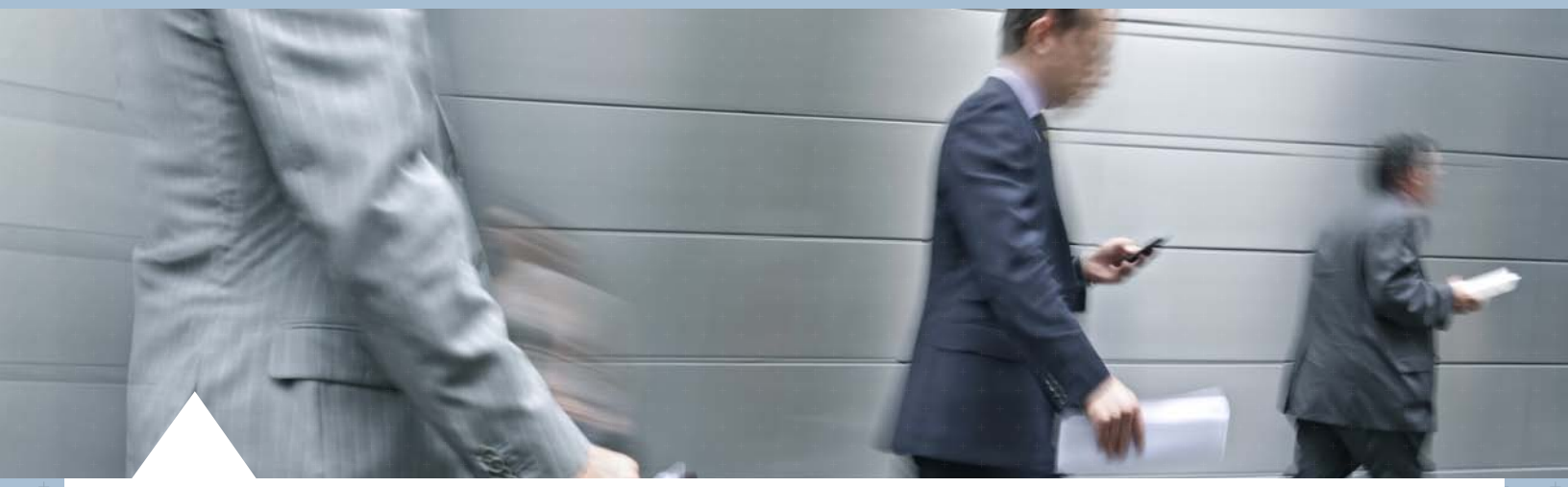

WHITE PAPER

Mobility **Without Limits**

Stepping up—and locking down—mobile device security in the enterprise

Executive Summary

Mobile devices are flooding corporate networks as next-generation, user-empowering business tools. In their wake flow both opportunities and challenges that mirror the transformation dilemma recently experienced as Web 2.0 and social networking began to infiltrate the enterprise. Now mobility applications are quickly maturing beyond simple texting and e-mail to include sophisticated business transactions and collaborative multimedia work interactions, with full content sharing and storage on the horizon. So CIOs need to apply care and due diligence for security policy, management and control—just as they did with social media.

Even though it started as a personal fad for reaching out to friends and family, social networking has proven to be a 21st-century business boon. With Facebook boasting more than 500 million active users and Twitter registering roughly 65 million tweets a day, the phenomenon has revolutionized the way the world conducts business—from how employees collaborate to how enterprises interact with customers.

JUNIPER NETWORKS

CIO Custom Solutions Group

Juniper Makes Mobile Security a Reality

From mobile devices to data centers, Juniper Networks delivers innovative software, silicon and systems that transform the experience and economics of networking. Its products enable you to securely mobilize your workforce for untold gains in productivity and agility—so you can fully modernize your infrastructure without sacrificing the user experience for the sake of security. Additional information can be found at **www.juniper.net**.

Still, the potential dangers of social networking—with its sheer reach and anonymity— initially blindsided many CIOs. Limiting enterprise usage out of pure fear was a common reaction. However, since the first wave of adoption, most CIOs have been able to establish control through use policies and security technology. Now enterprises have fully embraced the trend and are basking in its rewards.

On the heels of that phenomenon, CIOs are now faced with the next big game-changer: mobility. Not surprisingly, users are taking to it as passionately as they did to social networking. "With the power and storage capacity of smartphones today, users can do essentially everything they can do on a laptop or PC," says Daniel Hoffman, chief mobile security evangelist at Juniper Networks, a network infrastructure provider based in Sunnyvale, Calif. "The big difference is that you'd be hard-pressed to find a smartphone with the same enterprise-grade security you see on those laptops and PCs."

