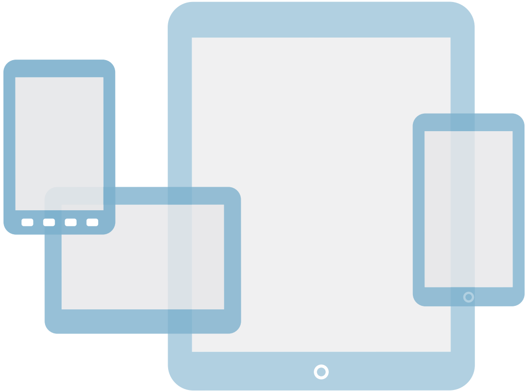
B.Y.O.D. WITHOUT THE R.I.S.K:

How CIOs can fully harness the enterprise mobility phenomenon

Today employees want the ability to work using their preferred mobile device from wherever they are and whenever they want. Not only that, they want quick and easy access to the information and applications they need to effectively do their jobs. It's no wonder smartphones have surpassed PCs as the preferred work tool of choice for consumers and enterprise users alike. With data mobility not just at an all time high but growing rapidly, how do CIOs enable such access while at the same time mitigate risk and ensure that company assets are protected?

The Consumerization of IT (CoIT) is well underway and as a result more and more employees are participating in the Bring Your Own Device (BYOD) phenomenon and using those devices anywhere and at any time to access and manipulate the information they need to do their job—from accessing a file on an internal server, collaborating, or simply using an app. Nowadays the average employee consumes and comprehends technology more fervently and confidently than ever before. But it's not just employees who appreciate technology and need access to the wireless network, it's third-party partners, contractors and suppliers who also bring along their own devices and need access. This modern-day mobile work environment poses a unique challenge for CIOs who need to secure a multitude of devices used by a multitude of people accessing a multitude of disparate components on a network.

Historically the legacy network has fulfilled the role of providing plumbing between hardwired, PC-based endpoints. As commonly deployed across the HQ campus and distributed to the global branch sites, they're compiled on multiple layers of management and



orchestration and contain far too many tiers of switches. Not only are they overly complicated, they consume too much power, dissipate too much heat and occupy too much space. What's more disconcerting beyond the challenges of their sheer form factor is the fact that legacy networks fail to align with the BYOD phenomenon or capitalize on mobility as the current access medium of choice.

Transforming the network transforms differentiation

Today's network must do more than just enable connectivity between multiple endpoints. It needs to be robust, highly resilient and enable mobility, performance, access, security, management and control at scale. And as if that's not too much to ask, it also needs to be transparent, agile, and consistently secure. That doesn't just mean putting a software client on the device and it's protected. Holistic security only comes from an all-encompassing seamless integration of wired, wireless and end point security.

A transformative overhaul may sound daunting but it simply means connecting together a wireless access network with a wired switch network that's high-end, resilient, and delivers performance-at-scale. This powerful combination not only secures mobile devices, but ensures their control, thus promoting productivity while mitigating risk. It also:

- enables third-party guest access to the network in a controlled yet flexible way that further mitigates risk.
- allows infrastructure modernization that leverages the benefits of wireless technology as the access medium of choice for simplicity and new levels of OpEx reduction.
- provides mobile endpoint device protection that enables employees and third-parties to bring and use their own mobile devices on site without threatening the peace-of-mind of the enterprise.

This is the new reality for CIOs as they look to build business-optimized IT platforms. Their IT infrastructure form factor now comprises service-oriented architectures, cloud computing, and virtualization. Now more than ever, the network is the fundamental glue between users, endpoints and services.

The strategy for enterprise and employee success

What first appeared to be both a management and risk mitigation nightmare can now be embraced as an opportunity for IT success that enables performance at scale, access security, management and control. A disruptive architecture that delivers an all-encompassing network platform spanning switching in the core, wireless access at the edge and an access management and protection client at the device, yields a new model. Not just any model, either, but one that securely delivers the flexibility that creates collaboration, agility and productivity for employees.

The best strategy for building this platform is a pragmatic approach that:

- leverages much needed disruptive technologies and IT architectural thinking to deliver the required business levels of security, performance and scale.
- provides both employee and guest BYOD network access with transparency, agility and control in a way that mitigates risk yet embraces how individuals desire to communicate and collaborate.
- allows even a fully depreciated network to be redesigned to meet today's performance, scale and security requirements—so that wireless is the access medium of choice and high performance Ethernet switching is the core that delivers immediate business benefits with an acceptable time to payback.

When CIOs have the ability to collapse infrastructure and use new components inside new network elements, which in turn have a smaller footprint, take up less space, consume less power and dissipate less heat, their OpEx dramatically improves. And as a result they also benefit from a more nimble, cost-effective, future-proof network.

By embracing the BYOD phenomenon and redesigning their infrastructure to not just optimally handle but leverage it, CEOs can confidently open their network to employees and interested third-parties without the concerns of exposing themselves to risk. This enables the CIO and the enterprise to remain open to gains in both productivity and operational efficiency and savings in OpEx. When CIOs deploy a robust network that's capable of securing everything from the device to the core, that not only integrates but enables mobility at scale, plus delivers better communication, collaboration, and productivity, they create a win-win situation for enterprise and employee alike.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters
Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters
Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

Printed on recycled paper