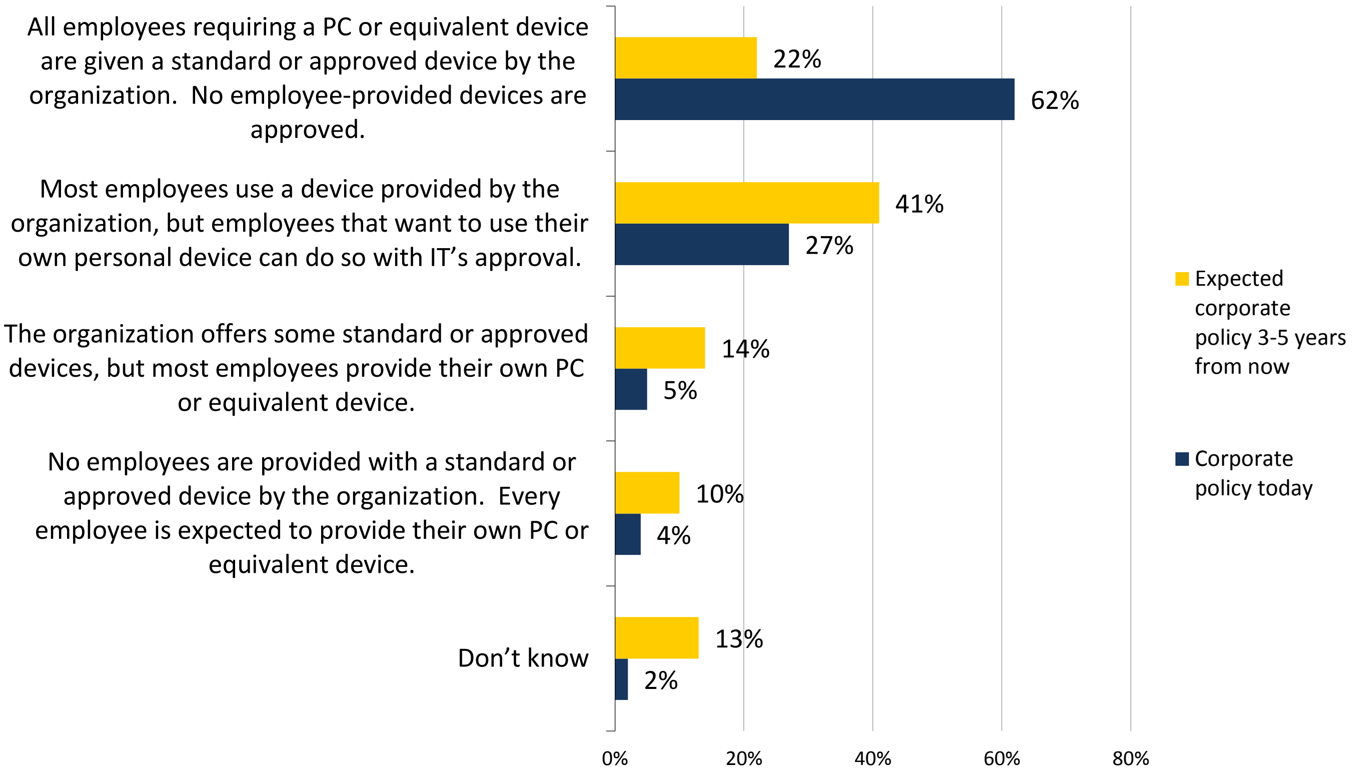
Contents

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. Indeed, previously conducted ESG research revealed that nearly one-third (32%) of organizations surveyed already employ a hybrid model in which IT provides endpoint devices to employees who want them, but also supports outside devices for those workers who would prefer to use a device of their choosing (see Figure 1).[1] Fast forward a few years and the number of organizations taking this dual-pronged approach is expected to nearly double to 55%; conversely, less than one-quarter (22%) will maintain their ban on all non-IT approved devices. Bottom-line: BYOD has arrived and it's not going anywhere.

Figure 1. Corporate Endpoint Device Policy: The Shift from Company-issued to Employee-provided

Which of the following best describes your organization's policy with respect to providing your employees with a PC or other core endpoint computing device they need to do their job? How will this change over the next 3-5 years? (Percent of respondents)



Source: Enterprise Strategy Group, 2014.

