

# SECURE MOBILE BANKING AND TRADING

## Bank and Trade Securities Securely Anytime, Anywhere Through the Junos Pulse Mobile Security Suite

### Challenge

Mobile banking, financial services, and security trading applications are some of the fastest growing mobile applications for users and businesses. Yet, security related to mobile banking and financial transactions remains a major concern for the users and institutions that use them.

### Solution

The Junos® Pulse Mobile Security Suite is a comprehensive solution that provides mobile device users of financial institutions secure access to banking and financial services information, protecting devices and the financial institution's network from threats.

### Benefits

- Mitigates the risk to banking and financial data from compromised, lost, or stolen mobile devices
- Provides real-time protection from mobile viruses and malware
- Monitors inbound and outbound traffic, scanning files over all network connections
- Enables financial institutions to remotely locate, lock, wipe, back up, and restore devices

Mobile banking and securities trading provides consumers with unprecedented convenience and virtually limitless access to their financial accounts and transactions. Consumers are rapidly adopting mobile financial practices, and financial institutions are marketing their mobile capabilities as never before. With more and more consumers using smartphones and other intelligent mobile devices, this is a trend that is not only likely to continue, but to grow by leaps and bounds.

A significant concern for consumers and financial institutions alike is the security related to these highly sensitive transactions. For many consumers, they are afforded a complete guaranty by their financial institution that any fraud or malicious activities resulting from mobile banking or trading will be fully covered. Banks and trading companies are offering this guarantee to entice customers to adopt this new technology without risk. International court rulings have clearly placed the burden and financial liability onto the financial institution as well. The integrity of mobile financial transactions is only as secure as the integrity of the mobile device on which the transaction is performed, and the environment from which the transactions are performed. As such, financial institutions are exposing themselves to significant financial liability by offering fraud guarantees without the appropriate level of insight into the security of the device or the environment from which a transaction is being processed.

### The Challenge

As more of today's workers are mobile, they are looking for more mobile solutions in their daily routines and lives. Mobile banking and security trading applications are fast becoming some of the most accessed and used mobile applications by users and businesses alike. The need for consumers and businesses to access, manage, and conduct transactions on their bank and securities accounts, while mobile, is growing into more of a requirement with each passing day.

But, the security related to these highly sensitive transactions is a major concern for consumers and financial institutions alike. Many financial institutions are providing their mobile banking consumers with a complete guaranty that any fraud or malicious activities resulting from their mobile banking or trading will be fully covered by the financial institution. Banks and trading companies guarantee full restitution of finances hacked or stolen when mobile, to encourage their customers to adopt new mobile capabilities without opening themselves, and their financial and securities information, to risk.

However, any mobile financial transaction is only as secure as the mobile device and the situation from which the transaction is performed. Banks and financial institutions are leaving themselves open to financial liability based on the incredible sums of cash and securities transacted each day using mobile devices.

Banks and financial institutions are delivering mobile banking and securities trading security by authenticating users, using Secure Socket Layer (SSL) technology to protect communications, and by providing anti-phishing measures to verify the identity of the mobile banking or trading website. But, these steps fail to address critical device and environmental security vulnerabilities. Security threats not presently addressed by existing mobile banking security include:

- Spyware capable of obtaining sensitive user authentication information
- Exposure or theft of financial information due to loss or theft of the mobile device
- Susceptibility to network-based attacks due to a lack of device firewall
- The use of unauthorized devices
- The use of unauthorized banking applications
- SSL “man-in-the-middle” attacks capable of intercepting user authentication credentials

### Junos Pulse Mobile Security Suite Solution

The *single best* way to address today’s mobile banking and securities trading issues is for banks and financial institutions to offer their mobile device users the Junos Pulse Mobile Security Suite.

The Mobile Security Suite is a comprehensive mobile security and device management solution spanning a broad range of mobile platforms. It protects mobile devices against viruses, spyware, trojans, worms, device theft, loss, and other threats that might befall them. It enables banks and financial services firms to provide smartphone and other mobile device users with secure, remote access to their banking and financial services information. With Mobile Security Suite, users can conduct transactions while mobile, protecting the user’s mobile device and the bank or financial institution’s network from a wide range of threats.

Simple to deploy and use, the bank or financial institution can include the Mobile Security Suite as part of its standard application download from the appropriate application store or marketplace for the user’s mobile operating system. The Mobile Security Suite works across the most popular and deployed mobile operating systems and handsets, including:

- Nokia Symbian S60 third and fifth editions
- Microsoft Windows Mobile 6.0, 6.1, and 6.5
- Google Android 2.0, 2.1, and 2.2
- BlackBerry 4.2 and later

By downloading and installing the Mobile Security Suite, users receive continuous protection against viruses, spyware, malware, direct network-based attacks, and mobile device loss and theft.

The Junos Pulse Mobile Security Suite is a unique solution that takes into account specific challenges presented by smartphones and mobile devices, such as limited device memory and limited battery capabilities. It also will not negatively impact device or network performance.

When a mobile user opens a mobile banking application which includes Junos Pulse Mobile Security Suite, the client analyzes the security posture of the wireless environment from which that user’s device is broadcasting. If a “man-in-the-middle” attack scenario is not detected, the user will be allowed to submit credentials for authentication to the mobile banking solution. The Mobile Security Suite analyzes the user’s mobile device, communicating the device’s security posture and unique device identity to authenticate both the user and device. This communication also ensures that the device is registered and permitted to be used for mobile banking. In this way, the Junos Pulse Mobile Security Suite offers multifactor authentication of the user and device for the mobile financial transaction.

