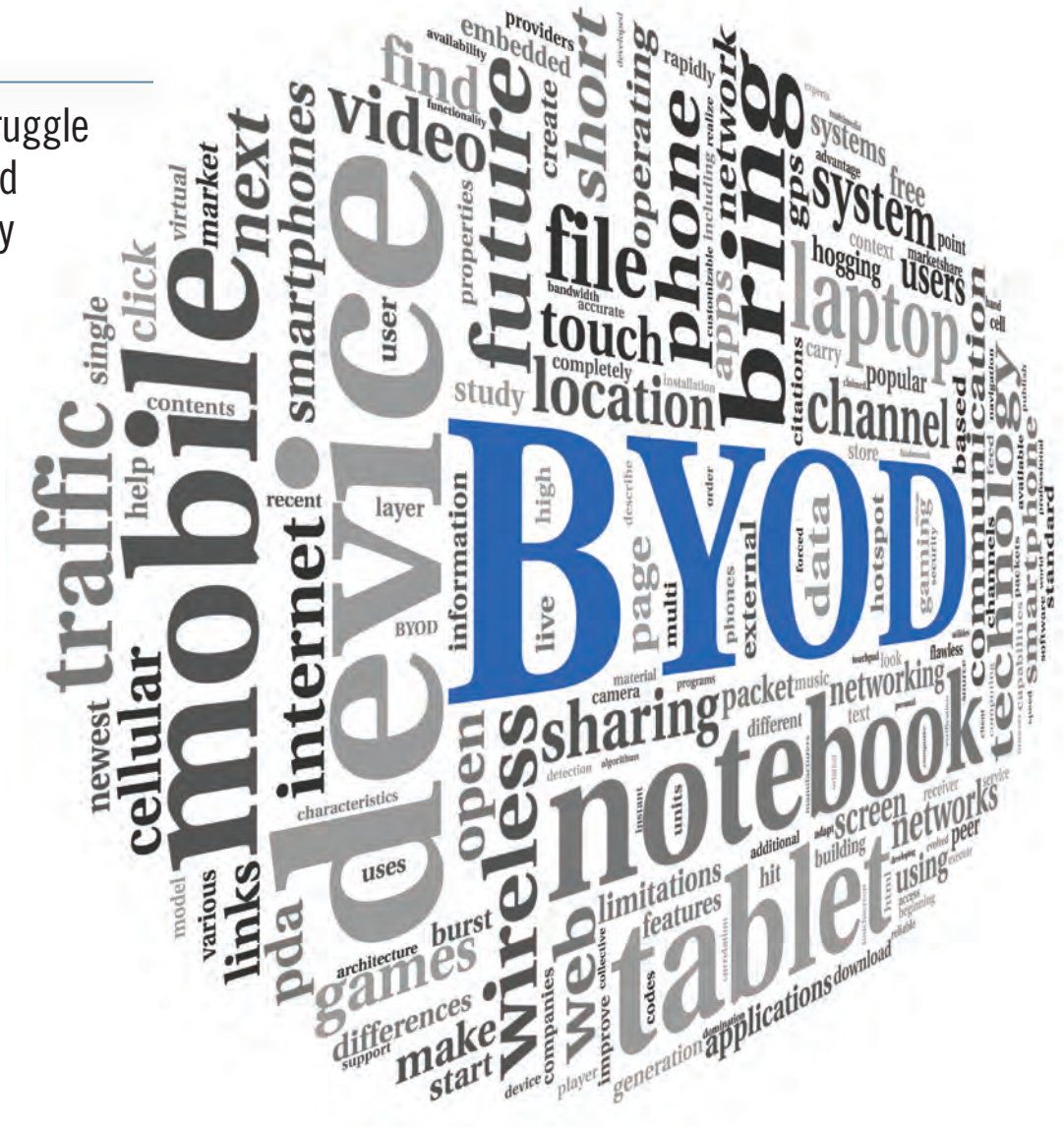
GATEPOINT RESEARCH

Top Network Considerations for Enterprise Mobility and BYOD

Survey pinpoints struggle to support BYOD and other worker-friendly technologies while achieving security & performance goals