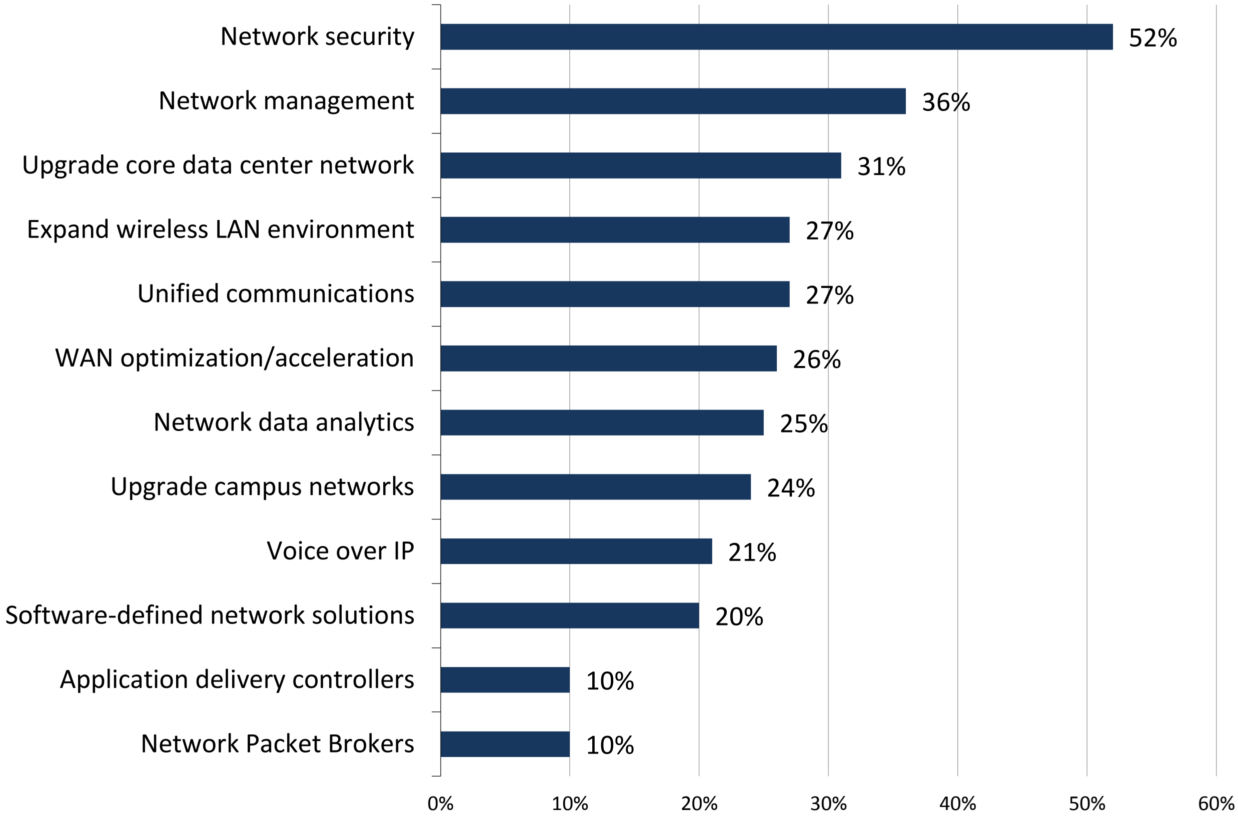
Indeed, what started as a bring your own device initiative, or BYOD, has morphed into BYO3 or more, as employees (and students) now have an assortment of mobile devices that typically include a smartphone, tablet, and PC. For colleges and universities, this list expands to include gaming devices that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

[1] Source: ESG Research Report, *Mobile Device and Application Usage Trends*, August 2013.

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 many organizations are prioritizing investments in solutions that fortify network security and management capabilities (see Figure 2).[2]

Figure 2. Areas for Network Infrastructure Investments

We would like to learn a bit more about your specific spending plans for network infrastructure in 2014. In which of the following areas will your organization make the most significant investments over the next 12 months? (Percent of respondents, N=301, five responses accepted)



Source: Enterprise Strategy Group, 2014.

BYOD, coupled with an 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, onboarding, 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.

