Building the Anytime, Anywhere Network

Mobile technologies are opening enormous new business opportunities. Capitalizing on them takes a new approach to networking.

Bask Iyer remembers the days when only the chosen few enjoyed access to mobile technologies. "It was limited to road warriors and executives," says Iyer, senior vice president and CIO of Sunnyvale, Calif.-based Juniper Networks Inc.

That was then, however. "Today mobility is no longer just for the privileged," Iyer observes. "It's available to everybody." As a result, mobile form factors are no longer something that Juniper's IT department merely accommodates when creating new applications. "They're the key interaction point," Iyer says. "We pay closer attention to the mobile experience these days than we do to the PC experience."

And Juniper is hardly alone. In the span of just a few short years, smartphones, tablets and other mobile devices have redefined the technological mainstream. Practically everyone now relies on them to stay connected with people, applications and information everywhere and all the time.

For the businesses these users work for and buy from, the upshot is an unprecedented range of opportunities for competitive differentiation, enhanced productivity and increased agility—opportunities they ignore at their peril. "If you're not thinking about new ways of leveraging mobility to make your people more efficient or to expand your customer base, it's a safe bet that your competitors are," says Iyer's colleague Abner Germanow, Juniper's director of enterprise marketing.

For corporate IT, capitalizing on mobility's potential means exchanging ironfisted control over access and devices for a more flexible approach. IT must balance firm administrative oversight with the freedom today's knowledge workers need to innovate in the anytime, anywhere economy. And making that demanding transition without compromising

INSIDE

security in the process means nothing less than embracing a totally new approach to building and managing networks.

Unprecedented Opportunity

The numbers alone provide a sense of the extent to which mobile devices have joined desktops and laptops as everyday technologies. Manufacturers shipped 461.5 million smartphones and some 63.6 million tablet devices worldwide in 2011, according to estimates from analysts at Gartner Inc. Collectively, that's over 44 percent more than the 364 million PCs Gartner expected computer makers to sell in 2011.

Furthermore, it's not just CEOs and gadget lovers snapping up all that mobile hardware. It's practically everyone. Indeed, by 2015 more than 200 million U.S. consumers will have a smartphone, tablet or both, according to research firm In-Stat. That's roughly 65 percent of everyone in the U.S. And it is becoming increasingly common for people to use multiple devices. Indeed, 52 percent of global information workers currently utilize three or more smart devices at the office, according to data from Forrester Research Inc., of Cambridge, Mass., while an incredible 14 percent juggle six or more devices.

Not surprisingly, with handheld devices becoming ubiquitous in people's private lives, mobile users are rapidly becoming the norm rather than the exception at work. In fact, 69 percent of corporate workers access business applications via a personal smartphone, and nearly 10 percent use a personal tablet for business purposes, according to data from Framingham, Mass.-based analyst firm IDC.

The upshot, for companies that encourage mobility rather than resist it, has been a dramatically more productive workforce. Armed with speedy devices and connectivity everywhere they go, employees can function effectively anywhere and anytime.

Mobility is also transforming the way companies engage with customers. "Businesses that have traditionally had an arm's length relationship with customers can now connect with them wherever they go, through mobile apps that enable people to place orders, check product availability, or utilize loyalty points," notes Germanow. And with handsets and the networks they run on becoming more sophisticated all the time, even-more-innovative services will soon be possible. "We'll eventually see mobile phones that are smart enough to see that you're headed to a meeting someplace where parking is limited and proactively offer to reserve you a spot," Germanow says.

Technical Headaches

For IT departments, the meteoric rise of mobility has created a range of significant challenges. Among the most commonly recognized is the need to extend the security policies they enforce inside the firewall to people and devices outside it. "A wired network user is typically static," observes Rohit Mehra, director of enterprise communications infrastructure at IDC. Mobile users, by contrast, may be connecting from anywhere on any of several devices, each of which may use a different operating system.

To further complicate matters, cybercrooks are increasingly employing PC-style malware to attack smartphones and tablets. The number of viruses targeting the Google Android platform alone rose an astonishing 3,325 percent in the last seven months of 2011, according to a Juniper Global Threat Center study, and hackers have begun adapting viruses and spyware originally developed for PCs to target mobile devices. Yet the management systems many companies rely on give them little to no visibility into which apps are accessing their network or what those systems are doing.