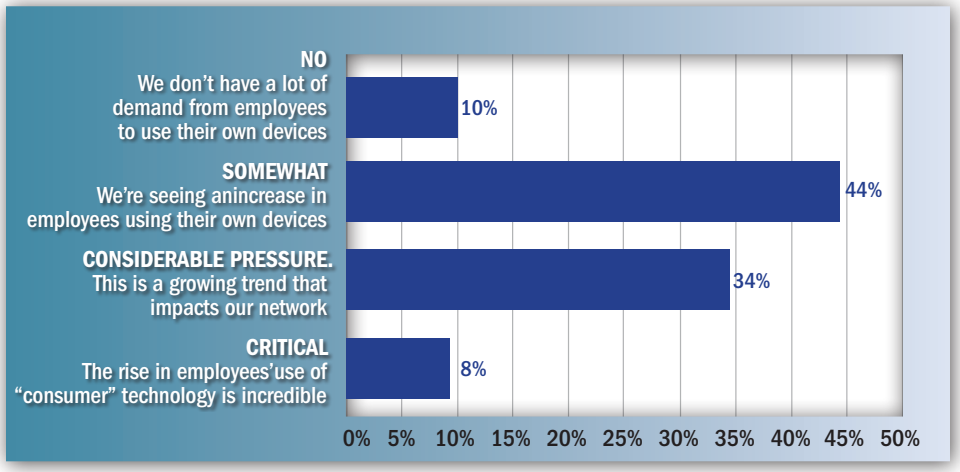


Even as IT executives and network administrators seek to increase performance and shore up defenses against misuse and increasingly sophisticated intrusions, they are under pressure to make it easier for workers to utilize the corporate network with "consumerized" technologies. The inherent conflict between these forces is increasing concern over security issues and the cost of supporting the growing array of mobile devices.

Contents

In a recent survey conducted by Gatepoint Research on behalf of Juniper Networks, 44 percent of respondents indicate they are formally supporting "Bring Your Own Device" policies. BYOD, as it is commonly referred to, allows employees (and others such as contractors and partners) to bring personal devices such as smart phones and laptops and access the corporate network to view or use enterprise resources.

Is there pressure to accommodate "consumer" technology in your IT environment?



Nine out of 10 of the survey respondents say they are feeling some degree of pressure to support BYOD, with 34 percent indicating it is considerable and 8 percent saying it is a critical issue with an incredible rise in employee use. BYOD is perhaps the epitome of the consumerization of IT movement and has expanded beyond devices to what some refer to as "Bring Your Own Technology," including applications, devices and even cloud-based services.

"There are a number of network issues that come into play with the consumerization issue," says Tina Herrera, director of campus product marketing with Juniper. "From a device perspective, network administrators want to know where has the device been and is it bringing viruses into my network. Is the device secure and will it protect the sensitive data?"

With BYOD, each type of mobile device is different and has unique vulnerabilities. Meanwhile enterprises must worry about increasingly numerous and sophisticated ways to attack each type of device. They must also defend against internal misuse of data to ensure those with legitimate access to data do not store it in an insecure manner or outright steal it.

Nonetheless, in addition to those that formally support BYOD, another 35 percent report that their companies allow network access for BYOD although they don't formally support it. For many business leaders the benefits outweigh the risks: workers are equipped to be more responsive across time zones and geographies, while the enterprise saves on hardware costs.

But somebody has to make sure that access to business-critical information is managed across an array of switching, security, routing and wireless products in a manner that meets the highest security requirements, achieves performance goals and doesn't create a management headache.

Network Implications

Today's multimedia and interactive applications present new ways of masking attacks, further increasing network vulnerability as well as soaking up bandwidth that can impact user experience for everyone on the network.

When it comes to social media such as Facebook and Linked In, network decision makers appear be flying the white flag of surrender. While just 16 percent of the respondents in the Gatepoint survey formally support use of social media apps, almost two-thirds (62 percent) allow workers to access them; only 22 percent prohibit such use. That undoubtedly reflects pressure from users who have adopted these types of services as everyday tools, whether for work or pleasure or both.

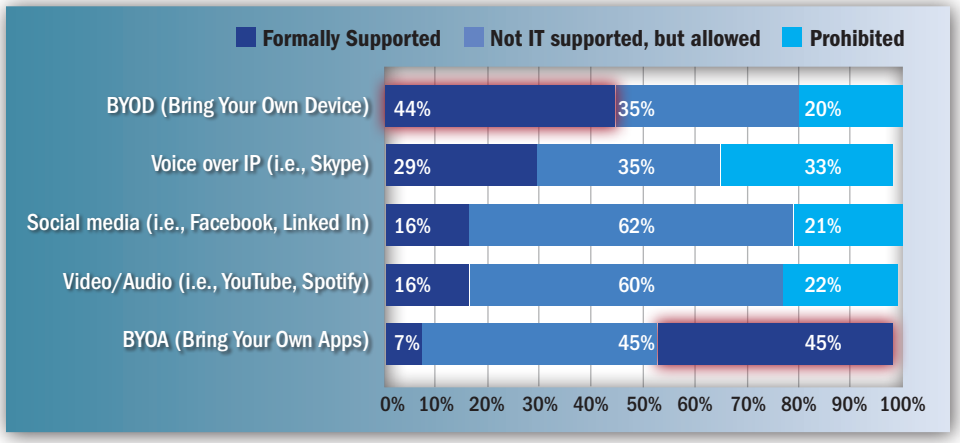
Allowing these new data types on enterprise networks creates additional pressure on administrators and architects to ensure that they are able to prioritize traffic. "IT has to be able to monitor and control that activity so that network resources and services are being prioritized for legitimate business reasons," says Juniper's Herrera. "Collaboration tools and video are very bandwidth intensive—so enterprises need to know how to prioritize and segment the traffic so that the highest priority data and the highest priority users get the bandwidth they need to be successful."