With this realization, CIOs must tackle the craze head-on with the same enthusiasm and rigor as they did social networking.

The Momentum Behind Mobility

The march to full mobility is certainly impressive, led by innovations such as BlackBerry, Android and Windows Phone 7 devices. Consumers can't seem to get enough, constantly clamoring for the latest-and-greatest gadgets. And they're incorporating those devices quite aggressively into their work lives. In fact, ABI Research forecasts that worldwide enterprise smartphone shipments will grow from 83 million units in 2010 to 171 million units in 2015. And that's on top of a worldwide installed base of 153 million units in 2010. Even tablet devices, such as the ever-popular Apple iPad, which made its debut as an "executive toy", is now moving quickly beyond the boardroom and into the general work population and day-to-day business use.

Widespread adoption is a foregone conclusion, considering how powerful and portable devices have become. These are not just high-end phones and tablets but rather fully functioning computers with their own operating systems and myriad applications. ABI says they are distinguished by their "highly functional and customizable experiences and ability to deliver full application processing capability to the user, regardless of the presence of a wide-area wireless network."

According to ABI, the "killer apps" that are driving mobile device use within the enterprise include, among others:

- Anywhere, anytime access to e-mail
- Mobilization of enterprise applications such as CRM, ERP and BI
- Unified communications such as instant messaging, videoconferencing, Web conferencing and document sharing
- Browser solutions
- Downloadable applications for tasks such as navigation and expense reporting

With Every Reward Comes Risk

Still, mobile devices are introducing new challenges and complexities for CIOs that directly mirror the impact Web 2.0 and social networking have recently had on enterprises. Users took to social networking technology with abandon, incorporating application after application into their office life—along with their bad habits of sharing sensitive data and downloading content from unknown sources. CIOs initially struggled to keep such activity under control.

Mobile technology is in the midst of a similar dilemma. It seems that every employee has one or more devices—some company-sanctioned, others entering the workplace unsanctioned. "Users are given a laptop, but they might buy their own mobile device," explains Hoffman. Even corporate programs offer choice based on user preference and job requirements, so CIOs end up with a heterogeneous environment comprising different mobile devices with different operating systems coming from different sources—and nary a device with sufficient built-in security.

At the same time, the processing power behind these handheld devices enables users to do much more than with

previous generations of products. They're enthusiastically opening otherwise closed doors by accessing new applications, performing complex business transactions, downloading information and sharing that information indiscriminately. "IT is effectively losing control," warns Hoffman, just as it did when desktop PCs gave way to laptops and netbooks, and social networking hit the enterprise.

Of course, losing control in the enterprise can prove disastrous, with threat vectors coming from the device, application and network levels. The following are some of the most crucial vulnerability points of mobile device use:

Malware. Mobile devices are just as—if not more—susceptible to malware as PCs and laptops are. Users download applications and open e-mail attachments every day on their mobile devices, resulting in high infection rates within enterprises. What's worse, today's malware strategies are typically financially motivated. The goal, Hoffman says, is to slip in unnoticed, steal valuable data and move on—unlike old-style viruses that were designed to "merely" wreak system havoc. As such, CIOs need to deploy the same protections to prevent infection as they do with traditional PCs and laptops.

Loss and Theft. "Most of us don't go anywhere without our smartphones," says Hoffman. That extreme portability makes mobile devices a prime candidate for loss—left behind in a cab or in the bleachers at a child's soccer game. They're also easy to steal; one careless moment at the coffee shop, and a device disappears. Hoffman relates this to his own company, in which one in 20 employees has reported the loss or theft of a device. Calling the carrier in such an event can prove fruitless. And without enterprise security, those devices can't be locked, located, wiped or restored. That's a dangerous scenario when one considers the sensitivity of the data that is likely involved.

Direct Attack. CIOs must always be on guard for direct attacks. Acts of corporate espionage, cyberterrorism and even outright theft are the makings of many a sensational news headline. Smart hackers will always go for the easiest target, and new technology is often fertile hunting ground. As such, mobile devices are becoming that target and can be used to hack into corporate networks. Furthermore, an eavesdropper within reception range of a wireless access point can insert himself as a "man in the middle" attacker. Most mobile devices lack the core security features commonly used to lock down PCs and laptops, so they are wide open to attacks.