Then there are the dangers associated with rogue wireless hotspots that surreptitiously collect user credentials, and with mobile apps that contain hidden malware. In fact, a 2011 study by the Juniper Global Threat Center found that 14.7 percent of mobile apps request user permissions that can be

INSIDE

used to place a call without a user's knowledge or approval, 4.8 percent are able to send a short message service (SMS) message without user authorization, and 30 percent can obtain a device's location without approval.

Coping with the loss or theft of devices is an equally urgent problem. For example, over the course of 2011, 17 percent of companies using Juniper's Junos Pulse Mobile Security Suite utilized the "locate" command to find a missing device, while over six percent employed the system's lock feature to guard against unauthorized use of a lost or stolen device, according to data submitted to Juniper by its customers.

In addition, users accessing streaming media and corporate applications via Wi-Fi hotspots and legacy mobile networks often face latency headaches. With scores of devices simultaneously transmitting data across the network, businesses are struggling to keep performance levels high and provide resilient, always-on connectivity to mobile users. And with more and more employees using personal mobile devices at the office as well as on the road, corporate wireless networks are experiencing traffic snarls as well. "You can definitely have some performance hits," says Chris Boykin, vice president of professional services at Future Com Ltd., a provider of network and security solutions based in Bedford, Texas. "Everybody's sharing that bandwidth." (For further discussion of mobility-related bandwidth constraints, see "Flatter networks deliver better performance for any devices and applications" on page 9).

Freedom and Control

One thing is for certain: Limiting users to corporate-provided or -approved devices is no longer an option. "If you block the users, you just force all this stuff underground and you may not have a clue where your data is going," observes Gartner vice president and distinguished analyst Ken Dulaney. "If you at least know about the problem, you can manage it." Moreover, companies that bar employees from bringing personal mobile devices to the office are likely to have trouble attracting and retaining top recruits.

Managing the mobility problem successfully, however, takes a network capable of giving mobile users the freedom they crave while also providing IT managers the control they need to keep their company's infrastructure and data safe. Among the core qualities networks must share are robust security, resilience, and device administration functionality, including features that defend against virulent malware on day zero. Networks must ensure mobile-device security mechanisms are used, protect communications from interception, and remotely locate, track, lock and wipe clean lost and stolen devices to protect sensitive personal and corporate data. The ability to enable consistently strong performance and nonstop seamless roaming while supporting a wide range of applications, device types, manufacturers, and operating systems over Wi-Fi as well as mobile networks is another must.

Significantly, this applies as much to wired infrastructures as it does to wireless networks, since the wired network is the mobile network's backbone. Though people often assume adding bandwidth will enable them to meet application and device connectivity needs, this is usually a costly, cumbersome, and inflexible solution. What's needed is a wired network architecture flexible enough to scale smoothly while delivering reliable connectivity and high performance. It must also be simple and powerful enough to pool and allocate network resources efficiently, so organizations can virtualize devices and manage large and growing environments with existing personnel. This, in turn, enables them to optimize their IT investments.

Today's networks also need more advanced features, including the ability to enforce security policies differently, depending on who the users are, what devices they're using, what applications they're using, where they're located, and how

INSIDE

they're accessing the network and its data. For example, some IT organizations consider mobile devices such as smartphones and tablets less secure and easier to lose or steal than laptops; others consider public networks inherently riskier than private ones. As a result, companies must equip their network to apply more rigorous controls to a smartphone or a tablet connecting to business applications from an airport via a free hotspot than to a notebook connecting from inside a conference room at corporate HQ. They also need the ability to identify, monitor, and analyze dozens or hundreds of mobile apps in real time, and classify them based on variables like who is using them, how much risk they pose, and what data they're accessing.

Furthermore, administrators need the ability to define security policies centrally yet enforce them at the point of network access or directly on mobile devices. "The enforcement should be distributed. The policy should be centralized," observes Edgar Lombera, vice president of engineering and principal architect at Torrey Point Group LLC, a networking consultancy headquartered in Sunnyvale, Calif. That way, companies can enjoy both the simplicity of consolidated rules and the efficiency of applying those rules simultaneously at multiple places near where users are working.