In addition to employee access, enterprise networks are expected to accommodate a rapidly growing number of partners, customers, patrons, vendors, and even casual visitors. More than ever they need identity management systems strong enough to ensure appropriate access but flexible enough not to get in the way.

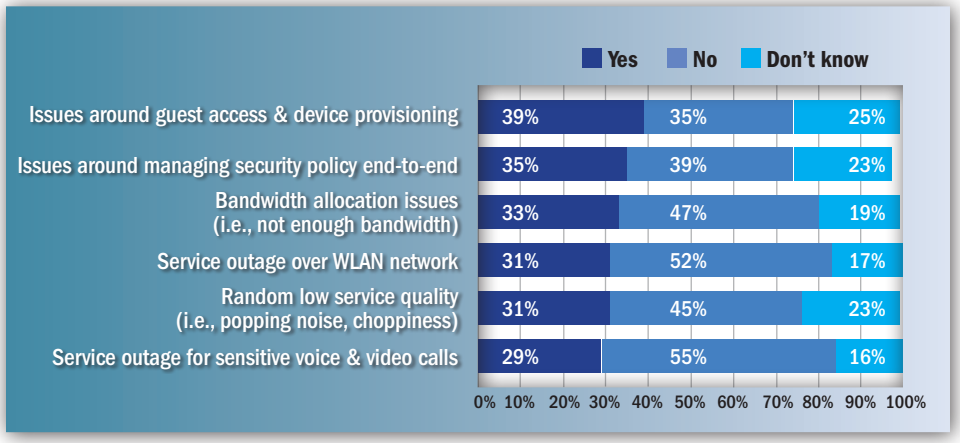
Because organizations must respond quickly to competitive and market changes and are often impacted by mergers and acquisitions, it's not unusual for organizations to end up with a patchwork of deployed technologies and management consoles. The result may be a hodge-podge of systems that don't "talk" to each other or leverage the benefits of a single place to provision, manage, and control the overall solution.

Nonetheless, IT is expected to provide enhanced levels of performance that support wide and responsive distribution of today's sophisticated business and entertainment applications. That can range from simple order entry and account management, to resource intensive VoIP telephony and

What's your company's policy with regards to giving access to the network via consumerized technology?



In the last year, did your network experience any of the following?



interactive video training programs. Indeed, 64 percent of respondents in the Gatepoint survey either formally support or allow the use of VoIP, and even more—76 percent—support or allow video and audio data from popular applications such as YouTube and Spotify.

Holding the Line on Security

At the same time as they strive to meet the demands of new media and data types, IT administrators and network architects must focus intently one how to protect business critical applications and intellectual property. They are also expected to further the cause of business agility by ensuring users have ready access to sophisticated online applications designed to fulfill their particular business needs.

Compounding the network security challenge is the wider, more diverse audience (including employees, partners, subcontractors, and offshore facilities) that all require access to critical data. As a result, comprehensive and collaborative security for the network, applications, data, and user is essential.

In the GateHouse survey, respondents say security on mobile devices that access the network is a critical top concern—averaging 4.35 on a scale of 1-to-5. Allowing workers to access the network from their own personal devices introduces a host of security and connectivity challenges.

"The number one way hackers get into the network is from these mobile devices," says Herrera. "People do all kinds things when they are away from work that can result in infections on their devices." Today's sophisticated attacks often fall "between the cracks" of traditional point security products.

While decision makers are well aware of the tools available to help them maintain defenses, according to Herrera, there is high anxiety over what the future holds in terms of new types of threats and attacks. "So we focus on making sure Juniper's solution has deep awareness of the devices being brought into the network and stays abreast of threats that impact different devices and the different operating systems those devices are using."