Juniper Networks Unified Access Control (UAC) delivers granular, identity-based network and application access control on the LAN. When UAC or another access control solution is deployed with Mobile Security Suite, they will receive the state of the device’s security posture. They will also determine if the consumer’s device meets a minimum baseline of security requirements for network and application access as determined by the bank or financial institution. Using existing LDAP capabilities, user and device authentication credentials are passed to the existing mobile banking authentication infrastructure. Based upon configured policies, authorizations, and user and device authentication, access to the mobile banking, financial, and trading application may be permitted, blocked, or limited.

## Features and Benefits

Junos Pulse Mobile Security Suite offers the broadest platform coverage with the most comprehensive range of security applications, including antivirus, anti-spam, personal firewall, loss and theft protection, and identity protection. The significant features and benefits of the Mobile Security Suite include:

| FEATURE   | BENEFIT   |
|---|---|
| Automatic virus and spyware definition updates  | Provides full real-time protection from the latest smartphone antivirus/malware threats   |
| File scanning over all network connections  | Protects the smartphone from potential malware that can infiltrate the device from multiple sources, including via SMS, MMS, Bluetooth, Wi-Fi, 2.5G, 3G, 4G, infrared, or desktop sync  |
| Inbound and outbound traffic monitoring   | Protects the mobile device from accessing harmful or questionable content, and prevents malicious content from being transferred to the device  |
| Blacklist and whitelist filtering   | Blocks calls and SMS spam (blacklist) and allows acceptable calls from a whitelist of contacts  |
| Loss or stolen device protection  | Mitigates risk of compromising corporate and personal data on a lost or stolen smartphone by remotely locating the device, locking it remotely, setting off an onboard alarm, or even remotely wiping the device contents to ensure corporate and personal security |
| Remote backup and restore   | Facilitates, remote backups of personal and business data, and easily imports the backed up data into a new device, if needed   |
| Short Message Service (SMS), Multimedia Messaging Service (MMS), and email message content monitoring | Enables the viewing of all messages sent and received, ensuring no inappropriate, illegal, or illicit contact   |

## Solution Components

The Mobile Security Suite is comprised of the Junos Pulse Mobile Security Gateway management console and the Juniper Networks Junos Pulse mobile client\*. These components are required to deploy security on mobile devices.

### Junos Pulse

The Junos Pulse mobile clients\* are available for download by users or banks and financial services firms from the respective application stores and marketplaces for the supported mobile device operating platforms. These application stores and marketplaces include:

- Google Android Market\*
- Nokia Ovi Store\*
- Microsoft Windows Marketplace\*
- BlackBerry App World\*

### Junos Pulse Mobile Security Gateway

The Junos Pulse Mobile Security Gateway is an easy to use console for managing and controlling all of the features and functionality of the Mobile Security Suite. The Mobile Security Gateway is available as a Software as a Service (SaaS) hosted option for easy deployment without the need for an onsite server, and wireless setup and maintenance.

The hosted SaaS deployment of the Mobile Security Gateway enables a web-based console using any SSL-enabled Web browser from which administrators may create and manage the mobile security and remote management policies of the Mobile Security Suite. The management console in the SaaS deployment is hosted by Juniper Networks on our secure data center, with protected access enabled so that administrators for banks and financial services firms can manage policies at any time, from virtually anywhere.

The user and device authentication, device integrity, and security checks can then be leveraged by the Juniper Networks Unified Access Control solution or other existing NAC appliances to allow, disallow, or limit mobile banking and financial services application access.

## Summary—Secure Mobile Banking and Financial Services and Transactions

With the explosion of smartphones and intelligent mobile devices, and the ever increasing use of these devices to access banking and financial services data and applications, the potential for threats to sensitive consumer and corporate financial data are real and emergent. The ability to ensure secure access to banking and financial data, and to enable protected financial transactions while assuring financial network and application security, should be a paramount concern and effort for banks and financial services firms today.

Junos Pulse and the Mobile Security Suite deliver the secure, assured banking and transactional services that today's mobile users require. These solutions secure mobile devices from viruses and malware, regardless of mobile operating platform, while mitigating financial data loss or theft and exploitation when a mobile device is lost or stolen. Simultaneously, Junos Pulse and the Mobile Security Suite provide banks and financial institutions with the assurance that a compromised user device or unauthenticated user cannot hack or breach their network and mobile banking, securities trading, or transactional services applications, delivering an unprecedented level of mobile security and peace of mind.

\* Junos Pulse for Google Android and Junos Pulse for BlackBerry will be available in late October 2010. Junos Pulse for Nokia Symbian will be available in late November 2010. Junos Pulse for Windows Mobile will be available in late December 2010.

## Next Steps

For more information on Juniper Networks Junos Pulse and Junos Pulse Mobile Security Suite, please refer to the Juniper Networks website at [www.juniper.net/us/en/products-services/software/software-platforms/junos-platform/junos-pulse](http://www.juniper.net/us/en/products-services/software/software-platforms/junos-platform/junos-pulse), and please contact your authorized Juniper Networks representative.

## About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at [www.juniper.net](http://www.juniper.net).

---

### 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](http://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

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

Copyright 2010 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.