Mobile-Ready Networks

Building a network capable of delivering all these capabilities takes a series of technologies designed from the ground up for the needs of the mobilized enterprise:

- **Coordinated, granular, context-based security software** that enforces policies consistently and continuously at the connection level across wired, wireless, and remote access networks, anywhere and anytime, while providing robust remote data wiping and access rights management capabilities.
- **Network systems that provide a consistent experience** for both users and IT across voice, video, data, presence, and service-oriented architecture by ensuring wired-like performance and seamless scalability across wired and wireless networks.
- **Network management solutions that utilize a single client application** for mobile device management, mobile security, SSL VPN, wireless provisioning, and network access.
- **Comprehensive access technologies** with real-time automation that provide a foundation for fast, secure, and reliable application delivery not only to all users but to all of their devices, including guest, BYOD, and IT-owned hardware.
- **Network device virtualization technologies** that simplify a network architecture sufficiently to manage device proliferation without inflating personnel resources, enhance device performance enough to support rich media and mobility applications, and easily scale to enable architecture flexibility and support an explosion in mobile devices and applications on the network.

Needless to say, equipping the network with these kinds of solutions won't be an overnight process for most companies. Those that invest the time and effort anyway, however, are likely to find the rewards worthwhile. "Opportunities to create new services and disrupt existing business models by using mobile devices are appearing every day," Germanow says. It will be companies with truly mobile-ready networks that capitalize on them first—and profit from them the most.

BYOD

Companies that bar employees from bringing personal mobile devices to the office are likely to have trouble attracting and retaining top recruits.

INSIDE

Securing the Mobile Enterprise

Today's mobile landscape requires companies to apply highly granular security policy, based on the user, device, location, time and application.

Enterprises are becoming relentlessly mobile, with employees of all stripes carrying not just one but likely two or three devices with which they want to connect to the network at various times. Maybe it's an Apple iPad for meetings in the office or on the road, a laptop from home or the coffee shop and a smartphone from anywhere in between.

Although there's little question that enabling employees to use the device of their choice to access the data and applications they need makes them more productive—not to mention happier—the practice does present a significant security challenge for IT. There's no denying that using mobile devices for business means that sensitive, critical corporate data and intellectual property have to be secured.

And it's not just the device that has to be secured; it's also the connection between the device and the company network or corporate cloud as well as the various applications in use. What's more, IT needs a way to ensure that only authorized users are using the devices and accessing corporate resources.

Wanted: A New Approach to Mobile Security

Meeting all enterprise objectives requires companies to take a new approach to mobile security, one that looks at security on a per-person rather than a device-specific basis. "Devices are ephemeral; people aren't," says Chris Christiansen, program vice president of IDC's Security Products and Services group. "And device identity doesn't help when a device is stolen, lost or misplaced or an unauthorized person is using it."

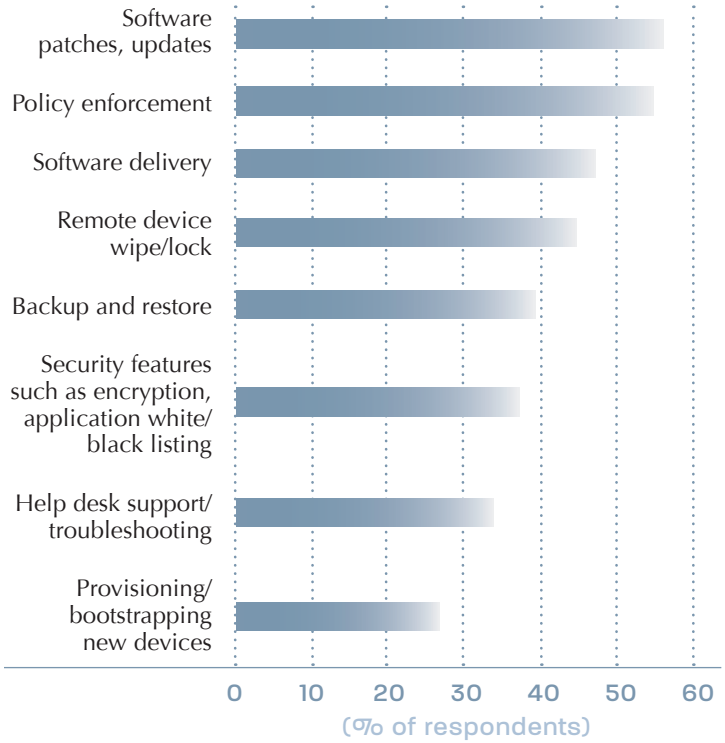
The goal is to have people's security profile follow them as they move among different locations and use different devices and applications. Security is provided for each device and the security profile dictates what each user can—and cannot—do with each one, taking into account criteria including where the user is and the application in use. At the same time, the approach can't be intrusive; if users find security getting in the way of their day-to-day tasks, they will find a way around it.