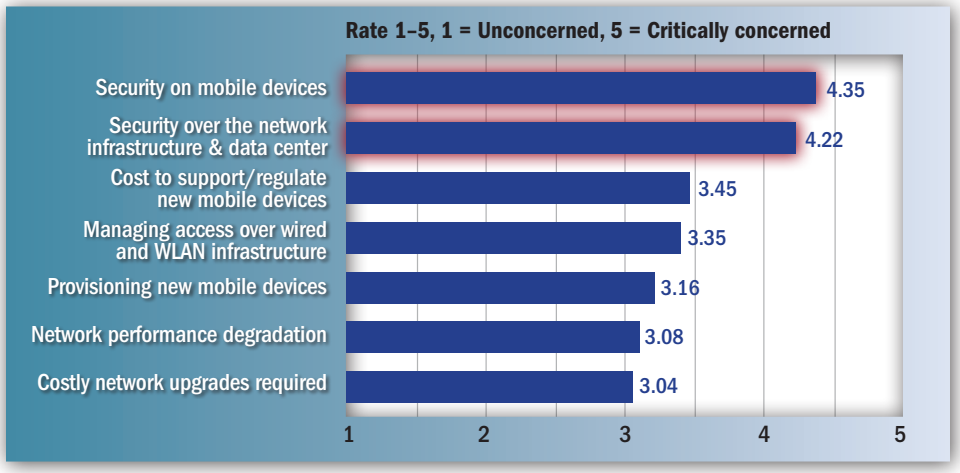
Policing Access

While security is the overwhelming concern of participants in the GateHouse survey, the growing reliance on mobile & remote devices creates anxiety and issues across a broad spectrum.

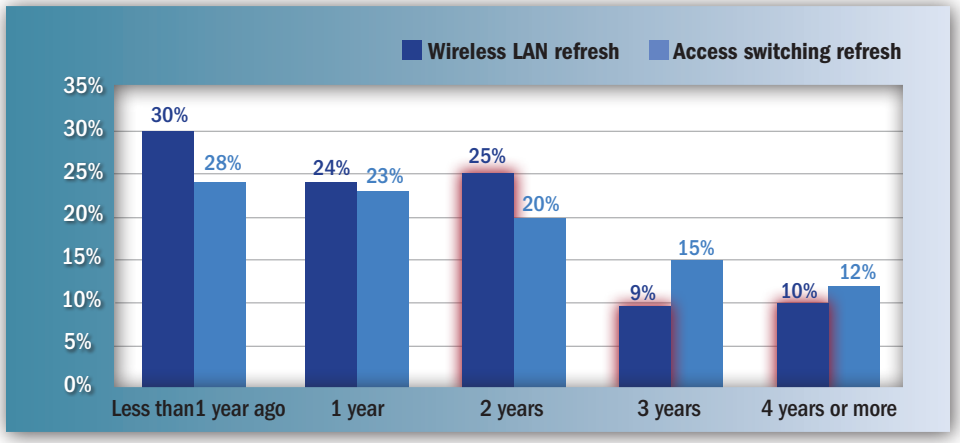
Managing access over wired and wireless LAN infrastructure rates at a 3.35 on a scale of 1-to-5 in terms of critical issues. Other issues rating higher than the midpoint include provisioning new mobile devices, network performance degradation and the need for costly network upgrades.

IT organizations are struggling with the best way to enable secure basic connectivity for mobile users across a wide variety of mobile platforms. A key challenge for these IT groups is how to maintain a consistent and uniform level of security policies across the mobile enterprise environment. They are also under tremendous pressure, internally and externally, to provide advanced anti-theft protection for lost or stolen mobile devices.

What are the concerns around giving access to the enterprise network with consumerized technology?



How long has it been since the last refresh of your wireless LAN and access switching infrastructure?



Over the past year, the number of respondents (39 percent) experiencing issues with guest access and device provisioning exceeded those (35 percent) who didn't. More than one-third experience issues around managing security policy end-to-end and just slightly less had bandwidth allocation issues.

"This all points back to the policies you create and how robust your policy solution is," says Herrera "Having the ability to set policies that are context aware—user, role, device and location based—while enforcing these policies at every point in the network is crucial."

With businesses increasingly reliant on wireless LAN as their primary access network, this is typically the first line of defense, Herrera notes. "Enterprises need a solution that recognizes the identity and the role of the user; with certain devices there are known security threats so the network solution needs to recognize the device and the person behind it to be able to give them the access they need to do their job without compromising security," she says.

Juniper Networks' Enterprise Solution

Juniper Networks designed enterprise network solutions that offer network protection, operational simplicity, stellar networking performance and flexibility, and total cost savings.

Juniper Networks enterprise network solutions use one OS, consolidating management, network policy enforcement, and control functions. This significantly reduces the learning curve, requiring less training and providing additional cost savings for ongoing configuration and management.

The company's Enterprise Mobility portfolio of resilient switching, security, and wireless products allows simple and secure access to business-critical information and collaboration. Juniper Mobile Security establishes barriers that secure the device, the network edge, and the application. It starts with qualifying the device, then provisioning and authenticating the user, and enforcing security policies at the user and application level. Juniper Mobile Security controls the device and avoids data leakage on an ongoing basis, and it can reach out to wipe out data if the device is lost or stolen. For more information, go to www.juniper.net/byod.

100 executives participated in the Gatepoint Research survey, with almost half working at the director level or higher. Respondents overwhelmingly work for large firms with more than half at companies with annual revenues greater than $1.5 billion.

What concerns do you have about operating an environment with a mix of switches?