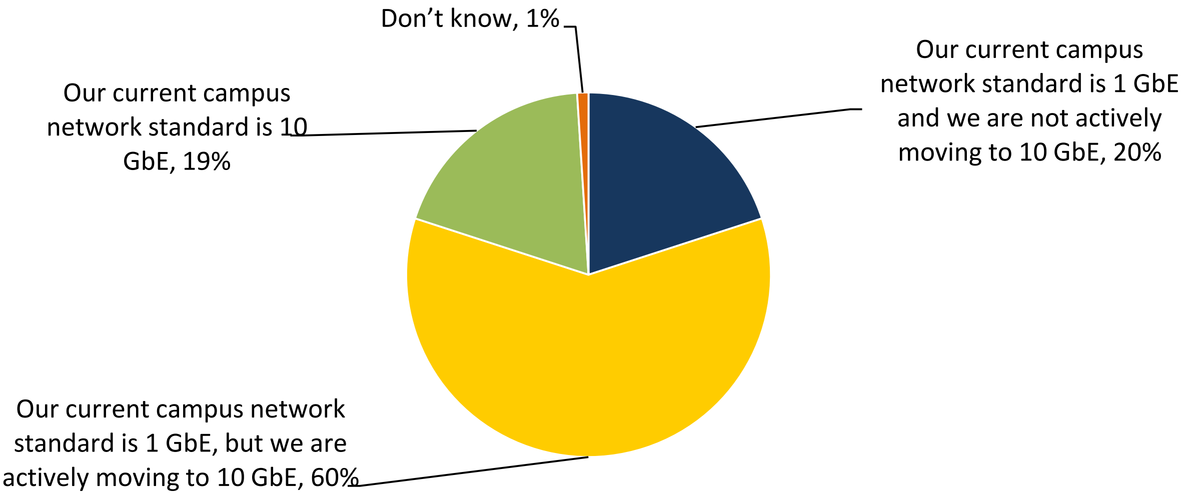
[2] Source: ESG Research Report, *2014 IT Spending Intentions Survey*, January 2014.

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. Modern campus networks also have to deal with a surge in new bandwidth-intensive applications, an increase in the number of computing devices, and—in general—more data traversing the campus. To cope with this rising tide of network traffic, organizations are taking steps to upgrade their wired campus networks. In fact, Figure 3 reveals that more than three-quarters (79%) of organizations said that they have either already standardized on 10 GbE (19%) or are actively planning a move from 1 GbE to 10 GbE (60%).[3] Probing further, 61% of these respondents attributed their move—or expected move—to 10 GbE to a proliferation of bandwidth intensive applications and/or endpoint devices, the latter attributed to BYOD initiatives.

Figure 3. Organizations' Campus Network Standards

Which of the following best represents your organization's wired campus network standards now and in the future? (Percent of respondents, N=300)



Source: Enterprise Strategy Group, 2014.

In addition to increased bandwidth requirements, 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 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 institutions that need to separate faculty from students.

[3] Source: ESG Research Brief, *Campus and Wireless Network Trends*, August 2014.

- 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 periods 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 Engage in a Holistic 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, ideally comprised of high-performing networking hardware and software solutions. 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 network goes beyond host to host or host to storage, and extends to the end-users accessing applications and resources in the data center or out in the cloud.

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 technologies in order to handle a service request. Organizations should consider:

- **Integrated wired and wireless networks.** For BYOD environments, a big part of creating that holistic network approach is the inclusion of both wired and wireless networks. Creating a unified network can guarantee any-to-any connectivity regardless of device or location, and ensure quality of experience to the most demanding of users. It will also ensure common policy enforcement so no matter where or how a user accesses 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 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 Extreme Networks Roadmap for BYOD

Extreme Networks recognized the issues facing organizations responding to the BYOD trend and offers 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 a software-defined architecture (SDA), Extreme Networks technologies can be deployed together to form a comprehensive solution, or individually as time and budget allow.

The main components of the Extreme Networks solution include:

- **A single unified network.** Extreme Networks' software-defined architecture combines wired/wireless edge to data center/core infrastructure hardware with a broad software portfolio. This can help enable organizations to deploy a comprehensive end-to-end network that delivers the any-to-any connectivity required by a dynamic environment.
- **Network-wide management.** Extreme Networks' centralized management console, Netsight, provides a solution designed to address the dynamic needs of IT. Netsight provides visibility and management, spanning from the data center to the unified edge. This includes auto discovery, flexible onboarding, guest access, multi-level device profiling, context-based policy management, and integration with VDI, MDM, and threat management solutions. Another potentially valuable element in Extreme Networks' SDA is their network-powered analytics engine, called Purview, which provides IT visibility to measure BYOD user engagement and experience.
- Extreme Networks Mobile IAM, the key element providing BYOD services within the SDA, which delivers:
  - Self-registration and social-login onboarding that can eliminate IT intervention.
  - Rapid and secure guest access with SMS credential delivery.
  - Active and passive onboarding and provisioning for traditional and non-traditional devices.
  - Auto discovery, multi-level device profiling, and context-based policy management.
  - Context-based policy distribution and enforcement (based on user identity, location, device type and application being used).
  - A single user interface (UI) for end-to-end management, auditing/reporting capabilities, and context-based policy enforcement.
  - Flexible deployment options (physical or virtual appliance).
- **Integration with MDM and VDI.** The Extreme Networks 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. BYOD initiatives are rapidly becoming BYO3, as individuals augment their laptops with smartphones and tablets, and the inclusion of non-traditional devices is on the horizon, as the Internet of Things becomes a reality. While having multiple tools is often to advantageous for employees, it creates 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.

Extreme Networks' software-defined architecture aims 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, Extreme Networks 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