INSIDE

Respondents to IDC's "2011 Mobile Enterprise Software Survey" neatly outlined the requirements they deem most important in a mobile device management system. Security was clearly a top concern, with software patches and updates the top requirement, followed closely by policy enforcement, remote device wipe/lock and application blacklisting/whitelisting (see Figure 1).

FIGURE 1

The most important features for an organization as it relates to mobile device management system.



SOURCE: IDC's Mobility Enterprise Software Survey, 2011

Pervasive Security

At the simplest level, Christiansen says, providing that kind of pervasive security means looking at the issue from a "to, from and in" perspective:

- When you send data to the device, can you authenticate the information and confirm that it is coming from a legitimate source?
- When data is coming from the device, can you confirm that the data hasn't been changed, the sender is authenticated to send it and there's a high level of trust in the information?
- When data is in the device or on a server, do you have assurance that it is stored correctly and hasn't been co-opted by another application, such as malware?

Providing proper authentication increasingly means two-factor authentication, in which users employ something they have (which may be the device itself or a third-party token) and something they know, such as a password. Protecting data on the device also means being able to lock the device or provide a "kill pill" to remotely wipe all data if the device is lost or stolen.

Organizations also want to control which applications users can download, to protect against the malware that is increasingly targeting mobile applications, particularly Android devices. Even if such malware doesn't succeed in infecting the device itself, Christiansen warns, the device may be used as a vector to pass malware along to other devices.

Devising a Security Policy

Addressing these security requirements necessitates policies to cover various user groups and requires enforcement mechanisms to ensure that the policies are carried out. The groups include not only internal constituencies but also

visitors, customers, partners, and increasingly, contractors.

For example, policies may allow employees to use their own devices at work so long as they agree to secure the device with a password and agree that the company reserves the right to wipe the e-mail account and certain data if the device is compromised.

In terms of applications, companies have to determine which ones won't be allowed (blacklisting) or, more often, simply define which applications are allowed (whitelisting) and deny all others. The list of acceptable applications will naturally vary, depending on the user group. Also, companies should be able to set a policy that precludes the use of certain mobile features and functions—such as the device's camera—if the device is used in an area of the company where sensitive information is stored. Similarly, perhaps the marketing group is allowed to access Web applications such as Facebook, but only for work-related purposes—meaning they can't use it to play games. And all policies for mobile devices have to sync with the company's overall IT security policies; you shouldn't be reinventing the wheel.

"What people really want is a single set of controls and policies so they can normalize the mobile security environment across multiple heterogeneous device types and operating environments," Christiansen says.

The Juniper Approach

In short, customers need a solution that covers all sorts of mobile requirements, from casual consumer activity to business-critical applications, but without layers of complexity. Customers need mobile security that is at once simple to implement and operate and also effective.

That's what Juniper's Simply Connected portfolio is all about. Simply Connected is a collection of integrated security, switching and wireless products that enables customers to build a secure, scalable, highly available solution for both company- and employee-owned devices. Simply Connected products enable companies to create security policies once and apply them across wired, wireless and remote access networks, in a context-aware fashion delivering holistic and coordinated security for all enterprise network access.

For example, whereas security reports might formerly have provided a list of security violations by IP address, forcing companies to spend time matching addresses with names, Juniper does all that work for them. That helps promote more-fruitful discussions between IT and business units about security, according to Christiansen.

"The intent is not to punish but to collaborate with the business units to change people's behavior in a positive way," he explains.

With a Juniper Simply Connected solution, businesses can:

- **Create policies only once,** across wired, wireless and remote access networks, including extensive device coverage for both BYOD and IT-managed devices, delivering consistent, secure access with Web 2.0 application visibility and control.
- **Juniper AppSecure provides a deep understanding** of application behaviors and traffic flows to provide protection from common evasion techniques and malware attacks. It also enables IT to define and enforce application policies and works with the SRX Series Services Gateway intrusion prevention system to repel various other forms of attack, including zero-day attacks for which no attack signature yet exists.
- **Add intelligence to their network** with context-aware policies that are tailored to the security risk, accounting for the user, device, application and location across the corporate network of switches, gateways, wireless LANs and users' devices.