Data Communication Interception. Mobile devices have become wholly integral to enterprise communications. But users are communicating as if on a private network—unaware of the potential threats. And with today's mobile computing power, it's not inconsequential sharing—collaborating on a new engineering project from a beach on Barbados, sharing legal documents from a hotel in Beijing. All of that data has to travel from the device to the server, Hoffman explains, during which time it can be sniffed. Still, mobile devices are rarely equipped with virtual private network (VPN) clients—even though a corporate laptop or remote PC would never lack such protection.

Mobile Security Made Simple

The key to impenetrable mobile security lies in product implementations targeting specific threat vectors coupled with sophisticated device management capabilities.

MOBILE THREAT	MOBILE SECURITY SOLUTION
Malware	**Antivirus and antispam features**
Loss and theft	**Ability to lock, locate, wipe and restore**
Direct attack	**Firewall technology**
Data communications interception	**VPN and encryption solutions**
Exploitation and misconduct	**Filtering capabilities**

Exploitation and Misconduct. According to Hoffman, one of the weakest links in any security strategy is the human element. Where there is a will to exploit, mobility is certainly a good way. Disgruntled employees, unscrupulous contractors or mischievous temporary workers can use mobile devices to leak data. Even well-intentioned workers can share inappropriate photos and links. So enterprises need to monitor what users are doing on and with their mobile devices, and apply the corporate standards deemed appropriate for local and remote users. After all, those users could very well be sharing critical information—such as passwords, forecasts, customer contacts and contract specifics—in simple, unprotected text messages.

Interestingly, Hoffman points out, these threat vectors relate directly to the vulnerabilities CIOs have been dealing with when it comes to enterprise PCs, remote systems and laptops. Still, mobile devices tend to lack the defenses mandated for such systems.

Locking Down Against Threats

Despite the seemingly ominous threat landscape, mobility is today's reality. CIOs and their IT organizations need to embrace smartphone mobility and create a comprehensive, federated security strategy that ensures the safety of the enterprise and its information assets.

From a strategic perspective, CIOs must look at mobile security holistically. Mobile devices require the same protection and due diligence afforded any other enterprise endpoint. It's important to consider what security measures have been deployed to desktops, remote systems and laptops and carry that same level of protection over to mobile devices. Apply the same corporate standards in terms of acceptable use parameters, and be sure to monitor and enforce policy. As with any other security strategy, awareness and education are crucial. Users have to understand the risks their mobile devices pose and the consequences of a security breach. And like security for social networking, this needs to be a top-down initiative.

"Tactically, you need to understand the threats and then supplement that knowledge with technology," Hoffman declares. That means embedding security across mobile devices, applications and networks and matching available security products to the threat vectors with downloadable client software for smartphones, tablets, notebooks and netbooks. In particular, CIOs need to deploy the appropriate antivirus and antispam solutions to protect against malware. They must equip each device with a VPN client to encrypt mobile communications traffic and a firewall to prevent targeted attacks on in-transit data. And, in the event of loss or theft, CIOs need decisive functionality for locking, locating, wiping and restoring missing devices.

At the same time, the right device management solution is the linchpin to success. CIOs must centrally support mobile devices in a zero-touch model—including all operating systems and the newest models as well as corporate-sanctioned and personal devices. Access to enterprise networks must be location-aware, identity-aware and application-aware. Mobile user activity should be granularly managed, with role-based access to applications—including Web, e-mail or client-server applications—with operational simplicity that provides automation and scale. And consistent enforcement of security policy across the enterprise network, regardless of device type, operating system or attempted network access method, is a must.

No Limits

"Most importantly, CIOs need to realize and accept that smartphones and other mobile devices **are** computers," says Hoffman. And pretty powerful ones at that. "Don't unnecessarily limit what users can do with these devices." Mobility can have a tremendous impact on the business, providing users with constant access to information and communications so they can send that final proposal to a customer from the airport, check an order's status from the coffee shop or collaborate with their team from home. It helps balance work and personal lives, resulting in a happy and productive workforce.

BOTTOM LINE: An IT organization can make all that happen and come out the hero. Just look at what has been accomplished in leveraging social networking in a controlled and secure manner. "Now CIOs can bring that same peace of mind to mobility, with strong knowledge of the threat environment and an equally strong arsenal of security tools," Hoffman concludes. So users—and businesses—can go forth and prosper.