> Junos Pulse Access Control Service running on a

INSIDE

MAG Series gateway device:

- Ensures that only authorized users gain access to various network resources, with security policies that follow them around the globe, accounting for their location, device or means of accessing the network and the resources they are trying to reach
- Uses the Junos Pulse client as its common user interface, minimizing and simplifying client deployments and saving IT cost and time

- **Choose between client and clientless deployment.** Although clientless deployment is more desired by end users, who can simply and securely onboard personal devices without IT intervention, client deployments present stronger security, by providing control and better protection for end users' devices.
  > The Junos Pulse Mobile Security Suite, a software as a service (SaaS) offering, is one of several services that runs under the Junos Pulse client, a multiservice, mobile network access, acceleration and security client that includes security applications ranging from antimalware and endpoint firewall capabilities to loss and theft prevention, device management, monitoring and control.
- **Have a holistic approach to enterprise access.** Connecting from outside the enterprise perimeter is as common today as connecting from within it and is one of the core elements of a mobile enterprise.
  > To secure data in transit to and from mobile devices, Juniper offers its Secure Access Series SSL VPN Appliances, delivering secure remote access from mobile devices, laptops and remote desktops to corporate resources.
- **Deliver a better user experience.** Today users are expecting to have the same experience, if not a better one, in connecting to the corporate network wirelessly than they do through a wired connection. Juniper delivers a single secure network for voice, video, data and SOA, providing a foundation for fast, secure, reliable delivery of applications and supporting strategic business processes in a mobile network.
  > The Juniper Simply Connected portfolio enables a mobile rich media experience to help maximize the power of the network and ensure quality of experience. The WLC Series, EX Series and SRX Series don't require trade-offs between scale and performance as you change and evolve your campus. So more locations, more users and more apps can be accommodated cost-effectively.
- **Provide always-on mobility** with robust design capabilities to enable connectivity for on-demand business applications, fewer devices, simplified management and more automation. Customers will be able to deploy mission-critical applications on a dependable network, with seamless scalability across wired and wireless connections, thereby futureproofing their investment.

Controls and Policies

"What people really want is a single set of controls and policies so they can normalize the mobile security environment across multiple heterogeneous device types and operating environments."

—Chris Christiansen, program vice president, IDC

Conclusion

Mobility is a requirement in today's enterprises, something employees have come to expect and rely on. But the mobile environment must be secured in a way that users don't find intrusive but that IT knows is sound. With its extensive lineup of scalable, simple-to-use tools and services, Juniper can help.

INSIDE

Flatter networks deliver better performance for any devices and applications

As more network traffic moves between servers, data center architects need to rethink and retool network fundamentals.

Users are becoming ever more mobile, employing a multitude of devices, from smartphones to tablets, to access corporate data and applications. CIOs understand the value mobility can bring to their businesses but are faced with a challenge: ensuring the devices deliver a quality user experience no matter which applications users employ.

Given the demands of the user base—which includes not only internal employees but also guests, contractors, suppliers and others—that challenge is significant, says Mike Spanbauer, principal analyst, Data Center Technology and Enterprise Networks, at the consulting firm Current Analysis. "These applications are being accessed from everywhere in real time, and user expectations are higher than ever," he says. "It's like trying to satisfy a bunch of teenagers who are exceptionally demanding, unforgiving and very savvy."

Although certain aspects of the performance of mobile applications rest with wireless service providers, the enterprise wireless LAN, data center and application architecture also play a large role in ensuring good performance for mobile applications.

INSIDE

Meeting the Wireless Challenge

Enterprise networks, which were originally architected for wired clients, are now being asked to support more wireless devices than wired ones, which leads to two big changes, says Abner Germanow, senior director of enterprise marketing at Juniper Networks:

- The wireless LAN needs to become more robust and reliable.
- The wired network doesn't need as many access ports, but it needs to support more traffic, due to the increase in the number of devices connecting to it and the constant march of more network-intensive applications.

The challenge for IT is to strike the right balance of wired vs. wireless networks and ensuring that they are reliable, scalable and secure, Germanow says.

Rethinking Legacy Architecture

Traditional enterprise networks were designed for wired devices. When all devices were physically connected to the LAN, having many ports and many connections was key to enabling connectivity and performance. This is no longer the case. Enterprise networks now need to deliver the required performance to deliver mobility applications on any device. On the enterprise network, delivering high performance to any device and application presents two key requirements:

- Wired networks no longer need to be designed to maximize the number of ports they deliver, but to maximize the performance of the applications they support.
- Because connectivity needs to be delivered to any device anywhere on the network, flexibility and scalability is critical to the design of any network. Therefore, simplifying the architecture of the wired network is essential to delivering mobile connectivity. Collapsing tiers by virtualizing network resources and limiting the number of wired connections is essential to delivering flexibility and scalability to enable mobility.
- To deal with the proliferation of mobile devices and applications, the wired network must also optimize personnel resources. Automation and management simplification are essential. For instance, companies need to reduce the number of independently managed devices by virtualizing devices, and implementing automation technologies such as auto-discover, auto-configure and pre-emptive fault notification capabilities.

Traditional data center network architectures are also optimized for client/server applications, in which a single server delivers an application to a given client across a local- or wide-area network. This is "north-south" network traffic, or server to client, for the most part. For the past decade or so, companies have been moving to more of a service-oriented architecture (SOA), in which applications are far more distributed, Germanow says. In a SOA environment, an application may call upon many different components to complete a single request. This is "east-west" network traffic, or server-to-server.

"Where you put the components has a direct impact on the performance of the application," Germanow says. Say you have 100 different components that can mix and match to create different applications. If components one through five exist on servers located on the same rack, any application that requires only those components will get good performance. But if components 95 through 100 live on the other side of the data center and they need to be combined with one through five, performance can suffer greatly, because the request will have to travel across multiple tiers of the three-tier architecture—access, aggregation and core—common in client/server environments.

INSIDE

Flattening the Tiers

The reason the three-tier architecture evolved was mainly the limited port density of network switches, Spanbauer says. Once all the ports were consumed at one tier, traffic had to be shuttled up to a higher tier. But now vendors are offering switches with greater port densities, which changes the equation. For the last three years, for example, Juniper has been offering EX Series switches, which support as many as 384 Gigabit Ethernet ports at wire speed in a single switch. What's more, up to 3072 Gigabit Ethernet ports can be managed in one single virtual switch. "You can get some pretty impressive port density out at the edge with low oversubscription ratios," Spanbauer says.

EX Series switches with Virtual Chassis are intended to enable companies to do away with the aggregation layer of switches, Germanow says. "That removes about 30 percent of the equipment and optimizes traffic between racks," he says. "It works really well in a Gigabit Ethernet or mixed 1G/10G environment."

Companies that require performance and efficiency for 10G environments can now opt for Juniper QFabric Series data-center fabric technology. Customers can build a switch with as many as 6,100 ports—creating a one-tier architecture—Spanbauer says.

"That optimizes application-to-application and server-to-server communications where one node talks directly to another," he says. "Your network architecture is no longer dictating your data flows."

Service Provider Connection

Another element critical for good mobile application performance is the connection to the service provider and ensuring traffic is prioritized appropriately, Spanbauer notes. Although enterprises can't control what goes on inside the service provider network, they can establish service-level agreements to establish what's expected.

"Control what you can, manage what you must and architect for optimal deployment within your sphere of control," he advises. With its Junos operating system deployed across its entire product line, Juniper delivers operational benefits that help make it easier to control and manage the network, he says.

It's also a good idea to consider the physical location of the data center and its proximity to your carrier's point of presence or even to collocate with the provider, Germanow says.

Deciding Where Data Lives

Companies also have to consider how many of their mobile applications will live on the mobile device, as opposed to on a server in the data center, Germanow adds. If users employ predominantly a 3G network, it may make sense to store more data on the device to minimize the need to connect to the remote server. But as users migrate to a 4G network, they may be able to access the data just as quickly over the network as they could if it were local. In such a case, it makes sense to store it in the data center, where IT can provide better security, Germanow says.

Such changing network capabilities also point to the need for a flexible data center architecture. "The pace at which your applications evolve is faster than the pace at which your infrastructure will evolve," Germanow says. "Ultimately, you need to build infrastructure that doesn't hold you back as application requirements change and the devices and networks they have access to evolve."

INSIDE